Aruba 5400R zl2 Switch Series

FIPS 140-2 Non-Proprietary Security Policy

Security Level 1 Validation

Hardware Versions: Switches: 5406R zl2 J9821A [1] and 5412R zl2 J9822A [2]; Interface Modules: J9537A [2], J9546A [2], J9986A [1,2], J9987A [1,2], J9988A [1,2], J9989A [2], J9990A [1,2], J9991A [2], J9992A [2], J9993A [1,2], J9995A [1,2], J9996A [2]); Management Module: J9827A [1,2]

Firmware version: KB.16.02.0015

Version 1.4

June 19, 2017

Disclaimer

The information contained in this document is subject to change without notice.

HEWLLETT PACKARD ENTERPRISE COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Hewlett Packard Enterprise (HPE) shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HPE products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be constructed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett Packard Enterprise assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett Packard Enterprise.

Table of Contents

TABLE OF TABLES and FIGURES

FIPS 140-2 Non-Proprietary Security Policy for the Aruba 5400R zl2 Switch Series

Keywords: Security Policy, CSP, Roles, Service, Cryptographic Module

TABLE 1 - LIST OF ABBREVIATIONS

Abbreviation	Full spelling
ACL	Access Control List
AES	Advanced Encryption Standard
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program

Abbreviation	Full spelling
CSP	Critical Security Parameter
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DOA	Dead on arrival
FIPS	Federal Information Processing Standard
HMAC	Hash-based Message Authentication Code
HTTP	Hyper Text Transfer Protocol
IRF	Intelligent Resilient Framework
KAT	Known Answer Test
LED	Light Emitting Diode
MPU	Main Processing Unit
NIST	National Institute of Standards and Technology
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RIP	Routing Information Protocol
RSA	Rivest Shamir and Adleman method for asymmetric encryption
sFlow	Sampled Flow
SFP	Small Form-Factor Pluggable
SFP+	Enhanced Small Form-Factor Pluggable
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer

1 Introduction

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Aruba 5400R zl2 Switch Series from Aruba Networks. This Security Policy describes how the Aruba 5400R zl2 Switch Series meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Overall Level 1 FIPS 140-2 validation of the module. The Aruba 5400R zl2 Switch Series is referred to in this document as Aruba 5400R zl2 Switch Series, the switches, the cryptographic modules, or the modules.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The HPE website (www.hpe.com) contains information on the full line of products from HPE.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to HPE and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Hewlett Packard Enterprise.

2 Overview

The Aruba 5400R zl2 Switch Series is an industry-leading mobile campus access solution with HPE Smart Rate multi-gigabit ports for high-speed connectivity and bandwidth for next wave 802.11ac devices. It brings enterprise-class resiliency and innovative flexibility and scalability to mobile-first networks.

Robust virtualization with AllianceOne solutions, hitless failover, QoS, and security with full L3 features and flexible connectivity including 40 Gigabit Ethernet ports and full PoE+, the Aruba 5400R requires no add-on software licensing and is SDN ready with OpenFlow support.

The Aruba 5400R zl2 Switch Series is suitable for a range of uses. These switches can be deployed at enterprise edge and remote branch offices, and converged networks. Each device is based on the Aruba OS-CX Software, version KB.16.02.0015 platform. The module firmware runs on a customized Greenhills (GHS) Integrity Operating System, version 5.0.11.

The Aruba 5400R zl2 Switch Series modules are being validated as a multi-chip standalone network device at FIPS 140-2 Overall Security Level 1.

Test Modules

Testing included 2 models in the Aruba 5400R zl2 Switch Series

- Aruba 5406R zl2 Switch (J9821A)
- Aruba 5412R zl2 Switch (J9822A)

The following two (2) test configurations are for the Aruba 5400R zl2 Switch Series. Each configuration has a main MPU.

Aruba 5406R zl2 Switch (J9821A)

FIGURE 1 - 5406R ZL2 SERIES SWITCH

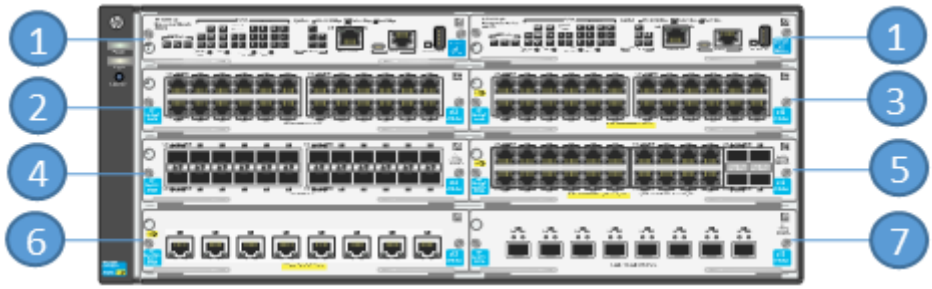

Table 2 lists the test configurations for the Aruba 5406R zl2 Switch Series

Chassis	Modules	Position
Aruba 5406R zl2 Switch (J9821A)	J9827A zl2 Management Module	1
	J9827A zl2 Management Module	1
	J9987A 24p 1000BASE-T v3 zl2 Module	2
	J9986A 24p 1000BASE-T PoE+ v3 zl2 Module	3
	J9988A 24p SFP v3 zl Module	4
	J9990A 20p PoE+ / 4p SFP+ v3 zl2 Module	5
	J9995A 8-port 1/2.5/5/10GBASE-T PoE+ MACsec v3 zl2 Module	6
	J9993A 8p 1G/10GbE SFP+ v3 zl2 Module	7

TABLE 2 - TEST CONFIGURATION 1

FIGURE 2 - 5412R ZL2 SERIES SWITCH

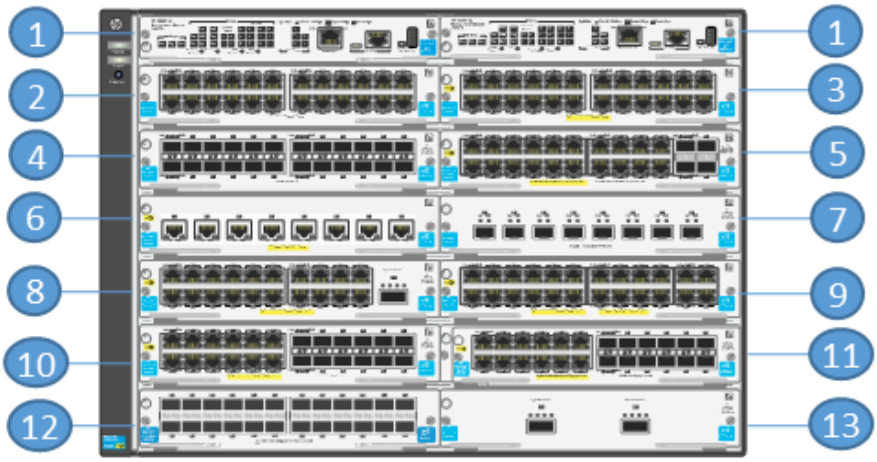

Table 3 lists the test configurations for the Aruba 5412R zl2 Switch Series

Chassis	Modules	Position

Aruba 5412R zl2 Switch (J9822A)	J9827A zl2 Management Module	1
	J9827A zl2 Management Module	1
	J9987A 24p 1000BASE-T v3 zl2 Module	2
	J9986A 24p 1000BASE-T PoE+ v3 zl2 Module	3
	J9988A 24p SFP v3 zl Module	4
	J9990A 20p PoE+ / 4p SFP+ v3 zl2 Module	5
	J9995A 8-port 1/2.5/5/10GBASE-T PoE+ MACsec v3 zl2 Module	6
	J9993A 8p 1G/10GbE SFP+ v3 zl2 Module	7
	J9992A 20p PoE+ / 1p 40GbE QSFP+ v3 zl2 Module	8
	J9991A 20p PoE+ / 4p 1/25/5/XGT PoE+ v3 z12 Module	9
	J9989A 12p PoE+ / 12p 1GbE SFP v3 zl2 Module	10
	J9546A 8-port 10GBASE-T v2 zl Module	11
	J9537A 24-port SFP v2 zl Module	12
	J9996A 2p 40GbE QSFP+ v3 zl2 Module	13

TABLE 3 - TEST CONFIGURATION 2

3 Security Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	3
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
12	Overall Level	1

TABLE 4 - VALIDATION LEVEL BY SECTION

4 Cryptographic Module Specifications

The Aruba 5400R zl2 Switch Series is a multi-chip standalone network device. The cryptographic boundary is defined as encompassing the "top," "front," "rear", "left," "right," and "bottom" surfaces of the case. The general components of the Aruba 5400R zl2 Switch Series include firmware and hardware, which are placed in the three-dimensional space within the case.

Aruba 5406R zl2 Switch (J9821A)

The Aruba 5406R zl2 Switch offers power and management redundancy in a modular 6-slot chassis supporting v2 zl and v3 zl2 modules providing 1GbE, 10GbE and 40GbE ports, multi-gigabit HPE Smart Rate ports, and full PoE+. Supports a maximum of 144 autosensing 10/100/1000 ports or 144 SFP ports or 48 SFP+ ports or 48 HPE Smart Rate Multi-Gigabit or 12 40GbE ports, or a combination.

The following are the specifications for this switch:

- Supports throughput of up to 571.4 Mpps.
- Switching capacity of 960 Gbps.
- The management features: CLI, out of band management (RJ-45, RS-232 or micro usb).

Aruba 5412R zl2 Switch (J9822A)

The Aruba 5412R zl2 Switch offers power and management redundancy in a modular 12-slot chassis supporting v2 zl and v3 zl2 modules providing 1GbE, 10GbE and 40GbE ports, multi-HPE gigabit HPE Smart Rate ports, and full PoE+. Supports a maximum of 288 autosensing 10/100/1000 ports or 288 SFP ports or 96 SFP+ ports or 96 HPE Smart Rate Multi-Gigabit or 24 40GbE ports, or a combination.

The following are the specifications for this switch:

- Supports throughput of up to 1142.8 Mpps.
- Switching capacity of 1920 Gbps.
- The management features: CLI, out of band management (RJ-45, RS-232 or micro usb).

The documents on HPE website describe the ports in detail along with the interpretation of the LEDs.

5 Cryptographic Module Port and Interfaces

The Aruba 5406R zl2 and 5412R zl2 cryptographic modules physical ports can be categorized into the following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface
- Power Interface

Aruba 5400R zl2 Series Ports

Console Port

There are two serial console ports on the switch. One port uses the RJ-45 serial cable and the other port uses a MicroUSB cable. This connection is described under “Connect the Management Console of the Switch” in Chapter 2, “Installing the 5400R zl2 Switches”. The console is a full-featured interface that can be used to configure, monitor, and troubleshoot the switch. It can be run on a PC, laptop, or hand held device emulating a VT-100 terminal, or on a standard VT-100 terminal.

Out-of-Band Management (OOBM) Port

This RJ-45 port is used to connect a dedicated management network to the switch.

To use: connect an RJ-45 network cable to the Management port to manage an HP 5400R zl2 Switch through Telnet from a remote PC or a UNIX workstation.

To use this port, the switch must have an IP address. IP settings can be configured through a Console port connection or automatically from a DHCP/Bootp server. A networked out-of-band connection through the Management port allows you to manage data network switches from a physically and logically separate management network.

For more information, see the "Network Out-of-Band Management (OOBM)" appendix in the Management and Configuration Guide at: www.hpe.com/us/en/networking/switches.html.

Aruba 5400R Series Ports

Additional information in the *HP 5400R zl2 Switches Installation and Getting Started Guide.*

The Aruba 5400R zl2 Series data and management ports are located on the switch front panel.

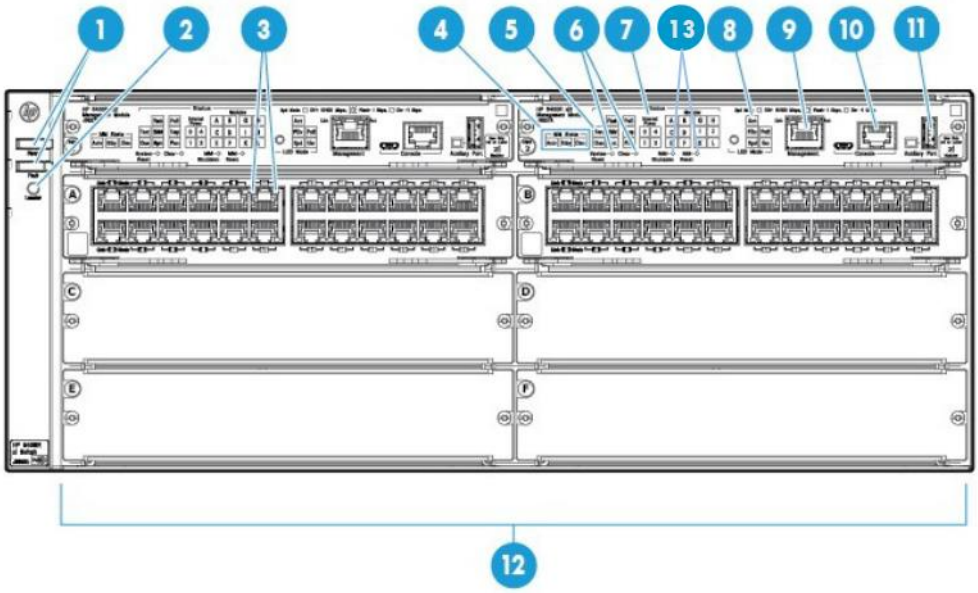

FIGURE 3 - FRONT OF ARUBA 5400R ZL2 SWITCH

This illustration shows the 5406R zl2 Switch, but the labeling and descriptions apply to all of the Aruba 5400R zl2 switches.

NUMBER	LABEL
1	Power and Fault LEDs
2	Locator LED
3	Module Link and Mode LEDs
4	Management Module Status LEDs
5	Status LEDs

6	System Reset and Clear buttons
7	Status LEDs for the Fans, Power Supplies, and Switch Modules
8	LED Mode Select button and indicator LEDs
9	OOBM Port
10	Console Port
11	Auxiliary Port
12	Switch Modules with Link and Mode LEDs for each port
13	MM Shutdown and MM Reset buttons

TABLE 5 - LIST OF PORTS ON FRONT PANEL

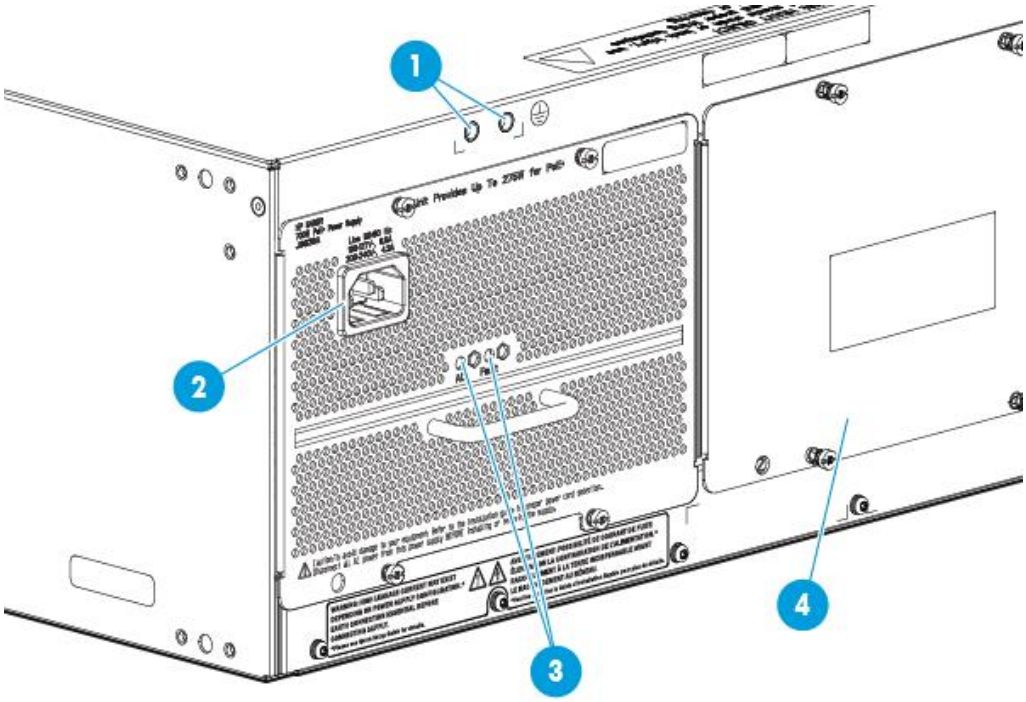

FIGURE 4 - BACK OF A 5406R ZL2 SWITCH WITH ONE POWER SUPPLY

NUMBER	LABEL

1	Ground lug mounting holes
2	AC power connector
3	Power and Fault LEDs
4	Slot for installing optional redundant power supply

TABLE 6 - LIST OF PORTS ON REAR PANEL

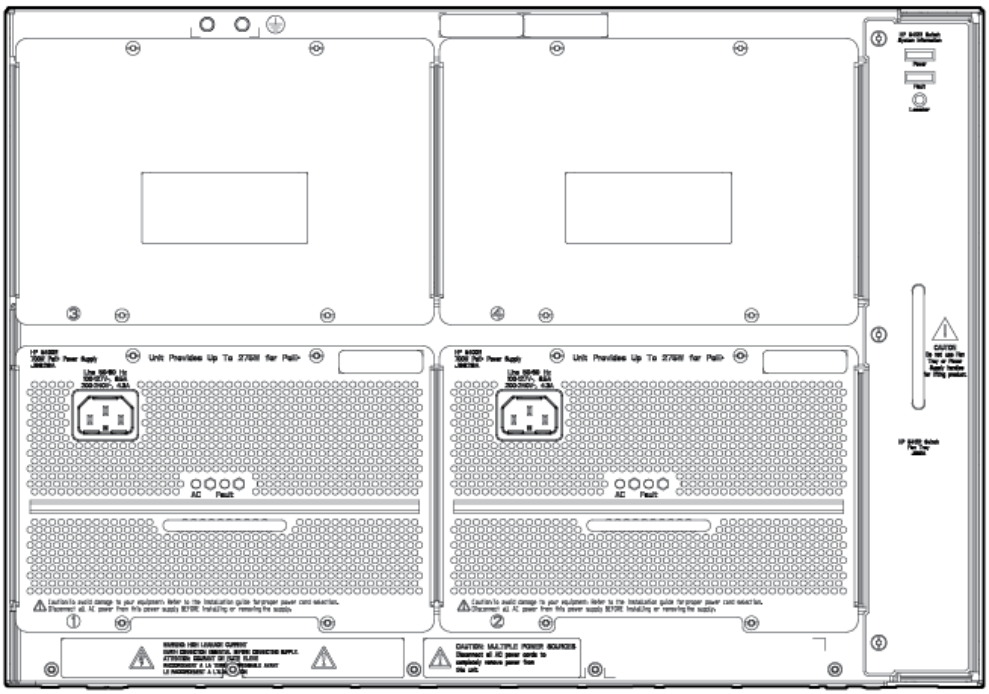

FIGURE 5 - BACK OF A 5412R ZL2 SWITCH WITH TWO POWER SUPPLIES

Load-sharing redundant power supplies can be installed in the back of the 5400R zl2 switches. To provide redundancy, each power supply should be connected to different AC power sources. Then, if one AC power source fails, the switch will continue to run.

Aruba 5400R zl2 Series Ports and Interfaces

The mapping of logical and physical interfaces to the FIPS validated configuration of the 5406R zl2 switch is detailed in Table 7.

TABLE 7 – MAPPING OF FIPS 140-2 LOGICAL INTERFACES TO THE 5406R ZL2 SWITCH

Physical Interfacing Component	FIPS 140-2 Logical Interfaces	5406R zl2 Switch Port/Interface
(2) Management Card	Data Input	(1) RJ-45 Gig-T OOBM port (2) RS-232[1] serial port (RJ-45, mini-USB) (1) Auxiliary (USB) port
	Data Output	(1) RJ-45 Gig-T OOBM port (2) RS-232 serial port (RJ-45 and mini-USB) (1) Auxiliary (USB) port
	Control Input	(1) RJ-45 Gig-T OOBM port (2) RS-232 serial port (RJ-45 and mini-USB) (1) Auxiliary (USB) port (1) System Reset Push Button (1) Clear Push Button (1) MM Shutdown Push Button (1) MM Reset Push Button (1) LED Mode Push Button
	Status Output	(1) RJ-45 Gig-T OOBM port (2) RS-232 serial port (RJ-45 and mini-USB) (1) Auxiliary (USB) port (35) LEDs
	Power Input	(1) AC[2] Power Interface

[1] RS – Recommended Standard

[2] AC – Alternating Current

Physical Interfacing Component	FIPS 140-2 Logical Interfaces	5406R zl2 Switch Port/Interface
(1) 700W PoE+ zl2 Power Supply	Status Output	(2) LED Indicators
(1) Status Panel	Status Output	(3) LED Indicators
(1) High performance fan tray	Status Output	(3) LED Indicators

The mapping of logical and physical interfaces to the FIPS validated configuration of the 5412R zl2 switch is detailed in Table 8.

TABLE 8 – MAPPING OF FIPS 140-2 LOGICAL INTERFACES TO THE 5412R ZL2 SWITCH

Physical Interfacing Component	FIPS 140-2 Logical Interfaces	5412R zl2 Switch Port/Interface
(2) Management Card	Data Input	(1) RJ-45 Gig-T OOBM port (2) RS-232 serial port (RJ-45 and mini-USB) (1) Auxiliary (USB) port
	Data Output	(1) RJ-45 Gig-T OOBM port (2) RS-232 serial port (RJ-45 and mini-USB) (1) Auxiliary (USB) port

Physical Interfacing Component	FIPS 140-2 Logical Interfaces	5412R zl2 Switch Port/Interface
	Control Input	(1) RJ-45 Gig-T OOBM port (2) RS-232 serial port (RJ-45 and mini-USB) (1) Auxiliary (USB) port (1) Reset Push Button (1) Clear Push Button (1) LED Mode Push Button
	Status Output	(1) RJ-45 Gig-T OOBM port (2) RS-232 serial port (RJ-45 and mini-USB) (1) Auxiliary (USB) port (35) LEDs
(2) 2750W PoE+ zl2 Power Supply	Power Input	(2) AC Power Interfaces
	Status Output	(4) LED Indicators
(1) Status Panel	Status Output	(3) LED Indicators
(1) High performance fan tray	Status Output	(3) LED Indicators

Aruba 5400R zl2 and v3 zl2 Interface Cards

The 5400R zl2 Switch Series modules support a number of different zl2 and v3 zl2 Series Interface Cards. The 5406R zl2 switches can support up to 6 zl2 and v3 zl2 Interface Cards, while the 5412R zl2 switches can support up to 12 zl2 and v3 zl2 Interface Cards. The type and number of interfaces vary on each type of Interface Card.

Aruba affirms that the 5400R zl2 Switch Series cryptographic modules will continue to operate at the same level of cryptographic security as the validated configurations when additional Interface Cards listed in Table 9 are introduced.

Table 9 – Mapping of FIPS 140-2 Logical Interfaces to Compatible zl and zl2 interface cards

Card Name	Supported FIPS 140-2 Logical Interfaces	Interface Card Ports/Interfaces
Aruba J9537A 24-port SFP v2 zl Module	Data In	(24) SFP ports
	Data Out	(24) SFP ports
	Control In	(24) SFP ports
	Status Out	(24) SFP ports, (48) LEDs
Aruba J9546A 8-port 10GBASE-T v2 zl Module	Data In	(8) RJ-45 10GBase-T ports
	Data Out	(8) RJ-45 10GBase-T ports
	Control In	(8) RJ-45 10GBase-T ports
	Status Out	(8) RJ-45 10GBase-T ports, (16) LEDs
Aruba J9986A 24p 1000BASE-T PoE+ v3 zl2 Module	Data In	(24) RJ-45 Gig-T PoE+ ports
	Data Out	(24) RJ-45 Gig-T PoE+ ports
	Control In	(24) RJ-45 Gig-T PoE+ ports
	Status Out	(24) RJ-45 Gig-T PoE+ ports (48) LEDs
	Power Out	(24) RJ-45 Gig-T PoE+ ports
Aruba J9987A 24p 1000BASE-T v3 zl2 Module	Data In	(24) RJ-45 Gig-T ports
	Data Out	(24) RJ-45 Gig-T ports
	Control In	(24) RJ-45 Gig-T ports
	Status Out	(24) RJ-45 Gig-T ports (48) LEDs
	Data In	(24) SFP ports

Aruba J9988A 24p SFP v3 zl Module	Data Out	(24) SFP ports
	Control In	(24) SFP ports
	Status Out	(24) SFP ports, (48) LEDs
Aruba J9989A 12p PoE+ / 12p 1GbE SFP v3 zl2 Module	Data In	(12) RJ-45 Gig-T PoE+ ports (12) SFP ports
	Data Out	(12) RJ-45 Gig-T PoE+ ports (12) SFP ports
	Control In	(12) RJ-45 Gig-T PoE+ ports (12) SFP ports
	Status Out	(12) RJ-45 Gig-T PoE+ ports (12) SFP ports (48) LEDs
	Power Out	(12) RJ-45 Gig-T PoE+ ports
Aruba J9990A 20p PoE+ / 4p SFP+ v3 zl2 Module	Data In	(20) RJ-45 Gig-T PoE+ ports (4) SFP+ ports
	Data Out	(20) RJ-45 Gig-T PoE+ ports (4) SFP+ ports
	Control In	(20) RJ-45 Gig-T PoE+ ports (4) SFP+ ports
	Status Out	(20) RJ-45 Gig-T PoE+ ports (4) SFP+ ports (48) LEDs
	Power Out	(20) RJ-45 Gig-T PoE+ ports

Aruba J9991A 20p PoE+ / 4p 1/25/5/XGT PoE+ v3 zl2 Module	Data In	(20) RJ-45 Gig-T PoE+ ports (4) RJ-45 1/2.5/5/10GBase-T PoE+ ports
	Data Out	(20) RJ-45 Gig-T PoE+ ports (4) RJ-45 1/2.5/5/10GBase-T PoE+ ports
	Control In	(20) RJ-45 Gig-T PoE+ ports (4) RJ-45 1/2.5/5/10GBase-T PoE+ ports
	Status Out	(20) RJ-45 Gig-T PoE+ ports (4) RJ-45 1/2.5/5/10GBase-T PoE+ ports (48) LEDs
	Power Out	(20) RJ-45 Gig-T PoE+ ports (4) RJ-45 1/2.5/5/10GBase-T PoE+ ports
Aruba J9992A 20p PoE+ / 1p 40GbE QSFP+ v3 zl2 Module	Data In	(20) RJ-45 Gig-T PoE+ ports (1) QSFP+ 40GbE port
	Data Out	(20) RJ-45 Gig-T PoE+ ports (1) QSFP+ 40GbE port
	Control In	(20) RJ-45 Gig-T PoE+ ports (1) QSFP+ 40GbE port
	Status Out	(20) RJ-45 Gig-T PoE+ ports (1) QSFP+ 40GbE port (44) LEDs
	Power Out	(20) RJ-45 Gig-T PoE+ ports
Aruba J9993A 8p 1G/10GbE SFP+ v3 zl2 Module	Data In	(12) SFP+ ports
	Data Out	(12) SFP+ ports
	Control In	(12) SFP+ ports

	Status Out	(12) SFP+ ports (24) LEDs
Aruba J9995A 8-port 1/2.5/5/10GBASE-T PoE+ MACsec v3 zl2 Module	Data In	(8) RJ-45 1/2.5/5/10GBase-T PoE+ ports
	Data Out	(8) RJ-45 1/2.5/5/10GBase-T PoE+ ports
	Control In	(8) RJ-45 1/2.5/5/10GBase-T PoE+ ports
	Status Out	(8) RJ-45 1/2.5/5/10GBase-T PoE+ ports (16) LEDs
	Power Out	(8) RJ-45 1/2.5/5/10GBase-T PoE+ ports
Aruba J9996A 2p 40GbE QSFP+ v3 zl2 Module	Data In	(2) QSFP+ 40GbE port
	Data Out	(2) QSFP+ 40GbE port
	Control In	(2) QSFP+ 40GbE port
	Status Out	(2) QSFP+ 40GbE port (8) LEDs

6 Roles, Services, and Authentication

Roles

Each cryptographic module supports three roles that an operator can assume: a Crypto Officer (Manager) role, a User (Operator) role, and a Security Officer role. Each role is accessed through proper role-based authentication to the switch. Services associated with each role are listed in the following sections.

The Crypto Officer is responsible for the set up and initialization of the Aruba 5400R zl2 Switch Series as documented in Section 11 (Delivery and Operation) of this document. The Crypto Officer has complete control of the switches and is in charge of configuring all of the settings for each switch. The Crypto Officer can create RSA key pairs for SSHv2. The Crypto Officer is also in charge of maintaining access control and checking error and intrusion logs.

The User role can show the current secure-mode of the switch and connect to the switch remotely via SSHv2.

The Security Officer role is to view and delete the security logs. This role can also copy the security logs from the switch and do not have permission to execute any other commands. The security logs cannot be viewed or deleted by other roles on the switch.

Table 10 presents the roles and roles description. The devices allow multiple management users to operate the networking device simultaneously. The Aruba 5400R zl2 Switch Series does not employ a maintenance interface and does not have a maintenance role.

FIPS Role	Role Description
Crypto Officer	Configuration of CSPs for normal switch operation
	Manage Crypto Officer, User, and BootROM passwords
	Reboot the system into a FIPS-Approved mode of operation
	Reboot the system into a non-FIPS Approved mode of operation
	Zeroize all keys and CSPs
	Establish a remote SSHv2 session with the switch
	Reboot the switch; perform self-tests on demand

	Display the current secure mode of the switch
	View syslog for system status, warnings, and errors
User	Establish a remote SSHv2 session with the module
	Display the current secure mode of the module
	Control the “Chassis Locate” LED
	View syslog for system status, warnings, and errors
Security Officer	View and delete security logs. Copy security logs from the switch. Do not have permission to execute any other commands on the switch by default. The security log commands are not executable from any other user including cryptographic-officer.

TABLE 10 - ROLES AND ROLE DESCRIPTION

Services

All services are available in FIPS mode and non-FIPS Approved mode.

The user can access the Aruba switches through:

- Console Port
- SSH

The console port and SSH present a command line interface.

Crypto Officer Services

The Crypto Officer role is responsible for the configuration and maintenance of the switches. The Crypto Officer services consist of the following:

TABLE 11 - CRYPTO OFFICER SERVICES

Description	Input	Output	CSP Access
View Device Status			
1. View currently running image version; 2. View installed hardware components status and version	Commands	Status of devices	None
View Running Status			

1. View memory status, packet statistics, interface status, current configuration, routing table, active sessions, temperature and SNMP MIB statistics.	Commands	Status of device functions	None
Perform Network Functions			
1. Network diagnostic service such as “ping”; 2. Network connection service such as “SSHv2” client; 3. Provide TLS service to protect the session between the switch and external server (e.g. Radius Server/Log Server) 4. Initial Configuration setup (IP, hostname, DNS server)	Commands and configuration data	Status of commands and configuration data	CSP2-1 SSH Private key (write/delete) CSP2-2 SSH Diffie-Hellman Key Pairs (write/delete) CSP2-3 SSH Session Key (write/delete) CSP2-4 SSH Session authentication Key (write/delete) CSP3-1 Crypto-Officer Password (write/delete) CSP4-1 DRBG seed (write) CSP4-2 DRBG V (write) CSP4-3 DRBG Key (write) CSP5-2 TLS Master secret (write/delete) CSP5-3 TLS Traffic encryption key (write/delete) CSP5-4 TLS traffic authentication key (write/delete) CSP5-6 TLS Server public key(write/delete)
Perform Security Management			

1. Change the role; 2. Reset and change the password of same/lower privilege user; 3. Maintenance of the User role and Security Officer password; 4. Maintenance of the bootware password; 5. Maintenance (create, destroy, import, export) of public key/private key/shared key; 6. Management (create, delete, modify) of the user roles; 7. Management of the access control rules for each role; 8. Management (create, delete, modify) of the user account; 9. Management of the time; 10. Maintenance (delete, modify) system start-up parameters; 11. File operation (e.g. dir, copy, del); 12. Perform self-tests 13. Shut down or Reboot the networking device;	Commands and configuration data	Status of commands and configuration data	CSP1-1 RSA private key (write/delete) CSP1-2 RSA Public keys (write/delete) CSP2-1 SSH Private key (write/delete) CSP2-2 SSH Diffie-Hellman Key Pairs (write/delete) CSP2-3 SSH Session Key (write/delete) CSP2-4 SSH Session authentication Key (write/delete) CSP3-1 Crypto-Officer Password (write/delete) CSP3-2 User-role Password (write/delete) CSP3-3 RADIUS shared secret keys (write/delete) CSP3-4 TACACS+ shared secret keys (write/delete) CSP3-5 Security-Officer Password(write/delete) CSP4-1 DRBG seed (delete) CSP4-2 DRBG V (delete) CSP4-3 DRBG Key (delete) CSP1-4 Key encrypting key (read) CSP5-1 TLS Server private key (write/delete) CSP5-2 TLS Master secret (write/delete) CSP5-3 TLS Traffic encryption key (write/delete) CSP5-4 TLS traffic authentication key (write/delete) CSP5-6 TLS Server public key(write/delete)
Perform Configuration Functions			
1. Save configuration; 2. Management of information center; 3. Define network interfaces and settings; 4. Set the protocols the switches will support (e.g. SFTP server, SSHv2 server); 5. Enable interfaces and network services; 6. Management of access control scheme 7. Shut down or Reboot the networking device; 8. Change Mode: This service configures the module to run in a FIPS Approved mode 9. Reset of the CSPs.	Commands and configuration data	Status of commands and configuration data	CSP1-1 RSA private key (write/delete) CSP1-2 RSA Public keys (read/write/delete) CSP3-1 Crypto-Officer Password (write/delete) CSP3-2 User-role Password (write/delete) CSP3-3 RADIUS shared secret keys (write/delete) CSP3-4 TACACS+ shared secret keys (write/delete) CSP3-5 Security-Officer Password(write/delete) CSP4-1 DRBG seed (delete) CSP4-2 DRBG V (delete) CSP4-3 DRBG Key (delete) CSP5-1 TLS Server private key (write/delete)

User Services

The following table describes the services available to user service.

TABLE 12 - USER SERVICES

Description	Input	Output	CSP Access
View Device Status			
1. View currently running image version; 2. View installed hardware components status and version	Commands	Status of devices	None
View Running Status			
1. View memory status, packet statistics, interface status, current configuration, routing table, active sessions, temperature and SNMP MIB statistics.	Commands	Status of device functions	None
Perform Network Functions			
1. Network diagnostic service such as “ping”; 2. Network connection service such as “SSHv2” client;	Commands and configuration data	Status of commands and configuration data	CSP2-1 SSH Private key (read/write/delete) CSP2-2 SSH Diffie-Hellman Key Pairs (read/write/delete) CSP2-3 SSH Session Key (read/write/delete) CSP2-4 SSH Session authentication Key (read/write/delete)

Security Officer Services

The following table describes the services available to security officer.

TABLE 13 - SECURITY OFFICER SERVICES

Description	Input	Output	CSP Access
Execution of Security Log Related Commands			
1. Security logs: The security user can only view security logs and does not have permission to execute any other commands on the switch.	Commands	Logs	CSP3-5 Security-Officer Password (write/delete)

Unauthenticated Services

- Cycle the power on the switch
- Perform self-tests at power on
- Observe status LED

Authentication Mechanisms

The Aruba 5400R zl2 Switch Series supports identity-based authentication to control access to all services provided by the switches. The username and password will be configured by the Crypto Officer and the operator or Security officer will be able to login using these credentials. Once the operator or security officer is authenticated, they will assume their respective role and will be able to carry out the available services listed in Table 11, Table 12, and Table 13.

Authentication Data Protection

The Aruba 5400R zl2 Switch Series does not allow the disclosure, modification, or substitution of authentication data to unauthorized operators. Authentication data can only be modified by the operator who has assumed the Crypto Officer role.

Identity-based Authentication

Each user is authenticated upon initial access to the device. The authentication is identity-based. All users can be authenticated locally, and optionally supports authentication via a RADIUS and TACACS+ server.

The authentication method is Username and Password.

To logon to the networking devices, an operator must connect to it through one of the management interfaces (console port, SSH) and provide a password.

A user must be authenticated using username and password. The minimum password length is 8 characters, and the maximum is 64. The passwords can contain the following, equaling 94 possibilities per character:

lower case letters (26),
upper case letters (26),
special characters (32) and
numeric characters (10)

Therefore, for 8 characters password, the probability of randomly guessing the correct sequence is 1 in 94^8 (this calculation is based on the use of the typical standard American QWERTY computer keyboard.)

The users who try to log in or switch to a different user privilege level can be authenticated by RADIUS and TACACS+ Server. The minimum password length is 8 characters, and the maximum is 64. Therefore, for 8 characters password, the probability of randomly guessing the correct sequence is one in 94^8. The device (RADIUS client) and the RADIUS server use a shared key to authenticate RADIUS

packets and encrypt user passwords exchanged between them. For more details, see RFC 2865: 3 Packet Format Authenticator field and 5.2 User-password.

The module requires an 8 character password with 94 possible characters per password character; therefore requiring 94^8/100,000 = $6.096x10^{10}$ password attempts in 60 seconds to surpass the 1:100,000 ratio. The processor speed is 666MHz, translating to $1.5x10^{-9}$ seconds per cycle. Assuming worst case scenario and no overhead, to process ($6.096x10^{10}$ passwords * 8 bits =) $4.877x10^{11}$ bits of data, it would take the processor (($4.877x10^{11}$ bits x$1.5x10^{-9}$ seconds per cycle)/8 bits per cycle=) 91 seconds to process all $6.096x10^{10}$ password attempts. Therefore the password strengths meet FIPS 140-2 requirements.

There is a CLI command to configure the minimum password length between 8 and 64.

7 Physical Security Mechanism

The 5400R Switch Series meets the FIPS 140-2 Level 1 security requirements as production grade equipment.

8 Cryptographic Algorithms

FIPS Approved Cryptographic Algorithms

The following table lists the FIPS-Approved algorithms Aruba 5400R zl2 Switch Series provide.

TABLE 14 - FIPS-APPROVED CRYPTOGRAPHY ALGORITHMS

CAVP Certificate	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
AES #4304	AES[3]	FIPS 197, SP 800-38A, SP 800-38D	CBC, ECB	128, 192, 256	Data Encryption/ Decryption
CVL #1018	TLS 1.0/1.1/1.2, SSHv2, SNMPv3 KDFs[4]	SP 800-135rev1			Key Derivation
DRBG #1365	DRBG	SP 800-90A	CTR (AES-256)		Deterministic Random Bit Generation
HMAC #2840	HMAC[5]	FIPS 198-1	HMAC SHA-1	160	Message Authentication
SHS #3543	SHS[6]	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest
DSA #1144	DSA	FIPS 186-4	DSA	1024	Digital Signature Verification
RSA #2325	RSA	FIPS 186-4	Fixed Public Exponent e 10001	2048, 3072	Key Pair Generation
			SHA-256, PKCS1 v.1.5	2048	Digital Signature Generation
			SHA-1, SHA-256, SHA-384, SHA-512, PKCS1 v1.5	1024- to 3072 bit keys	Digital Signature Verification

[3] ECB is not used by any of the module's services.

[4] This module supports the SNMP, SSH and TLS protocols with SP 800-135 rev 1 KDF primitives. However, the SNMP, SSH and TLS Protocols have not been reviewed or tested by the CMVP or CAVP

[5] HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, and HMAC SHA-512 are not used by any of the module's services.

[6] SHA-224 is not used by any of the module's services

CAVP Certificate	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
Triple-DES #2325	Triple-DES	SP 800-67	Triple-DES - CBC	168	Data Encryption/ Decryption

FIPS Allowed Cryptographic Algorithms

The following table contains the set of FIPS Allowed cryptographic algorithms that can also be used in FIPS-mode.

TABLE 15 - FIPS-ALLOWED CRYPTOGRAPHY ALGORITHMS

Algorithm	Application
Diffie-Hellman (L = 2048, N = 224)	Key establishment (provides 112 bits of encryption strength)
Message Digest 5 (MD5)	KDF in TLS 1.0/1.1 Message authentication for use with OSPF, BGP, RADIUS, TACACS, and RIP
NDRNG	Seeding for the Approved DRBG (contain no less than 256 bits of entropy)
EC Diffie-Hellman	TLS Curves supported : secp256r1, secp384r1, secp521r1, secp224r1 (provides 112 to 256 bits of encryption strength)
RSA	Key wrapping; Key establishment (provides 112 bits of encryption strength)

Non-FIPS Approved Cryptographic Algorithms

The following table contains the set of non-FIPS Approved algorithms that are implemented but may not be used when operating in FIPS-mode. These algorithms are used in non-FIPS-mode.

TABLE 16 - NON-FIPS APPROVED CRYPTOGRAPHY ALGORITHMS

Algorithm	Application
DES	Encryption/Decryption

Algorithm	Application
Diffie-Hellman (< 2048-bits)	Key Agreement
RC4	Encryption/Decryption
MD5	Hashing
HMAC MD5	Message Authentication
RSA (<2048-bits)	SSH Key Pair Generation, Digital Signature Generation Digital Signature Verification
ECDSA (non-compliant)	Digital Signature Generation Digital Signature Verification

9 Cryptographic Key Management

Cryptographic Security Parameters

The networking devices use a variety of Critical Security Parameters (CSP) during operation. The following table lists the CSP including cryptographic keys used by the Aruba 5400R zl2 Switch Series. It summarizes generation, storage, and zeroization methods for the CSP.

TABLE 17 - CRYPTOGRAPHIC SECURITY PARAMETERS

#	Key/ CSP Name	Algorithm	Key Size	Description	Key / CSP Entry		Key / CSP Output		Zeroization
					Origin	Storage	Output	Format	
Public key management									
CSP1-1	RSA private key	RSA	2048 bits	Identity certificates for the networking device itself.	Internal	FLASH (plain text)	No	NA	Using CLI command to zeroize.
CSP1-2	RSA Public keys	RSA	2048 bits	Public keys used to validate the firmware image.	Generated Externally	FLASH (plain text)	No	NA	This is part of the software code.
SSH									

#	Key/ CSP Name	Algorithm	Key Size	Description	Key / CSP Entry		Key / CSP Output		Zeroization
					Origin	Storage	Output	Format	
CSP2-1	SSH Private key	RSA	2048 bits, 3072 bits	private key used for SSH protocol	Internal	RAM/ FLASH (plain text)	No	NA	Using CLI command to zeroize
CSP2-2	SSH Diffie-Hellman Key Pairs	Diffie-Hellman	L=2048 bits N=224 bits	Key agreement for SSH sessions.	Internal	RAM (plain text)	No	NA	Automatically when handshake finishing
CSP2-3	SSH Session Key	AES-CBC	128 bits, 256 bits	SSH session symmetric key	Derived from handshake	RAM (plain text)	No	NA	Automatically when SSH session terminated
CSP2-4	SSH Session authentication Key	HMAC-SHA1	160 bits	SSH session authentication key	Derived from handshake	RAM (plain text)	No	NA	Automatically when SSH session terminated
Authentication, Authorization, and Accounting									
CSP3-1	Crypto-Officer Password	Password	8 ~ 64 bytes	Critical security parameters used to authenticate the administrator login	Entered Electronically	FLASH / RAM (obfuscated / plain text)	No	NA	Using CLI command to zeroize
CSP3-2	User-role Password	Password	8 ~ 64 bytes	Critical security parameters used to authenticate the user- role.	Entered Electronically	FLASH / RAM (obfuscated / plain text)	No	NA	Using CLI command to zeroize

#	Key/ CSP Name	Algorithm	Key Size	Description	Key / CSP Entry		Key / CSP Output		Zeroization
					Origin	Storage	Output	Format	
CSP3-3	RADIUS shared secret	Shared Secret	15 ~ 32 bytes	Used for authenticating the RADIUS server to the networking device and vice versa. Crypto-Officer in plain text form and stored in plain text form.	Entered Electronically	FLASH / RAM (obfuscated / plain text)	Via “show run” command	plain text	Using CLI command to zeroize
CSP3-4	TACACS+ shared secret	Shared Secret	15 ~ 100 bytes	Used for authenticating the TACACS+ server to the networking device and vice versa.	Entered Electronically	FLASH / RAM (obfuscated /plain text)	Via “show run” command	plain text	Using CLI command to zeroize
CSP3-5	Security-Officer Password	Password	8 ~ 64 bytes	Critical security parameters used to authenticate the security officer.	Entered Electronically	FLASH / RAM (obfuscated / plain text)	No	NA	Using CLI command to zeroize
Random Bits Generation									

#	Key/ CSP Name	Algorithm	Key Size	Description	Key / CSP Entry		Key / CSP Output		Zeroization
					Origin	Storage	Output	Format	
CSP4-1	DRBG seed	SP 800 - 90A CTR_DRBG	384 bits	Input to the DRBG that determines the internal state of the DRBG	Internal	RAM (plaintext)	No	NA	Resetting or rebooting the networking device
CSP4-2	DRBG V	SP 800 - 90A CTR_DRBG	128 bits	Generated by entropy source via the CTR_DRBG derivation function. It is stored in DRAM with plaintext form	Internal	RAM (plaintext)	No	NA	Resetting or rebooting the networking device
CSP4-3	DRBG Key	SP 800 - 90A CTR_DRBG	256 bits	DRBG key used for SP 800-90A CTR_DRBG	Internal	RAM (plaintext)	No	NA	Resetting or rebooting the networking device
TLS									
CSP5-1	TLS Server private key	RSA	2048 bits	Private key used for TLS negotiations.	Internal	RAM /FLASH (plain text)	No	NA	Using CLI command to zeroize

#	Key/ CSP Name	Algorithm	Key Size	Description	Key / CSP Entry		Key / CSP Output		Zeroization
					Origin	Storage	Output	Format	
CSP5-2	TLS Master secret	Shared key	384 bits	Shared secret used for creating TLS traffic keys.	Generated internally	RAM (plain text)	No	NA	Automatically zeroize when session terminated.
CSP5-3	TLS Traffic encryption key	AES-CBC Triple-DES	128 / 256 bits 168 bits	Used for encrypting TLS data.	Internal / Derived from handshake	RAM (plain text)	No	NA	Automatically zeroize when session terminated.
CSP5-4	TLS traffic authentication key	HMAC-SHA1	160 bits	Used for authenticating HTTPS data.	Internal / Derived from handshake	RAM (plain text)	No	NA	Automatically zeroize when session terminated.
CSP5-5	TLS Elliptic Curve Diffie-Hellman Key Pairs	EC Diffie-Hellman	secp256r1, secp384r1, secp521r1, secp224r1	Key agreement for TLS sessions.	Internal	RAM (plain text)	No	NA	Automatically when handshake finishing
CSP5-6	TLS Server public key	RSA	2048 bits	Key agreement for TLS sessions.	Internal	FLASH / RAM (plain text)	No	NA	Using CLI command to zeroize
Other									

#	Key/ CSP Name	Algorithm	Key Size	Description	Key / CSP Entry		Key / CSP Output		Zeroization
					Origin	Storage	Output	Format	
CSP6-1	Non-Approved Encrypting key	AES	256 bits	Key used to obfuscate keys stored in the 'config' file	Generated Externally	FLASH (plain text)	No	NA	This is part of the software code.

10 Self-Tests

The Aruba 5400R zl2 Switch Series performs cryptographic self-tests during power-up. The purpose of these self-tests is to verify functionality and correctness of the cryptographic algorithms listed below. Should any of the power-up self-tests or conditional self-tests fail, the module will cease operation, inhibiting all data output from the modules. The module will automatically reboot and perform power-up self-tests. Successful completion of the power-up self-tests will return the module to normal operation.

Power-Up Self-Tests

Power-up self-tests are performed when the Aruba 5400R zl2 Switch Series first powers up. There are two instances of power-up self-tests that are performed.

- BootROM instance
- Firmware Instance

BootROM Power-Up Self-Tests

The first instance is performed by the BootROM image. The BootROM, used for the selection of a cryptographic firmware image, performs the following self-tests:

- Known Answer Tests (KATs)
  - SHA-1 KAT
  - SHA-256 KAT
  - SHA-512 KAT
  - RSA Sign and Verify KATs
- BootROM integrity check
- Firmware integrity check (after image has been selected)

The BootROM performs the integrity check on itself to ensure that its image is valid. To perform an integrity check on itself, as well as on images that can be downloaded within, the BootROM first performs a RSA signature verification, and then check the SHA-256 hash of the image. If the BootROM integrity check fails, the switch shall be returned to HPE. If the firmware integrity check fails, the switch will transition to the BootROM console where a new image with a valid signature can be downloaded.

Firmware Power-Up Self-Tests

The power-up self-tests are performed on Aruba 5400R zl2 Switch Series once a FIPS Approved image has been loaded by the BootROM and are performed by that image. The following power up self-tests are performed:

- CTR DRBG KATs (instantiate, generate and reseed).
- SHA1 KAT, SHA256 KAT, SHA512 KAT
- HMAC_SHA1 KAT
- Triple-DES CBC Encrypt and Decrypt KATs
- AES-CBC Encrypt and Decrypt KATs
- DSA-1024 PCT, DSA-2048 PCT*
- RSA-2048 Sign and Verify KATs
- ECDSA PCT*

*These self-tests are for future use.

When there is power up self test failure, the error message indicating as to which crypto algorithm failed in self test will be displayed and the switch will be crashed and the switch should be rebooted.

Example error message with SHA1 power up self test failure is:

"Crypto powerup selftests for SHA1_KAT failed."

Conditional Self-Tests

Conditional self-tests implemented by the switches:

- Continuous RNG Test for DRBG
- Continuous RNG Test for NDRNG
- DSA PCT
- RSA PCT
- Firmware Load Test (BootROM)
- Firmware Load Test (Firmware)

11 Delivery and Operation

Secure Delivery

To ensure no one has tampered with the goods during delivery, inspect the Networking switch physical package and check as follows:

1. Outer Package Inspection

    1) Check that the outer carton is in good condition.
    2) Check the package for a HPE Quality Seal or IPQC Seal, and ensure that it is intact.
    3) Check that the IPQC seal on the plastic bag inside the carton is intact.

4) If any check failed, the goods shall be treated as dead-on-arrival (DOA) goods.

2. Packing List Verification

   Check against the packing list for discrepancy in material type and quantity. If any discrepancy found, the goods shall be treated as DOA goods.

3. External Visual Inspection

   Inspect the cabinet or chassis for any defects, loose connections, damages, and illegible marks. If any surface defect or material shortage found, the goods shall be treated as DOA goods.

4. Confirm Software/firmware

   1) Version verification
      To verify the software version, start the networking device, view the self-test result during startup, and use the **show version** command to check the software version. If software loading failed or the version information is incorrect, please contact HPE for support.

   2) RSA with SHA-256 verification
      To verify that software/firmware has not been tampered, run **verify signature flash <primary/secondary>** on the networking device. The command will return a pass or fail message.

5. DOA (Dead on Arrival)

   If the package is damaged, any label/seal is incorrect or tampered, stop unpacking the goods, retain the package, and report to HPE for further investigation. The damaged goods will be replaced if necessary.

Secure Operation

The Aruba 5400R zl2 Switch Series is capable of two different modes of operation.

- Standard Secure-Mode - non-FIPS Approved mode of operation for the switches
- FIPS Mode - FIPS-Approved mode of operation for the switches

In FIPS Mode, services such as Telnet, TFTP[7], HTTP[8], and SNMPv2 have to be disabled. Auxiliary ports and buttons capable of manual reset and password clearing need to be disabled on the front panel of the modules. Other services in the modules need to be enabled, such as SSHv2, SFTP and SNMPv3. The following initialization steps in this policy must be followed to ensure that the Aruba 5400R zl2 Switch Series is running in a FIPS-Approved mode of operation.

For more information on switch software commands related to Secure Mode, see the chapter titled "Secure Mode (3800, 5400zl, and 8200zl Switches)" in version KB.15.18 or later the Access Security Guide for your switch.

Note: The FIPS set-up instructions here-in are to be executed from the local serial port of the switch.

Note: The examples show an "`Aruba-Switch#`" prompt. Prompts will differ based on the specific switch model number.

Pre-Initialization

Prior to enabling the switch for a FIPS-Approved mode of operation, the Crypto Officer must download the latest FIPS-Approved firmware image from HPE and load it onto the switch. In the following example, the FIPS firmware image is downloaded as the primary flash image using this command structure: `Copy tftp flash <tftp server> <FIPS image>`

```
Aruba-Switch# copy tftp flash 192.168.1.1 KB_16.02.0015.swi
```

Once the image has been downloaded, the Crypto Officer must reboot the switch (still in Standard Secure-Mode) with the newly loaded FIPS-Approved firmware image.

```
Aruba-Switch# boot system flash primary
```

The switch will reboot to the primary flash image. Once presented with the CLI, the Crypto Officer must download the FIPS-Approved image a second time. This is a mandatory measure to ensure that a FIPS-Approved image is being downloaded appropriately. The FIPS firmware image will be downloaded as the primary flash image:

```
Aruba-Switch# copy tftp flash 192.168.1.1 KB_16.02.0015.swi
```

After completing the download, the Crypto Officer will set the configuration file of the switch to its default settings. This will erase custom keys and other custom configuration settings.

```
Aruba-Switch# erase startup-config
```

After the startup configuration file has been set to its default settings, the Crypto Officer will enter the 'configuration' context and reboot the switch into a FIPS-ready mode of operation. This means that

---

FIPS 186-4

[11] FIPS 46-3

only FIPS-Approved algorithms and operations are used. Authentication, CSPs, and other services still need to be set up to bring the switch to a FIPS-Approved mode of operation.

```
Aruba-Switch# configure

Aruba-Switch(config)# secure-mode enhanced
```

Before transitioning to FIPS-mode, the Crypto Officer will be asked to confirm whether or not they would like to zeroize the switch, erasing all Management Card files except for the firmware image. Zeroization is required when bringing the switch out of or into a FIPS-Approved mode of operation. This is required so that private keys and CSPs established in one mode of operation cannot be used in another. Zeroization can take up to an hour to complete.

```
The system will be rebooted and all Management Module files
except software images will be erased and zeroized.  This will
take up to 60 minutes and the switch will not be usable during
that time.  Continue (y/n)?
```

After the Crypto Officer confirms the above message, the switch will reboot directly into the last loaded firmware image (the FIPS firmware image), run cryptographic self-tests, and do complete zeroization of the switch. Once completed, the switch is ready to be configured to run in a FIPS-Approved mode of operation.

```
ATTENTION: Zeroization has started and will take up to 60 minutes.
           Interrupting this process may cause the switch
           to become unstable.


Backing up firmware images and other system files...
Zeroizing the file system...  100%
Verifying cleanness of the file system...  100%
Restoring firmware images and other system files...
Zeroization of the file system completed.
Continue initializing..initialization done.
```

Initialization and Configuration

The steps outlined in this section will require the Cryptographic Officer to enter the 'configuration' context in order to execute the commands necessary for initializing the module.

```
Aruba-Switch# configure
```

The Crypto Officer must create passwords for himself or herself, the User, and for the BootROM console in order to meet the security requirements laid out by FIPS PUB 140-2. All other commands for password management not used in this document are prohibited in the FIPS-Approved mode of operation. A password for the BootROM console is necessary to ensure that only an authorized operator is able to access the BootROM console services. The Crypto Officer shall be the only one with knowledge of the BootROM password.

```
Aruba-Switch(config)# password operator

New password for operator: **********

       Please retype new password for operator: **********


Aruba-Switch(config)# password manager

New password for manager: **********

Please retype new password for manager: **********


Aruba-Switch(config)# password rom-console

       Enter password:  **********

Re-enter password:  **********
```

Following password initialization, the Crypto Officer will disable Telnet services.

```
Aruba-Switch(config)# no telnet-server
```

SSHv2 services will be turned on to allow the User and Crypto Officer to access the switch's CLI services remotely. To do this, the Crypto Officer must first generate a new RSA key pair (2048 or 3072 bits) to be used for secure key and message transportation though the SSHv2 connection.

```
Aruba-Switch (config)# crypto key generate ssh rsa bits 3072

Installing new key pair.  If the key/entropy cache is

depleted, this could take up to a minute.
```

The follow command enables the SSHv2 server:

```
Aruba-Switch (config)# ip ssh
```

SFTP/SCP services must be enabled in order to download new firmware images and security updates from HPE Networking. It may also be necessary to access an SFTP server to save a copy of the

configuration file or device log to an external storage device securely. Enabling SFTP will disable the TFTP service.

```
Aruba-Switch (config)# ip ssh filetransfer

Tftp and auto-tftp have been disabled.
```

As an added security measure, the Crypto Officer will type the following commands to ensure the switch does not have access to the TFTP client and server services:

```
Aruba-Switch (config)# no tftp client

Aruba-Switch (config)# no tftp server
```

In order to disable SNMPv1 and SNMPv2, the Crypto Officer must first initialize SNMPv3. Set-up of SNMPv3 requires that an initial user be created with an associated MD5 authentication hash. After creating the 'initial' user, the Crypto Officer will type in an authentication password and associated privacy password for the 'initial' user:

```
Aruba-Switch (config)# snmpv3 enable

SNMPv3 Initialization process.

Creating user 'initial'

Authentication Protocol: MD5

Enter authentication password: *******

Privacy protocol is DES

Enter privacy password: *******
```

Following the creation of the 'initial' user, the Crypto Officer will be asked if they would like to create a second user that uses SHA-1 for authentication. The Crypto Officer will type 'y' then press the "Enter" or "Return" key in order to create the second user.

```
User 'initial' has been created

Would you like to create a user that uses SHA? [y/n] y



Enter user name: crypto_officer

Authentication Protocol: SHA

Enter authentication password: **************

Privacy protocol is DES

Enter privacy password: **************
```

Once the FIPS-Approved user has been created with their associated authentication and privacy passwords, the Crypto Officer will limit access to SNMPv1 and SNMPv2c messages to 'read only'. This does not disable SNMPv1 and SNMPv2.

```
User creation is done.  SNMPv3 is now functional.

    Would you like to restrict SNMPv1 and SNMPv2c messages to have
    read only access (you can set this later by the command 'snmp
    restrict-access')? [y/n] y
```

The privacy protocol for the SNMPv3 "crypto officer" user must be changed from DES to AES-128. Use the following command to manually change the privacy protocol for the "crypto officer" user. Substitute the "*" with a secure password.

```
Aruba-Switch (config)# snmpv3 user crypto_officer auth sha
****** priv aes ******
```

The following commands will be typed by the Crypto Officer in order to delete the unapproved SNMPv3 user ('initial') and to disable use of SNMPv1 and SNMPv2.

```
Aruba-Switch (config)# no snmpv3 user initial

Aruba-Switch (config)# no snmp-server enable

Aruba-Switch (config)# snmpv3 only
```

Plaintext connections to the switch are not allowed in a FIPS-Approved mode of operation and must be disabled with the following command:

```
Aruba-Switch (config)# no web-management plaintext
```

HTTPS[9] access to the module must be disabled. The Crypto Officer can use the following command to disable SSL[10] v3.1/TLS[11] 1.0 web management services.

```
Aruba-Switch (config)# no web-management ssl
```

To prevent unintentional factory reset of the switch, the "Reset" button located on the Management Card of the Aruba 5400R zl2 series switches must be disabled. The Crypto Officer must confirm the prompt with a 'y' to complete the command.

```
Aruba-Switch (config)# no front-panel-security factory-reset
```

[9] HTTPS – Secure Hypertext Transfer Protocol

[10] SSL – Secure Socket Layer

[11] TLS – Transport Layer Security

```
                    **** CAUTION ****

        Disabling the factory reset option prevents switch configuration
        and passwords from being easily reset or recovered.  Ensure that
        you are familiar with the front panel security options before
        proceeding.


    Continue with disabling the factory reset option[y/n]? y
```

To prevent unintentional password reset of the switch, the “Clear” button located on the Management Card of the Aruba 5400R zl2 series switches must be disabled. The Crypto Officer must confirm the prompt with a ‘y’ to complete the command.

```
Aruba-Switch (config)# no front-panel-security password-clear

                        **** CAUTION ****

    Disabling the clear button prevents switch passwords from being
    easily reset or recovered.  Ensure that you are familiar with
    the front panel security options before proceeding.


Continue with disabling the clear button [y/n]? y
```

The auxiliary port located on the Management Card must be disabled avoid any unauthorized modifications to the module and its operational environment. Please note: The autorun feature will not function when the USB port is disabled.

```
Aruba-Switch (config)# no usb-port
```

The start-up configuration file needs to be written with the new settings that have been applied in this section. The following command will write the new start-up configuration file:

```
Aruba-Switch (config)# write memory
```

The last steps to ensure that the switch is running in a FIPS-Approved mode of operation is to set the default boot image to the primary image and then reboot the switch into the newly configured FIPS-Approved firmware image.

```
Aruba-Switch (config)# boot set default primary

Aruba-Switch (config)# boot system flash primary
```

Use the following command to confirm the switch is running in a FIPS-Approved mode of operation:

```
Aruba-Switch (config)# show secure-mode

Secure-mode     : Enabled
```

Zeroization

Zeroization is required when bringing the switch out of or into a FIPS-Approved mode of operation. This is required so that private keys and CSPs established in one mode of operation cannot be used in another. The Aruba 5400R zl2 series switches will execute full system zeroization when the switch is changing secure-mode states. For example, this can be done by calling `secure-mode enhanced` while the switch is in a "secure-mode standard" state. The module will not execute zeroization if calling `secure-mode enhanced` while the switch is currently in the "secure-mode enhanced" state.

Zeroization can also be done by executing the `erase all zeroize` command. This command has the same effect as the above commands; however the switch will not transition to the opposite mode from which the command was called in. The `secure-mode` commands shall only be called when accessing the switch directly through a serial connection. Otherwise status information about the zeroization process will not be displayed nor will the operator be able to access the module remotely until remote access has been set up. The only things that will remain on the switch after zeroization has completed are the BootROM image and the firmware images.

Secure Management

Once the Aruba 5400R zl2 series switches have been configured for a FIPS-Approved mode of operation, the Crypto Officer will be responsible for keeping track of and regenerating RSA key pairs for SSHv2 authentication to the switches. Remote management is available via SSHv2. The Crypto Officer is the only operator that can change configuration settings of the switch, which includes access control, password management, and port security. Physical access to and local control of the Aruba 5400R zl2 series switches shall be limited to the Cryptographic Officer.

User Guidance

The user is only able to access the Aruba 5400R zl2 series switches remotely via SSHv2. When accessing the switches remotely via SSHv2, the User will be presented with the same CLI interface as if connected locally. In an SSHv2 session, the user is able to see most of the health information and configuration settings of the switches, but is unable to change them.

BootROM Guidance

The primary purpose of the BootROM console is to download a new firmware image should there be a problem booting the current FIPS-Approved image. The BootROM may be accessed when rebooting the Aruba 5400R zl2 series switches locally through the serial port. When entering into the BootROM, the BootROM selection menu will present the Crypto Officer with three options. Option *0* allows the Crypto Officer to access BootROM console services. Option *1* and Option *2* allow the Crypto Officer to boot the system into either the primary or secondary firmware image, respectively. Only a FIPS approved firmware image may be selected from the menu. If nothing is pressed within 3 seconds of being presented with the selection menu, the switch will boot into the last booted image.

When accessing the BootROM console from the BootROM selection menu, the Crypto Officer will be prompted for the BootROM password which was previously configured by the Crypto Officer during switch initialization. This password shall be different than the Crypto Officer password. A limited set of commands is available to the Crypto Officer within the BootROM console that allows the Crypto Officer to download a new image, reboot the switch, zeroize the switch, or display BootROM image versioning information. The BootROM console may be exited at any time, to access the image selection menu, via the `quit` command.

12 Mitigation of Other Attacks

The networking devices do not claim to mitigate any attacks in a FIPS approved mode of operation.

13 Documentation References

Obtaining documentation

You can access the HPE Networking products page: https://www.hpe.com/us/en/networking.html#.UcMNEpzzlX0, where you can obtain the up-to-date documents of HPE Switches, such as datasheet, installation manual, configuration guide, command reference, and other reference documents.

Technical support

For technical or sales related question please refer to the contacts list on the HPE website: http://www.hpe.com.