Aruba 620, 650 and Dell W-620, W-650

Controllers with ArubaOS FIPS Firmware Non-Proprietary Security Policy FIPS 140-2 Level 2 Release Supplement

Version 2.4

December 2013

Contents

Preface

This security policy document can be copied and distributed freely.

Purpose of this Document

This release supplement provides information regarding the Aruba 620 and 650 Mobility Controllers and Dell W-620 and W-650 controllers with FIPS 140-2 Level 2 validation from Aruba Networks. The material in this supplement modifies the general Aruba hardware and firmware documentation included with this product and should be kept with your Aruba product documentation.

This supplement primarily covers the non-proprietary Cryptographic Module Security Policy for the Aruba Mobility Controller. This security policy describes how the switch meets the security requirements of FIPS 140-2 Level 2 and how to place and maintain the switch in a secure FIPS 140-2 mode. This policy was prepared as part of the FIPS 140-2 Level 2 validation of the product.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules) details the U.S. 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) Web-site at:

http://csrc.nist.gov/groups/STM/cmvp/index.html

Aruba Dell Relationship
Aruba Networks is the OEM for the Dell PowerConnect W line of products. Dell products are identical to the Aruba products other than branding and Dell software is identical to Aruba software other than branding.

The contents of this document will use the Aruba 620 and 650 as examples and all corresponding Dell models follow the same rules.

Table 1: Aruba and Dell Part Numbers

Aruba Part Number	Aruba Firmware	Dell Part Number	Dell Firmware
620-F1	ArubaOS_6xx_6.1.2.3-FIPS, ArubaOS_6xx_6.1.4.1-FIPS, ArubaOS_6xx_6.1.4.5-FIPS, ArubaOS_6xx_6.1.4.7-FIPS	W-620-F1	DELL_PCW_6xx_6.1.2.3-FIPS, DELL_PCW_6xx_6.1.4.1-FIPS, DELL_PCW_6xx_6.1.4.5-FIPS, DELL_PCW_6xx_6.1.4.7-FIPS
620-USF1	ArubaOS_6xx_6.1.2.3-FIPS, ArubaOS_6xx_6.1.4.1-FIPS, ArubaOS_6xx_6.1.4.5-FIPS, ArubaOS_6xx_6.1.4.7-FIPS	W-620-USF1	DELL_PCW_6xx_6.1.2.3-FIPS, DELL_PCW_6xx_6.1.4.1-FIPS, DELL_PCW_6xx_6.1.4.5-FIPS, DELL_PCW_6xx_6.1.4.7-FIPS
650-F1	ArubaOS_6xx_6.1.2.3-FIPS,	W-650-F1	DELL_PCW_6xx_6.1.2.3-FIPS,

	ArubaOS_6xx_6.1.4.1-FIPS, ArubaOS_6xx_6.1.4.5-FIPS, ArubaOS_6xx_6.1.4.7-FIPS		DELL_PCW_6xx_6.1.4.1-FIPS, DELL_PCW_6xx_6.1.4.5-FIPS, DELL_PCW_6xx_6.1.4.7-FIPS
650-USF1	ArubaOS_6xx_6.1.2.3-FIPS, ArubaOS_6xx_6.1.4.1-FIPS, ArubaOS_6xx_6.1.4.5-FIPS, ArubaOS_6xx_6.1.4.7-FIPS	W-650-USF1	DELL_PCW_6xx_6.1.2.3-FIPS, DELL_PCW_6xx_6.1.4.1-FIPS, DELL_PCW_6xx_6.1.4.5-FIPS, DELL_PCW_6xx_6.1.4.7-FIPS

NOTE — References to Aruba, ArubaOS and Aruba 600 series apply to both the Aruba and Dell versions of these products and documentation.

NOTE — Products ending with -USF1 are to be sold in the US only. Products ending with -F1 are considered 'rest of the world' and must not be used for deployment in the United States. From FIPS perspective, both -USF1 and -F1 models are identical and fully FIPS compliant.

Related Documents

Product Manuals

The following items are part of the complete installation and operations documentation included with this product:

- Aruba 620 and 650 Mobility Controllers with ArubaOS FIPS Firmware Non-Proprietary Security Policy (this document)
- *Aruba 620 Mobility Controller Installation Guide*
- *Aruba 650 Mobility Controller Installation Guide*
- *ArubaOS 6.1 User Guide*
- *ArubaOS 6.1 CLI Reference Guide*
- *ArubaOS 6.1 Quick Start Guide*
- *ArubaOS 6.1 Upgrade Guide*
- Aruba AP Installation Guides

Additional Product Information

More information is available from the following sources:

- The Aruba Networks Web-site contains information on the full line of products from Aruba Networks:

  http://www.arubanetworks.com

- The Dell Web site contains information on the full line of products from Dell.

  http://www.dell.com/

- The NIST Validated Modules Web-site contains contact information for answers to technical or sales-related questions for the product:

  http://csrc.nist.gov/groups/STM/cmvp/index.html

The Aruba 620 and 650 Mobility Controllers

This chapter introduces the Aruba 620 and 650 Mobility Controllers with FIPS 140-2 Level 2 validation. It describes the purpose of the controller, its physical attributes, and its interfaces.

Overview

Aruba Networks has developed a purpose-built Wireless LAN voice and data switching solution designed to specifically address the needs of large-scale WiFi network deployments for Government agencies and global enterprises. The Aruba Mobility Controller solution provides advanced security and management of the corporate RF environment and enforces User security and service policies to both wired and wireless users.

The Aruba Wireless FIPS 140-2 Level 2 validated Mobility Controlling platform serves value-add high speed data and QoS assured voice services to thousands of mobile wireless users simultaneously from a single, cost effective, redundant and scalable solution that performs centralized functionality for:

- Uncompromised User security, authentication and encryption
- Stateful LAN-speed firewalling
- VPN termination
- Wireless intrusion detection, prevention and rogue containment
- RF Air monitoring
- Powerful packet processing switching
- Mobility management
- Advanced RF management

Advanced User and network service / element management

The Aruba FIPS 140-2 Level 2 validated Mobility Controller solution is a highly available, modular and upgradeable switching platform which connects, controls, secures, and intelligently integrates wireless Access Points and Air Monitors into the wired LAN, serving as a gateway between a wireless network and the wired network. The wireless network traffic from the APs is securely tunneled over a L2/L3 network and is terminated centrally on the switch via 10/100/1000 Ethernet physical interfaces where it is authenticated, assigned the appropriate security policies and VLAN assignments and up-linked onto the wired network.

The Aruba Mobility Controller solution consists of the three major components:

- Aruba Mobility Controller. This is an enterprise-class switch into which multiple Access Points (APs) and Air Monitors (AMs) may be directly or in-directly (tunneled over a L2/L3 network) connected and controlled.
- Aruba Wireless Access Point. This is a next-generation wireless transceiver which functions as an AP or AM. Although third-party APs can be used with the Aruba WLAN system, the Aruba AP provides the most comprehensive features and simpler integration.
- Aruba's ArubaOS Switch firmware. This firmware intelligently integrates the Mobility Controller and APs to provide load balancing, rate limiting, self-healing, authentication, mobility, security, firewalls, encryption, and centralization for monitoring and upgrades.

The switch configurations tested during the cryptographic module testing included:

- Aruba 620 (620-USF1)
- Dell W-620 (W-620-USF1)
- Aruba 650 (650-USF1)
- Dell W-650 (W-650-USF1)
- The exact firmware versions tested were:
    - ArubaOS_6xx_6.1.2.3-FIPS, ArubaOS_6xx_6.1.4.1-FIPS, ArubaOS_6xx_6.1.4.5-FIPS, ArubaOS_6xx_6.1.4.7-FIPS
    - DELL_PCW_6xx_6.1.2.3-FIPS, DELL_PCW_6xx_6.1.4.1-FIPS, DELL_PCW_6xx_6.1.4.5-FIPS, DELL_PCW_6xx_6.1.4.7-FIPS

Physical Description

See Aruba 620 Chassis or Aruba 650 Chassisfor a list of what ships with this product.

Dimensions

The Aruba 620 Mobility Controller has the following physical dimensions:

- Size:
    - Width 12.6" (320 mm)
    - Height 1.75" (45 mm)
    - Depth 6.8" (173 mm)
- Weight: 2.7 lbs/1.23 kgs

The 620 Rack Mounting Kit provides the means to install a 620 controller in a standard 19-inch rack.

The Aruba 650 Mobility Controller has the following physical dimensions:

- Size:
    - Width 13.6" (346 mm)
    - Height 1.5" (38 mm)
    - Depth 8.9" (226 mm)
- Weight: 4.9 lbs/2.2 kgs

The Aruba 650 Mobility Controller is rack mountable in a standard 19-inch rack.

Cryptographic Module Boundaries

For FIPS 140-2 Level 2 validation, the Mobility Controller has been validated as a multi-chip standalone cryptographic module. The chassis physically encloses the complete set of hardware and firmware components and represents the cryptographic boundary of the switch. The cryptographic boundary is defined as encompassing the top, front, left, right, rear, and bottom surfaces of the case.

Aruba 620 Chassis

The Aruba 620 Mobility Controller chassis is designed to be 1U not-modular. The following diagrams (Aruba and

Aruba) show the front and rear view of the chassis respectively. The Aruba 620 Mobility Controller chassis contains:

- 1x Console (RS-232) RJ-45 port
- 4xFast Ethernet (10/100BASE-T) port
- 4x Fast Ethernet (10/100BASE-T) with PoE+ port
- 1x Gigabit Ethernet (1000BASE-T) port
- 1x ExpressCard® port
- 1x USB 2.0 port
- 1x AC input voltage 100-240 V, Universal Input

Figure 1 *Aruba 620 Mobility Controller Front View*

ExpressCard Slot

Port LEDs
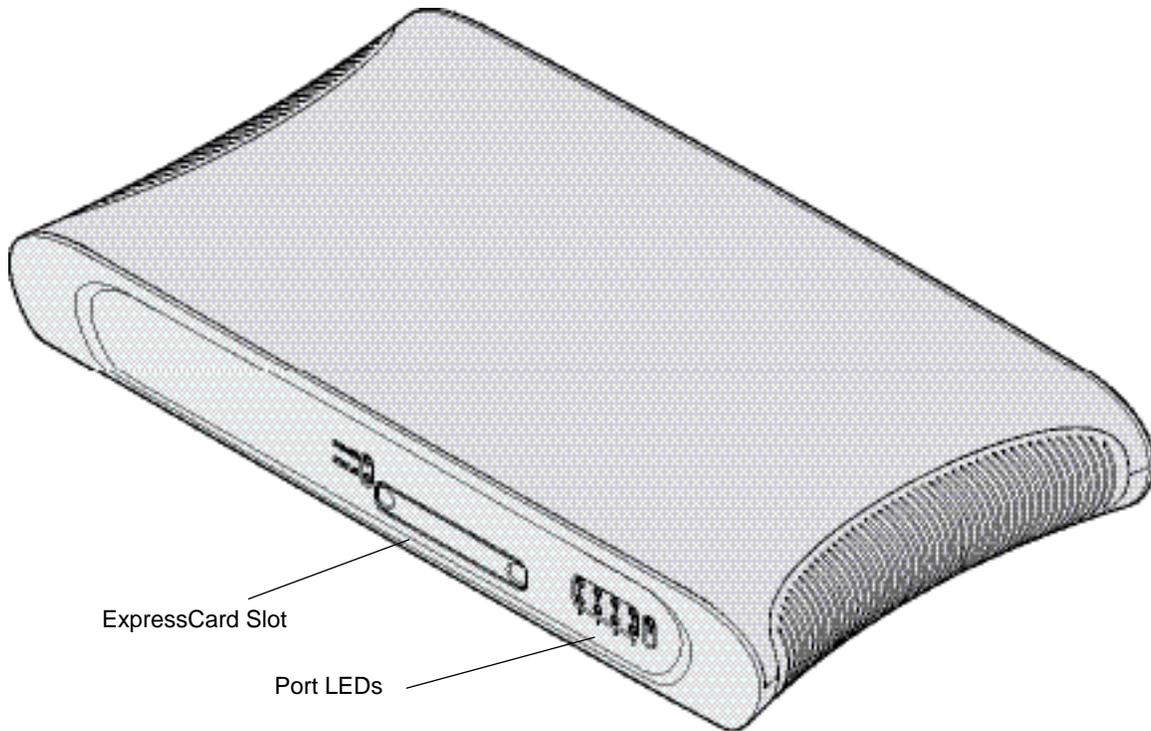
Figure 2 *Aruba 620 Mobility Controller Rear View*

Serial Console Port

10/100Base-T
Ethernet Ports

10/100/1000Base-T
Gigabit Ethernet Port

Media Eject Button

USB port

AC Power Socket
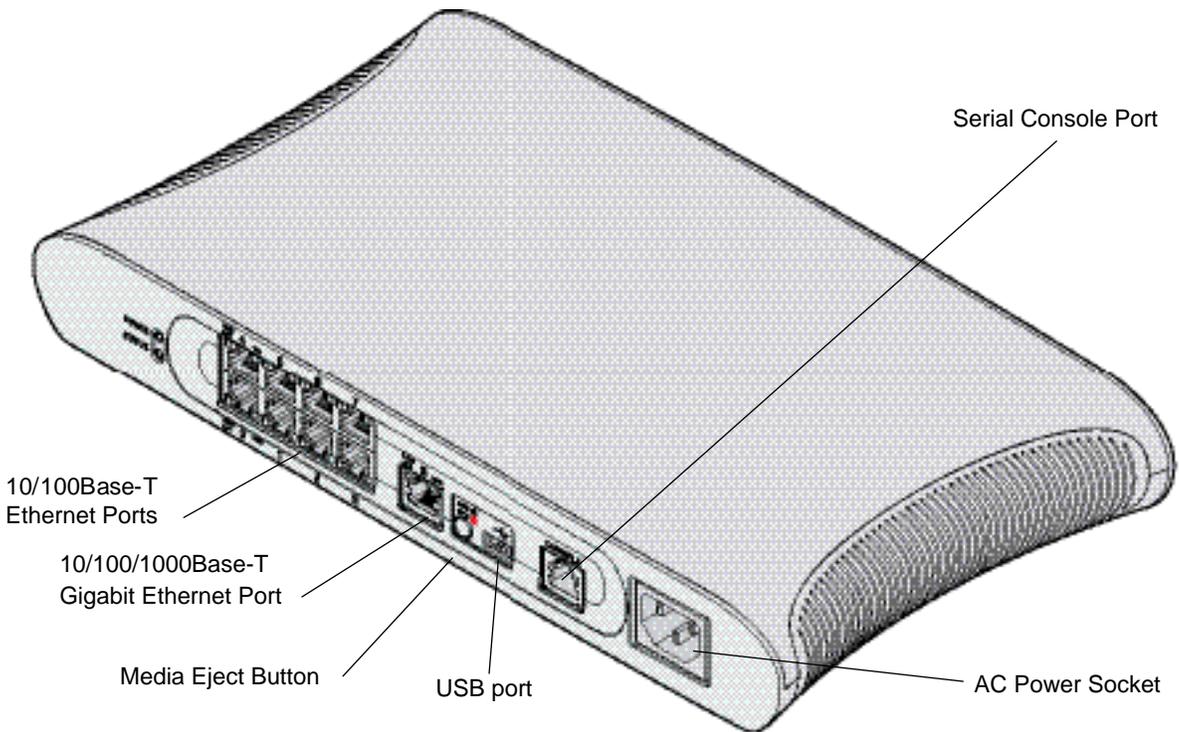
The Aruba 620 is equipped with a media eject button, which allows users to eject storage devices safely and place the system in standby. Pushing the media eject button changes the state of the Aruba 620; the table below describes the states and LED behaviors associated with use of the media eject button:

Table 2: Media Eject Button LED Behavior

Initial State	LED State	Action	Status LED	Function	LED Action Completed
NAS Media Operational	Green-solid	Press and hold media eject button for 1 to 5 seconds only	Amber-flashing	Un-mount all NAS media	Amber-solid
NAS Media Unmounted	Amber-solid	Press and hold media eject button for 1 to 5 seconds only	Amber-flashing	Mount all attached NAS devices, and return to fully functional operation	Green-solid
Operational	Green-solid	Press and hold media eject button for more than 5 seconds only	Red-flashing	Controller goes into Standby	Red-solid
Operating with NAS Media un-mounted	Amber-solid	Press and hold media eject button for more than 5 seconds only	Red-flashing	Controller goes into Standby	Red-solid
Standby	Red-solid	Press media eject button	Amber-flashing	Controller wake-up	Green-solid

In non-rack deployments, the Aruba 620 is placed with the front facing out. This allows the cables to be hidden and creates a more aesthetically pleasing look. Therefore, a set of LEDs displaying link activity on the ports is placed on the front side. Same LEDs also exist in back side too. For information about the behavior of these LEDs, see table below.

Table 3: Aruba 620 LED Status Indicators

LED	Label	Function	Indicator	Status
Power	POWER	Input Power Status Indicator	On (Solid Green)	Power on
			Off	No Power

Status	STATUS	Module Status Indicator	On (Solid Green)	Device is operational
			On (Solid Red)	Device failed or is in Standby
			On (Solid Amber)	Device is loading software
			Off	No power
10/100/1000Base-T Port	LNK/ACT	Link/Activity Status Indicator	On (Solid Green)	Link has been established
			On (Flashing Green)	Port is transmitting or receiving data
			Off	No link on port
	1000	Interface Speed	On (Solid Green)	1000 Mbps
			Off	10/100 Mbps
10/100Base-T Ports	LINK/ACT	Link/Activity Status Indicator	On (Solid Green)	Link has been established
			On (Flashing Green)	Port is transmitting or receiving data
			Off	No link on port
	PoE	PoE Status Indicator	On (Solid Green)	PoE is being provided
			On (Solid Amber)	The attached device has requested PoE, but PoE is not being provided by the port
			Off	PoE is not being provided
	100	Interface Speed	On (Solid Green)	100 Mbps
			Off	10 Mbps

Aruba 650 Chassis

The Aruba 650 Mobility Controller chassis is also 1U not-modular. The following diagrams (Aruba and

Aruba) show the front and rear view of the chassis respectively. The Aruba 650 Mobility Controller chassis contains:

- 1x Console (RS-232) RJ-45 port
- 2x Gigabit Ethernet (10/100/1000Base-T)
- 4x Gigabit Ethernet (10/100/1000Base-T) with PoE+
- 2x Gigabit Ethernet pluggable (1000Base-X SFP)
- 1x ExpressCard® port
- 4x USB 2.0 port
- 1x AC input voltage 100-240 V, Universal Input

Figure 3 *Aruba 650 Mobility Controller Front View*

10/100/1000Base-T
Gigabit Ethernet Ports

USB ports

Serial Console Port

Media Eject Button

10/100/1000Base-T Gigabit
Ethernet Ports with PoE

1000Base-X (SFP) Ports
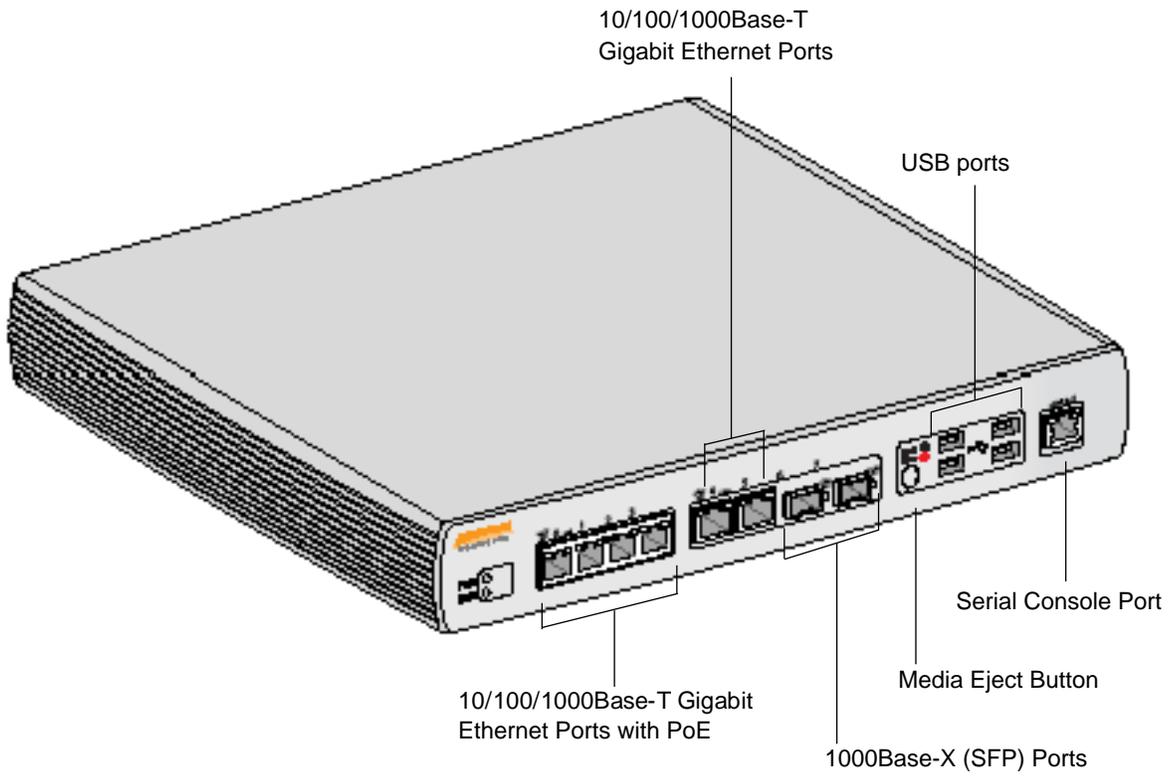
Figure 4 *Aruba 650 Mobility Controller Rear View*

Antennae Interfaces
(651 Only)

ExpressCard Slot

AC Power Socket
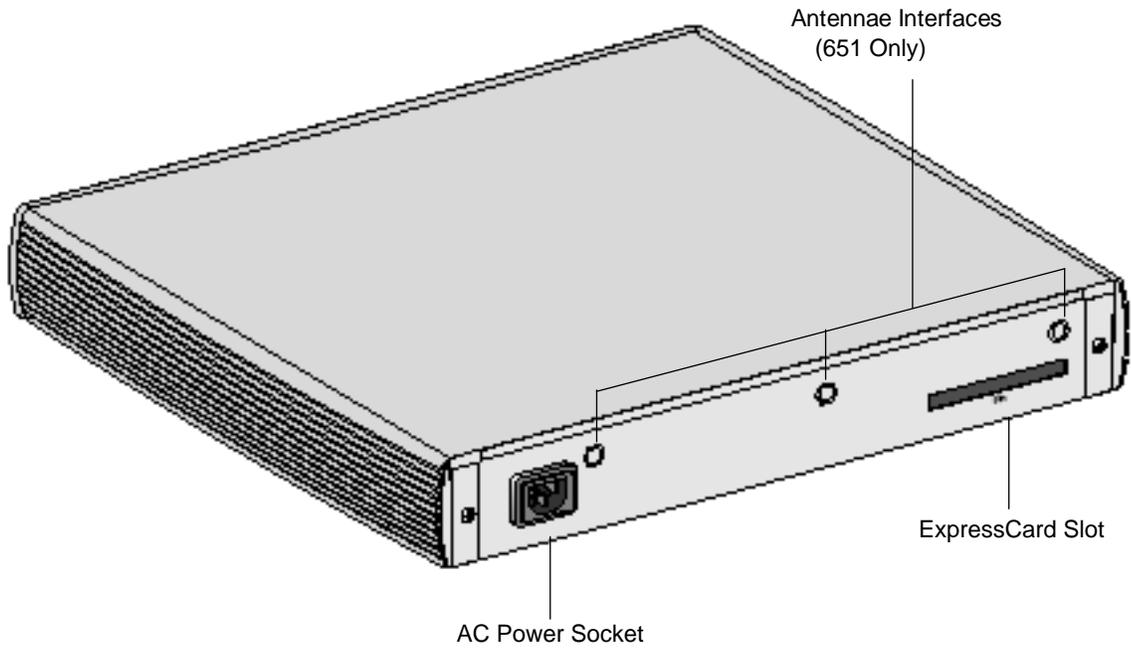
The Aruba 650 Series is equipped with a media eject button, which allows users to eject storage devices safely and place the system in standby. Pushing the media eject button changes the state of the Aruba 650 Series; the table below describes the states and LED behaviors associated with use of the media eject button.

Table 4: Media Eject Button LED Behavior

Initial State	LED State	Action	Status LED	Function	LED Action Completed
NAS Media Operational	Green-solid	Press and hold media eject button for 1 to 5 seconds only	Amber-flashing	Un-mount all NAS media	Amber-solid
NAS Media Unmounted	Amber-solid	Press and hold media eject button for 1 to 5 seconds only	Amber-flashing	Mount all attached NAS devices, and return to fully functional operation	Green-solid
Operational	Green-solid	Press and hold media eject button for more than 5 seconds only	Red-flashing	Controller goes into Standby	Red-solid
Operating with NAS Media un-mounted	Amber-solid	Press and hold media eject button for more than 5 seconds only	Red-flashing	Controller goes into Standby	Red-solid
Standby	Red-solid	Press media eject button	Amber-flashing	Controller wake-up	Green-solid

The behavior of the Power, Status and port LEDs is described in the table below:

Table 5: Aruba 650 Series LED Status Indicators

LED	Label	Function	Indicator	Status
Power	POWER	Input Power Status Indicator	On (Solid Green)	Power on
			Off	No Power
Status	STATUS	Module Status Indicator	On (Solid Green)	Device is operational

			On (Solid Red)	Device failed or is in Standby
			On (Solid Amber)	Device is loading software
			Off	No power
1000Base-X Ports (SFP)	LNK/ACT	Link Status Indicator	On (Solid Green)	Link has been established
			On (Flashing Green)	Port is transmitting or receiving data
			Off	No link on port
10/100/1000Base-T Ports	LNK/ACT	Link/Activity Status Indicator	On (Solid Green)	Link has been established
			On (Flashing Green)	Port is transmitting or receiving data
			Off	No link on port
	1000	Interface Speed	On (Solid Green)	1000 Mbps
			Off	10/100 Mbps
10/100/1000Base-T Ports with PoE	LINK/ACT	Link/Activity Status Indicator	On (Solid Green)	Link has been established
			On (Flashing Green)	Port is transmitting or receiving data
			Off	No link on port
	PoE	PoE Status Indicator	On (Solid Green)	PoE is being provided
			On (Solid Amber)	The attached device has requested PoE, but PoE is not being provided by the port
			Off	PoE is not being provided

FIPS 140-2 Level 2 Features

Intended Level of Security

The Aruba 620 and 650 Mobility Controllers and associated modules are intended to meet overall FIPS 140-2 Level 2 requirements as shown in Table 2-1.

Table 6: Intended Level of Security

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-tests	2

10	Design Assurance	2
11	Mitigation of Other Attacks	2

Physical Security

The Aruba Mobility Controller is a scalable, multi-processor standalone network device and is enclosed in a robust steel housing. The switch enclosure is resistant to probing and is opaque within the visible spectrum. The enclosure of the switch has been designed to satisfy FIPS 140-2 Level 2 physical security requirements.

To protect the Aruba 620 and 650 Mobility Controllers from any tampering with the product, TELs should be applied by the Crypto Officer as covered under "Tamper-Evident Labels" on page 32.

Operational Environment

The operational environment is non-modifiable. The control plane Operating System (OS) is Linux, a real-time, multi-threaded operating system that supports memory protection between processes. Access to the underlying Linux implementation is not provided directly. Only Aruba Networks provided interfaces are used, and the CLI is a restricted command set.

Logical Interfaces

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in the following table.

Table 7: FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interfaces	Module Physical Interface
Data Input Interface	10/100 Mbps Ethernet Port
	10/100/1000 Mbps Ethernet Port
	Express Card slot (disabled)
	USB 2.0 ports
Data Output Interface	10/100 Mbps Ethernet Port
	10/100/1000 Mbps Ethernet Port

	Express Card slot (disabled)
	USB 2.0 ports
Control Input Interface	10/100 Mbps Ethernet Port
	10/100/1000 Mbps Ethernet Port
	Express Card slot (disabled)
	Media Eject Button
	Serial Console port (disabled)
Status Output Interface	10/100 Mbps Ethernet port
	10/100/1000 Mbps Ethernet ports
	LEDs
	Serial Console port (disabled)
Power Interface	Power Supply
	PoE

Data input and output, control input, status output, and power interfaces are defined as follows:

- Data input and output are the packets that use the firewall, VPN, and routing functionality of the modules.
- Control input consists of manual control inputs for media eject. It also consists of all of the data that is entered into the switch while using the management interfaces.
- Status output consists of the status indicators displayed through the LEDs, the status data that is output from the switch while using the management interfaces, and the log file.
- LEDs indicate the physical state of the module, such as power-up (or rebooting), utilization level, activation state (including fan, ports, and power) and status of connected media. The log file records the results of self-tests, configuration errors, and monitoring data.

- A power supply is used to connect the electric power cable. Operating power is also provided to a compatible Power Over Ethernet (POE) device when connected. The power is provided through the connected Ethernet cable.

The switch distinguishes between different forms of data, control, and status traffic over the network ports by analyzing the packets header information and contents.

Roles and Services

The Aruba Mobility Controller supports role-based authentication. There are two roles in the switch (as required by FIPS 140-2 Level 2) that operators may assume: a Crypto Officer role and a User role. The Administrator maps to the Crypto-Officer role and the client Users map to the User role.

Crypto Officer Role

The Crypto Officer role has the ability to configure, manage, and monitor the switch. Three management interfaces can be used for this purpose:

- CLI

  The Crypto Officer can use the CLI to perform non-security-sensitive and security-sensitive monitoring and configuration. The CLI can be accessed remotely by using the SSHv2 secured management session over the Ethernet ports or locally over the serial port. In FIPS mode, the serial port is disabled.

- Web Interface

  The Crypto Officer can use the Web Interface as an alternative to the CLI. The Web Interface provides a highly intuitive, graphical interface for a comprehensive set of switch management tools. The Web Interface can be accessed from a TLS-enabled Web browser using HTTPS (HTTP with Secure Socket Layer) on logical port 4343.

- Bootrom Monitor Mode

  In Bootrom monitor mode, the Crypto Officer can reboot, update the Bootrom, issue file system-related commands, modify network parameters, and issue various show commands. The Crypto Officer can only enter this mode by pressing any key during the first four seconds of initialization. Bootrom Monitor Mode is disabled in FIPS mode.

The Crypto Officer can also use SNMPv1/2c/3 to remotely perform non-security-sensitive monitoring and use get and getnext commands. See the table below for descriptions of the services available to the Crypto Officer role.

Table 8: Crypto-Officer Services

Service	Description	Input	Output	CSP Access
SSH v 2.0	Provide authenticated and encrypted remote management sessions while using the CLI	SSH key agreement parameters, SSH inputs, and data	SSH outputs and data	Diffie-Hellman key pair (read/ write access), session key for SSH (read/write access), RNG keys (read access); Crypto Officer's password (read access)

IKEv1/IKEv2-IPSec	Provide authenticated and encrypted remote management sessions to access the CLI functionality	IKEv1/IKEv2 inputs and data; IPSec inputs, commands, and data	IKEv1/IKEv2 outputs, status, and data; IPSec outputs, status, and data	RSA or ECDSA key pair for IKEv1/IKEv2 (read access), Diffie-Hellman or Elliptic curve Diffie-Hellman key pair for IKEv1/IKEv2 (read/write access), pre- shared keys for IKEv1/IKEv2 (read access); Session keys for IPSec (read/write access)
Configuring Network Management	Create management Users and set their password and privilege level; configure the SNMP agent	Commands and configuration data	Status of commands and configuration data	Crypto Officer's password for CLI (read/write access)
Configuring the module Platform	Define the platform subsystem firmware of the module by entering Bootrom Monitor Mode, File System, fault report, message logging, and other platform related commands	Commands and configuration data	Status of commands and configuration data	None
Configuring Hardware Controllers	Define synchronization features for module	Commands and configuration data	Status of commands and configuration data	None
Configuring the Internet Protocol	Set IP functionality	Commands and configuration data	Status of commands and configuration data	None
Configuring Quality of Service (QoS)	Configure QOS values for module	Commands and configuration data	Status of commands and configuration data	None
Configuring the VPN	Configure Public Key Infrastructure (PKI); configure the Internet Key Exchange (IKEv1/IKEv2) Security Protocol; configure the IPSec protocol	Commands and configuration data	Status of commands and configuration data	RSA and ECDSA keys pair (read/write access), Pre-shared key (read/write access)
Configuring DHCP	Configure DHCP on module	Commands and configuration data	Status of commands and configuration data	None
Configuring Security	Define security features for module, including Access List, AAA, and firewall functionality	Commands and configuration data	Status of commands and configuration data	AAA User password (read/write access), RADIUS password (read/ write access)

HTTPS over TLS	Secure browser connection over Transport Layer Security acting as a Crypto Officer service (web management interface)	TLS inputs, commands, and data	TLS outputs, status, and data	RSA key pair for TLS; TLS Session Key
IPSec tunnel establishment for RADIUS protection	Provided authenticated/encrypted channel to RADIUS server	IKEv1/IKEv2 inputs and data; IPSec inputs, commands, and data	IKEv1/IKEv2 outputs, status, and data; IPSec outputs, status, and data	Preshared key/RSA private key for IKEv1/IKEv2 (read access), Diffie-Hellman and Elliptic curve Diffie-Hellman key pair for IKEv1/IKEv2 (read/write access), Session keys for IPSec (read/write access)
Self-test	Run Power On Self-Tests and Conditional Tests	None	Error messages logged if a failure occurs	None
Configuring Bypass Operation	Configure bypass operation on the module	Commands and configuration data	Status of commands and configuration data	None
Updating Firmware	Updating firmware on the module	Commands and configuration data	Status of commands and configuration data	None
Configuring OCSP Responder	Configuring OCSP responder functionality	OCSP inputs, commands, and data	OCSP outputs, status, and data	RSA/ECDSA key pair for signing OCSP responses
Configuring Control Plane Security (CPSec)	Configuring Control Plane Security mode to protect communication with APs using IPSec and issue self signed certificates to APs	Commands and configuration data, IKEv1/IKEv2 inputs and data; IPSec inputs, commands, and data	Status of commands, IKEv1/IKEv2 outputs, status, and data; IPSec outputs, status, and data and configuration data, self signed certificates	RSA private key for IKEv1/IKEv2 and certificate signing (read access), Diffie-Hellman key pair for IKEv1/IKEv2 (read/write access), Session keys for IPSec (read/write access)
Status	Cryptographic officer may use CLI "show" commands or view WebUI via TLS to the view the switch configuration, routing tables, and active sessions; view health, temperature, memory status, voltage and packet statistics, review account logs, and view physical interface status.	Commands and configuration data	Status of commands and configuration	None

User Role

The User role can access the switch's IPSec and IKEv1/IKEv2 services. Service descriptions and inputs/outputs are listed in the following table:

Table 9: User Service

Service	Description	Input	Output	CSP Access
IKEv1/IKEv2-IPSec	Access the module's IPSec services in order to secure network traffic	IPSec inputs, commands, and data	IPSec outputs, status, and data	RSA and ECDSA key pair for IKEv1/IKEv2 (read access); Diffie-Hellman and Elliptic curve Diffie-Hellman key pair for IKEv1/IKEv2 (read and write access); pre-shared keys for IKEv1/IKEv2 (read access)
HTTPS over TLS	Access the module's TLS services in order to secure network traffic	TLS inputs, commands, and data	TLS outputs, status, and data	RSA key pair for TLS; TLS Session Key
EAP-TLS termination	Provide EAP-TLS termination	EAP-TLS inputs, commands and data	EAP-TLS outputs, status and data	EAP-TLS RSA private key (read) EAP-TLS ECDSA private key (read)
802.11i Shared Key Mode	Access the module's 802.11i services in order to secure network traffic	802.11i inputs, commands and data	802.11i outputs, status and data	802.11i Pre-Shared Key (read) 802.11i Session key (read/write)
802.11i with EAP-TLS	Access the module's 802.11i services in order to secure network traffic	802.11i inputs, commands and data	802.11i outputs, status, and data	EAP-TLS RSA private key (read) EAP-TLS ECDSA private key (read) 802.11i Pair-Wise Master Key (read/write) 802.11i Session key (read/write)
Data link (Layer 2) Encryption	Access the module's Layer 2 encrypted tunnel services to secure network traffic Data link encryption inputs, commands and data	Data link encryption inputs, commands and data	Data link encryption, status, and data	Data link encryption AES key (read)

Authentication Mechanisms

The Aruba Mobility Controller supports role-based authentication. Role-based authentication is performed before the Crypto Officer enters privileged mode using admin password via Web Interface or SSH or by entering enable command and password in console. Role-based authentication is also performed for User authentication.

This includes password and RSA/ECDSA-based authentication mechanisms. The strength of each authentication mechanism is described below.

Table 10: Estimated Strength of Authentication Mechanisms

Authentication Type	Role	Strength
Password-based authentication (CLI and Web Interface)	Crypto Officer	Passwords are required to be at least six characters long. Numeric, alphabetic (upper and lowercase), and keyboard and extended characters can be used, which gives a total of 95 characters to choose from. Therefore, the number of potential six-character passwords is 95^6 (735091890625).
RSA-based authentication (IKEv1/IKEv2)	User	RSA signing and verification is used to authenticate to the module during IKEv1/IKEv2. This mechanism is as strong as the RSA algorithm using a 1024 or 2048 bit key pair.
Pre-shared key-based authentication (IKEv1/IKEv2)	User	Pre-shared keys must be at least six characters long and up to 64 bytes long. Even if only uppercase letters were used without repetition for a six character pre-shared key, the probability of randomly guessing the correct sequence is one in 165,765,600.
Pre-shared key based authentication (802.11i)	User	1024 and 2048 bit RSA keys correspond to effective strength of 2^{80} and 2^{112} respectively.
EAP-TLS authentication	User	1024 and 2048 bit RSA keys correspond to effective strength of 2^{80} and 2^{112} respectively.
ECDSA-based authentication (IKEv1/IKEv2)	User	ECDSA signing and verification is used to authenticate to the module during IKEv1/IKEv2. Both P-256 and P-384 keys are supported. ECDSA P-256 provides 128 bits of equivalent security, and P-384 provides 192 bits of equivalent security.

Unauthenticated Services

The Aruba Mobility Controller can perform SNMP management, VLAN, bridging, firewall, routing, and forwarding functionality without authentication. These services do not involve any cryptographic processing.

Additional unauthenticated services include performance of the power-on self-test and system status indication via LEDs.

Cryptographic Key Management

Implemented Algorithms

FIPS-approved cryptographic algorithms have been implemented in hardware and firmware.

Hardware encryption acceleration is provided for bulk cryptographic operations for the following FIPS approved algorithms:

- AES (Cert. #779#649, #650, #651)
- Triple-DES (Cert. #673#600, #601 #602)
- SHS (Cert. #781#682, #683, #684)
- HMAC (Cert. #426)

The firmware supports the following cryptographic implemetations.

ArubaOS OpenSSL Module implements the following FIPS-approved algorithms:

- AES (Cert. #1854)
- Triple-DES (Cert. #1201)
- SHS (Cert. #1631)
- RNG (Cert. #972)
- RSA (Cert. #937)
- HMAC (Cert. #1101)
- ECDSA (#258)

ArubaOS Crypto Module implementation supports the following FIPS Approved Algorithms:

- AES (Cert. #1850)
- Triple-DES (Cert. #1198)
- SHS (Cert. #1627)
- RNG (Cert. #969)
- RSA (Cert. #933)
- HMAC (Cert. #1098)
- ECDSA (Cert. #257)

ArubaOS UBOOT Bootloader implements the following FIPS-approved algorithms:

- RSA (Cert. #935)
- SHS (Cert. #1629)

Non-FIPS Approved Algorithms

The cryptographic module implements the following non-approved algorithms that are not permitted for use in the FIPS 140-2 mode of operations:

- DES
- HMAC-MD5
- MD5

- RC4
- NDRNG

In addition, withing the FIPS Approved mode of operation, the module supports the following allowed key establishment schemes:

- Diffie-Hellman (key agreement; key establishment methodology provides 80 bits of encryption strength; non-compliant less than 80-bits of encryption strength)
- EC Diffie-Hellman (key agreement; key establishment methodology provides between 128 and 192 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 80 bits of encryption strength)

Critical Security Parameters

The following are the Critical Security Parameters (CSPs) used in the switch.

Table 11: CSPs Used in Aruba Mobility Controllers

CSPs	CSPs type	Generation	Storage and Zeroization	Use
Key Encryption Key (KEK)	Triple-DES 168-bit key	Hard Coded	Stored in Flash and zeroized by using the CLI command wipe out flash	Encrypts IKEv1/IKEv2 Pre-shared key, RADIUS server shared secret, RSA private key, ECDSA private key, 802.11i pre-shared key and Passwords.
IKEv1/IKEv2 Pre-shared key	64 character pre-shared key	CO configured	Stored encrypted in Flash with the KEK. Zeroized by changing (updating) the pre-shared key through the User interface.	User and module authentication during IKEv1, IKEv2
RADIUS server shared secret	6-128 character shared secret	CO configured	Stored encrypted in Flash with the KEK. Zeroized by changing (updating) the pre-shared key through the User interface.	Module and RADIUS server authentication
Enable secret	6-64 character password	CO configured	Store in ciphertext in flash. Zeroized by changing (updating) through the user interface.	Administrator authentication
IPSec session encryption keys	168-bit Triple-DES or 128/192/256-bit AES-CBC or 128/256-bit AES-GCM keys	Established during the Diffie-Hellman key agreement	Stored in plaintext in volatile memory. Zeroized when the session is closed.	Secure IPSec traffic

IPSec session authentication keys	HMAC SHA-1 key	Established during the Diffie-Hellman key agreement	Stored in plaintext in volatile memory. Zeroized when the session is closed.	User authentication
SSH Diffie-Hellman shared secret	128-octet intermediate value used for key derivation	Established during the SSH Diffie-Hellman key agreement	Stored in plain text in volatile memory, Zeroized when session is closed.	Key agreement in SSH
IKEv1/IKEv2 Diffie-Hellman private key	768/1024-bit (MODP group) or 256/384-bit (Elliptic curve group) Diffie-Hellman private key. Note: Key size 768 bits is not allowed in FIPS mode.	Generated internally during IKEv1/IKEv2 negotiations	Stored in the volatile memory. Zeroized after the session is closed.	Used in establishing the session key for an IPSec session
IKEv1/IKEv2 Diffie-Hellman shared secret	128 octet or 32/48 octet (Elliptic curve Diffie Hellman) intermediate value used for cryptographic key derivation	Established during the Diffie-Hellman Key Agreement	Stored in plaintext in volatile memory. Zeroized when session is closed.	Key agreement in IKEv1/IKEv2
IKEv1/IKEv2 session authentication key	160-bit HMAC-SHA1or 256 byte HMAC-SHA-256-128 or 384 byte HMAC-SHA-384-192 key	Established as a result of Diffie-Hellman key agreement.	Stored in plaintext in volatile memory. Zeroized when session is closed.	IKEv1/IKEv2 payload integrity verification
IKEv1/IKEv2 session encryption key	168-bit Triple-DES or 128/192/256-bit AES-CBC key	Established as a result of Diffie-Hellman key agreement.	Stored in plaintext in volatile memory. Zeroized when session is closed.	IKEv1/IKEv2 payload encryption
SSH session keys	168-bit Triple-DES or 128/192/256-bit AES keys	Established during the SSH key exchange using the Diffie-Hellman key agreement	Stored in plaintext in volatile memory. Zeroized when the session is closed.	Secure SSH traffic
SSH session authentication key	160-bit HMAC-SHA-1	Established during the SSH key exchange using the Diffie-Hellman key agreement	Stored in plaintext in volatile memory. Zeroized when the session is closed.	Secure SSH traffic
SSH Diffie-Hellman Private Key	768/1024-bit Diffie-Hellman private key. Note: Key size 768 bits is not allowed in FIPS mode.	Generated internally during the SSH session negotiations	Stored in the volatile memory. Zeroized after the session is closed.	Used in establishing the session key for an SSH session.

TLS pre-master secret	48 byte secret	Externally generated input to the module by being wrapped by RSA public key	Stored in plaintext in volatile memory. Zeroized when the session is closed.	Key agreement during TLS
TLS session encryption key	AES 128, 192, 256	Generated in the module	Stored in plaintext in volatile memory. Zeroized when the session is closed.	Key agreement during 802.1x connection
TLS session authentication key	160-bit HMAC-SHA1 key	Generated in the module	Stored in plaintext in volatile memory. Zeroized when the session is closed.	Key agreement during 802.1x connection
RSA Private Key	RSA 1024/2048 bit key	Generated in the module	Stored in flash memory encrypted with KEK. Zeroized by the CO command **write erase all**.	Used by TLS and EAP-TLS/PEAP protocols during the handshake, used for signing OCSP responses, and used by IKEv1/IKEv2 for device authentication and for signing certificates
ECDSA Private Key	ECDSA suite B P-256 and P-384 curves	Generated in the module	Stored in flash memory encrypted with KEK. Zeroized by the CO command **write erase all**.	Used by TLS and EAP-TLS/PEAP protocols during the handshake.
skeyid	Intermediate 160-bit/256-byte/384-byte value used in key derivation	Established during the Diffie-Hellman Key Agreement	Stored in plaintext in volatile memory. Zeroized when session is closed.	Key agreement in IKEv1/IKEv2
skeyid_d	Intermediate 160-bit/256-byte/384-byte value used in key derivation	Established during the Diffie-Hellman Key Agreement	Stored in plaintext in volatile memory. Zeroized when session is closed.	Key agreement in IKEv1/IKEv2
802.11i Pre-Shared Key (PSK)	802.11i pre-shared secret key (256-bit)	CO configured	Stored in flash memory encrypted with KEK. Zeroized by the CO command **write erase all**.	Used by the 802.11i protocol
802.11i Pair-Wise Master key (PMK)	802.11i secret key (256-bit)	Derived during the EAP-TLS/PEAP handshake	Stored in the volatile memory. Zeroized on reboot.	Used by the 802.11i protocol
802.11i session key	AES-CCM key (128 bit), AES-GCM key (128/256-bit)	Derived from 802.11 PMK	Stored in plaintext in volatile memory. Zeroized on reboot.	Used for 802.11i encryption

Data link (Layer 2) encryption key	AES key (256 bit)	Derived during the EAP-TLS handshake	Stored in plaintext in volatile memory. Zeroized on reboot.	Used to encrypt tunneled Layer 2 frames
Data link (Layer 2) integrity key	HMAC-SHA1 key (160-bit)	Derived during EAP-TLS handshake storage and zeroization: Stored in plaintext in volatile memory	Stored in plaintext in volatile memory. Zeroized on reboot.	Used to integrity-protect tunneled Layer 2 frames
Passwords	6-character password	CO configured	Stored encrypted in Flash with KEK. Zeroized by either deleting the password configuration file or by overwriting the password with a new one.	Authentication for accessing the management interfaces, RADIUS authentication
ArubaOS OpenSSL RNG Seed for FIPS compliant ANSI X9.31, Appendix A2.4 using AES-128 key algorithm	Seed (16 bytes)	Derived using NON-FIPS approved HW RNG (/dev/urandom)	Stored in plaintext in volatile memory only. Zeroized on reboot.	Seed ANSI X9.31 RNG
ArubaOS OpenSSL RNG Seed key for FIPS compliant ANSI X9.31, Appendix A2.4 using AES-128 key algorithm	Seed key (16 bytes, AES-128 key algorithm)	Derived using NON-FIPS approved HW RNG (/dev/urandom)	Stored in plaintext in volatile memory only. Zeroized on reboot.	Seed ANSI X9.31 RNG
ArubaOS cryptographic Module RNG seed for FIPS compliant 186-2 General purpose (x-change Notice); SHA-1 RNG	Seed (64 bytes)	Derived using NON-FIPS approved HW RNG (/dev/urandom)	Stored in plaintext in volatile memory. Zeroized on reboot.	Seed 186-2 General purpose (x-change Notice); SHA-1 RNG
ArubaOS cryptographic Module RNG seed key for FIPS compliant 186-2 General purpose (x-change Notice); SHA-1 RNG	Seed key (64 bytes)	Derived using NON-FIPS approved HW RNG (/dev/urandom)	Stored in plaintext in volatile memory. Zeroized on reboot.	Seed 186-2 General purpose (x-change Notice); SHA-1 RNG

Self-Tests

The Aruba Mobility Controller performs both power-up and conditional self-tests. In the event any self-test fails, the switch will enter an error state, log the error, and reboot automatically.

The following self-tests are performed:

Aruba Hardware Known Answer Tests:

- AES KAT
- AES-CCM KAT
- AES-GCM KAT
- Triple DES KAT
- HMAC (HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512) KAT

ArubaOS OpenSSL Module:

- AES KAT
- Triple-DES KAT
- RNG KAT
- RSA KAT
- ECDSA (sign/verify)
- SHA (SHA1, SHA256 and SHA384) KAT
- HMAC (HMAC-SHA1, HMAC-SHA256 and HMAC-SHA384) KAT

ArubaOS Cryptographic Module

- AES KAT
- Triple-DES KAT
- SHA (SHA1, SHA256, SHA384 and SHA512) KAT
- HMAC (HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512) KAT
- RSA (sign/verify)
- ECDSA (sign/verify)
- FIPS 186-2 RNG KAT

ArubaOS Uboot BootLoader Module

- Firmware Integrity Test: RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-1

Following Conditional Self-tests are performed in the switch:

ArubaOS OpenSSL Module

- Bypass Test
- CRNG Test on Approved RNG
- ECDSA Pairwise Consistency Test
- RSA Pairwise Consistency Test
- Firmware Load Test - RSA PKCS#1 v1.5 (2048 bits) signature verification

ArubaOS Crypto Module

- CRNG Test on Approved RNG
- ECDSA Pairwise Consistency Test
- RSA Pairwise Consistency Test

Conditional Tests on Hardware

- CRNG test on non-Approved RNGs

Self-test results are logged in a log file. Upon successful completion of the power-up self tests, the module logs a KATS: passed message into a log file. Confirm the file update by checking the associated time of the file.

In the event of a hardware KATs failure, the log file records one of the following messages depending on the algorithm being tested:

- `AES256 HMAC-SHA1 hash failed`
- `AES256 Encrypt failed`
- `AES256 Decrypt Failed`
- `3DES HMAC-SHA1 hash failed`
- `3DES Encrypt failed`
- `3DES Decrypt Failed`
- `DES HMAC-SHA1 hash failed`
- `DES Encrypt failed`
- `DES Decrypt Failed`
- `HW KAT test failed for AESCCM CTR. Rebooting`
- `AESCCM Encrypt Failed`

This text is followed by this message:

```
The POST Test failed!!!!

Rebooting…
```

Alternating Bypass State

The controller implements an alternating bypass state when:

- a port is configured in trusted mode to provide unauthenticated services
- a configuration provides wireless access without encryption

The alternating bypass status can be identified by retrieving the port configuration or the wireless network configuration.

Mitigation of Other Attacks

ArubaOS includes two modules that provide protection from attacks. These are:

- XSec
- Wireless Intrusion Protection

XSec

xSec is a highly secure data link layer (Layer 2) protocol that provides a unified framework for securing all wired and wireless connections using strong encryption and authentication. xSec provides greater security than Layer 3 encryption technologies through the use of FIPS-validated encryption algorithms (AES-CBC-256 with HMAC-SHA1) to secure Layer 2 traffic, as well as the encryption of Layer 2 header information including MAC addresses. xSec was jointly developed by Aruba Networks and Funk Software.

Many government agencies and commercial entities that transmit highly sensitive information over wireless networks mandate that strong Layer 2 encryption technologies be deployed to ensure absolute data privacy. U.S. DoD Directive 8100.2 requires that all data transmitted using commercial wireless devices be encrypted at Layer 2 or Layer 3. The U.S. Navy and Army are requiring Layer 2 encryption, and cryptographic engines used for all sensitive government communications must be validated as meeting FIPS 140-2 requirements.

xSec has been designed to address this requirement and to provide a number of additional benefits.

Wireless Intrusion Detection

Aruba's Wireless Intrusion Protection (WIP) module eliminates the need for a separate system of RF sensors and security appliances. The WIP module provides extraordinary capabilities to Aruba's enterprise mobility system, giving administrators visibility into the network, along with the power to thwart malicious wireless attacks, impersonations and unauthorized intrusions.

Wireless intrusion detection is only the first step in securing the corporate environment from unwanted wireless access. Without adequate measures to quickly shut down intrusions, detection is almost worthless. Without accurate classification of APs and stations (e.g., valid, rogue, or neighbor), providing an automated response to possible intrusion is impossible.

Aruba access points constantly scan all channels of the RF spectrum, capturing all 802.11 traffic and locally examining the captured data. Only policy violations are sent to the central mobility controller to ensure minimal impact on wired network performance. While scanning the environment, the Aruba system learns about all wireless APs and stations and classifies these devices based on traffic flows seen on the wire and in the air. This traffic is collected and correlated on the mobility controller.

Aruba's WIP module provides both detection and prevention capabilities. Users and devices are detected and classified so administrators can react to both unintentional and malicious WLAN access. No other system on the market provides such capabilities.

Unique Station and User Classification

Aruba's patent-pending classification system automatically identifies and classifies all APs and stations connected to the network. The system works by comparing traffic seen in the air with traffic seen on the wire. When a match is found, it is known with certainty that the device belongs to the local network rather than a neighboring network. This avoids false alarms for the administrator, because only true rogue devices are classified as such.

Detecting and Disabling Rogue APs

Aruba's classification algorithms allow the system to accurately determine who is a threat and who is not. Once classified as rogue, these APs can be automatically disabled. Administrators are also notified of the presence of rogue devices, along with their precise physical location on a floorplan, so that they may be removed from the network.

Denial of Service and Impersonation Protection

Wireless networks, by their nature, make an attractive target for denial of service attacks. Such attacks include software that floods the network with association requests, attacks that make a laptop look like thousands of APs, and deauthentication floods. Aruba mobility controllers equipped with the Aruba WIP module maintain signatures of many different wireless attacks and are able to block them so service is not disrupted.

Advanced Denial of Service (DoS) protection keeps enterprises safe against a variety of wireless attacks, including association and de-authentication floods, honeypots and AP and station impersonations. Based on location signatures and client classification, Aruba access points will drop illegal requests and generate alerts to notify administrators of the attack.

Man-in-the-Middle Protection

One of the common attacks possible in wireless networks is the "man-in-the-middle" attack. During a man-in-the-middle attack, a hacker masquerades as a legitimate AP. Then, acting as a relay point, this man-in-the-middle fools users and other APs into sending data through the unauthorized device. An attacker can then modify or corrupt data or conduct password-cracking routines.

Aruba access points monitor the air to detect other wireless stations masquerading as valid APs. When such masquerading is detected, appropriate defense mechanisms are put into place. Aruba mobility controllers also track unique "signatures" for each wireless client in the network. If a new station is introduced claiming to be a particular client, but without the proper signature, a station impersonation attack is detected.

Policy Definition and Enforcement

Aruba WIP provides a number of policies that can be configured to take automatic action when a policy is violated. Examples of wireless policies include weak WEP implementation detection, AP misconfiguration protection, ad-hoc network detection and protection, unauthorized NIC type detection, wireless bridge detection and more.

Using Wireless to Protect your Wired Network

Even if wireless LANs are not sanctioned at this time, no security conscious company can afford to do nothing. Aruba's WIP will keep wireless traffic from working its way into the wired network through rogue APs unknowingly attached to a network port. With Aruba's mobility system equipped with WIP, the enterprise network is protected against wireless security holes. And when the enterprise is ready to deploy wireless LANs, the Aruba system can be easily reconfigured to provide a scalable and secure wireless LAN infrastructure.

Using Wireless to Protect your Existing Wireless Network

Aruba's mobility system with WIP delivers the detection and protection necessary to keep your existing wireless network safe from undesirable wireless access. ArubaOS WIP complements and enhances any existing WLAN deployment, including Cisco deployments, by providing advanced RF security and control features not found in first-generation wireless products.

Installing the Controller

This chapter covers the physical installation of the Aruba 620 and 650 Mobility Controllers with FIPS 140-2 Level 2 validation. The Crypto Officer is responsible for ensuring that the following procedures are used to place the switch in a FIPS-approved mode of operation.

This chapter covers the following installation topics:

- Precautions to be observed during installation
- Requirements for the switch components and rack mounting gear
- Selecting a proper environment for the switch
- Mounting the switch in a rack
- Connecting power to the switch

Pre-Installation Checklist

The following tools and equipment are required for installation of an Aruba 650 Series controller.

- Rack Mount Bracket (x2, not used for tabletop installation)
- 6-32 x 1/4" Phillips Flat Head Screws (4x, included with rack mount brackets)
- 12-24 x 5/8" Phillips Flat Head Screws (4x, 19-inch (48.26 cm) rack system mount screws).
- Suitable Screwdrivers for both screw types.
- AC Power Cord (country-specific)
- Left and right side bezels (not used for rack mounting)

To deploy an Aruba 650 Series controller on a flat surface, such as a tabletop, insert the four rubber mounting feet to the bottom of the unit, attach side bezels by snapping them into place and then place the unit on a hard flat surface.

The following tools and equipment are required for installation of an Aruba 620 controller.

- Rack Mount Bracket (x2, not used for tabletop installation)
- Screws (4x, included with rack mount brackets)
- Suitable Screwdriver.
- AC Power Cord (country-specific)
- Left and right side bezels (not used for rack mounting)

To deploy an Aruba 620 controller on a flat surface, such as a tabletop, insert the four rubber mounting feet to the bottom of the unit, attach side bezels by snapping them into place and then place the unit on a hard flat surface.

Precautions

- Installation should be performed only by a trained technician.
- Dangerous voltage in excess of 240 VAC is always present while the Aruba Power Supply is plugged into an electrical outlet. Remove all rings, jewelry, and other potentially conductive material before working with this product.
- Never insert foreign objects into the chassis, the power supply, or any other component, even when the power supplies have been turned off, unplugged, or removed.
- Main power is fully disconnected from the switch only by unplugging all power cords from their power outlets. For safety reasons, make sure the power outlets and plugs are within easy reach of the operator.
- Do not handle electrical cables that are not insulated. This includes any network cables.
- Keep water and other fluids away from the product.
- Comply with electrical grounding standards during all phases of installation and operation of the product. Do not allow the switch chassis, network ports, power supplies, or mounting brackets to contact any device, cable, object, or person attached to a different electrical ground. Also, never connect the device to external storm grounding sources.
- Installation or removal of the chassis or any module must be performed in a static-free environment. The proper use of anti-static body straps and mats is strongly recommended.
- Keep modules in anti-static packaging when not installed in the chassis.
- Do not ship or store this product near strong electromagnetic, electrostatic, magnetic or radioactive fields.
- Do not disassemble chassis or modules. They have no internal user-serviceable parts. When service or repair is needed, contact Aruba Networks.

The Security Kit

The Aruba Mobility Controller FIPS 140-2 Level 2 Security Kit modifies the standard Aruba Mobility Controller hardware, firmware, and documentation to assure FIPS 140-2 Level 2 validation.

Product Examination
The units are shipped to the Crypto Officer in factory-sealed boxes using trusted commercial carrier shipping companies. The Crypto Officer should examine the carton for evidence of tampering. Tamper-evidence includes tears, scratches, and other irregularities in the packaging.

Package Contents
The product carton should include the following:

- Aruba 620 or 650 Mobility Controller
- Rack/tabletop mounting kit
- Aruba User Documentation CD
- Tamper-Evident Labels

Tamper-Evident Labels

After testing, the Crypto Officer must apply Tamper-Evident Labels (TELs) to the switch. When applied properly, the TELs allow the Crypto Officer to detect the opening of the chassis cover, the removal or replacement of modules or cover plates, or physical access to restricted ports. Vendor provides FIPS 140 designated TELs which have met the physical security testing requirements for tamper evident labels under the FIPS 140-2 Standard. TELs are not endorsed by the Cryptographic Module Validation Program (CMVP).

 The tamper-evident labels shall be installed for the module to operate in a FIPS Approved mode of operation.

 Aruba Provides double the required amount of TELs. If a customer requires replacement TELs, please call customer support and Aruba will provide the TELs   (Part # 4010061-01).
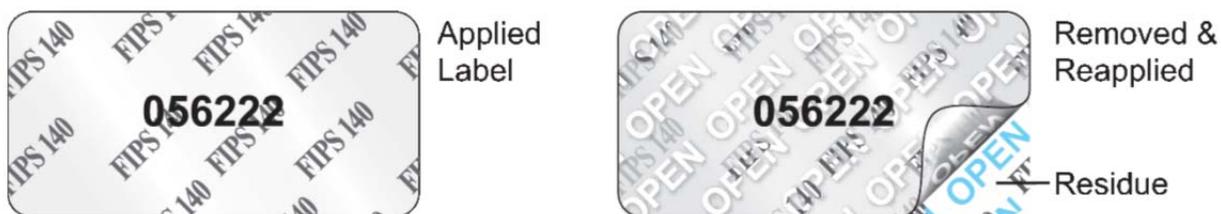
 The Crypto officer shall be responsible for keeping the extra TELs at a safe location and managing the use of the TELs.

Reading TELs

Once applied, the TELs included with the switch cannot be surreptitiously broken, removed, or reapplied without an obvious change in appearance:

Figure 1 *Tamper-Evident Labels*

Each TELs also has a unique serial number to prevent replacement with similar labels.

Required TEL Locations

Aruba 620

This sections displays all the TEL locations on the Aruba 620. The Aruba 620 requires a minimum of 8 TELs to be applied as follows:

To detect opening of the chassis cover:

1. Spanning the front face plate and left and bottom chassis cover

2. Spanning the front face plate and top chassis cover

3. Spanning the front face plate and bottom chassis cover

4. Spanning the front face plate and right and bottom chassis cover

5. Spanning the front face plate and right and bottom chassis cover

6. Spanning the front face plate and top chassis cover

7. Spanning the front face plate and bottom chassis cover

8. Spanning the front face plate and left and bottom chassis cover

To detect access to restricted ports:

3. Spanning the Express Card slot

7. Spanning the serial port

Figure 2 *Aruba 620 — Front view*

Figure 3 *Aruba 620 — Back view*

Figure 4 *Aruba 620 — Left-side view*

Figure 5 *Aruba 620 — Right-side view*
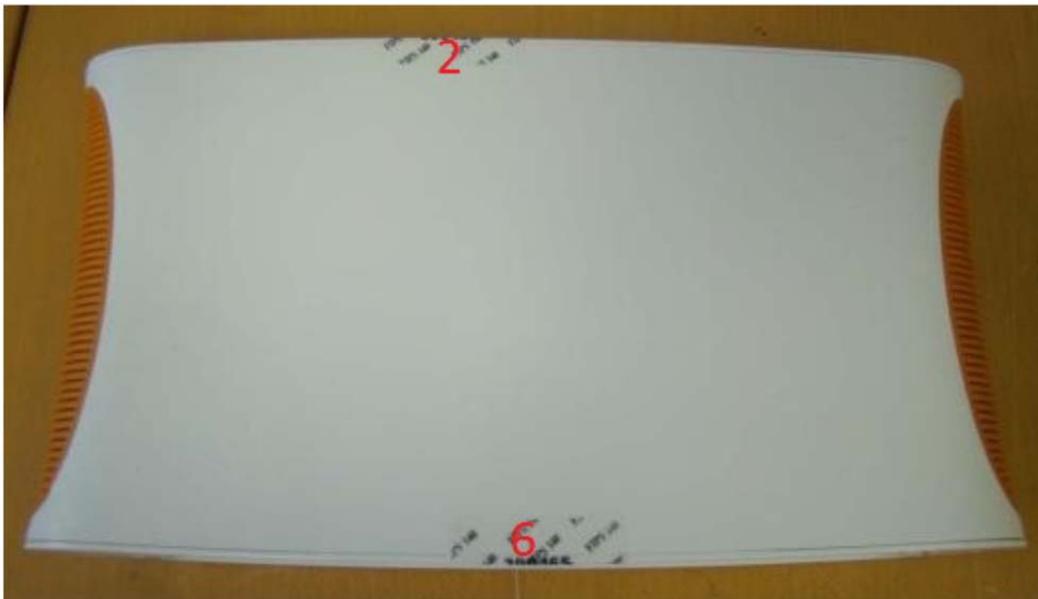

Figure 6 *Aruba 620 — Top view*

Figure 7 *Aruba 620 — Bottom view*

Aruba 650

This sections displays all the TEL locations on the Aruba 650. The Aruba 650 requires a minimum of 8 TELs to be applied as follows:

To detect opening of the chassis cover:

1. Spanning the front face plate and left chassis cover

2. Spanning the front face plate and bottom chassis cover

3. Spanning the front face plate and right chassis cover

4. Spanning the right chassis cover and top chassis cover

6. Spanning the left chassis cover and top chassis cover

7. Spanning the front face plate and bottom chassis cover

8. Spanning the rear face plate and bottom chassis cover

To detect access to restricted ports:

2. Spanning the serial port

5. Spanning the Express Card slot

Figure 8 *Aruba 650 — Front view*

Figure 9 *Aruba 650 — Back view*

Figure 10 *Aruba 650 — Left-side view*

Figure 11 *Aruba 650 — Right-side view*

Figure 12 *Aruba 650 — Top view*

- *Aruba 650 — Bottom view*

Applying TELs

The Crypto Officer is responsible for securing and having control at all times of any unused tamper evident labels. The Crypto Officer should employ TELs as follows:

- Before applying a TEL, make sure the target surfaces are clean and dry.
- Do not cut, trim, punch, or otherwise alter the TEL.
- Apply the wholly intact TEL firmly and completely to the target surfaces.
- Ensure that TEL placement is not defeated by simultaneous removal of multiple modules.
- Allow 24 hours for the TEL adhesive seal to completely cure.
- Record the position and serial number of each applied TEL in a security log.

Once the TELs are applied, the Crypto Officer (CO) should perform initial setup and configuration as described in the next chapter.

Ongoing Management

The Aruba 620 and 650 Mobility Controllers meet FIPS 140-2 Level 2 requirements. The information below describe how to keep the switch in FIPS-approved mode of operation. The Crypto Officer must ensure that the switch is kept in a FIPS-approved mode of operation.

Crypto Officer Management

The Crypto Officer must ensure that the switch is always operating in a FIPS-approved mode of operation. This can be achieved by ensuring the following:

- FIPS mode must be enabled on the switch before Users are permitted to use the switch (see "Enabling FIPS Mode" on page 41)
- CO can check if the switch is in FIPS mode using the WebUI **Configuration > Network > Controller > Systems Settings** or 'FIPS enable' is   shown on the SSH Command Line Interface (CLI) after issuing the command `show fips`
- The admin role must be root.
- Passwords must be at least six characters long.
- VPN services can only be provided by IPsec or L2TP over IPsec.
- Access to the switch Web Interface is permitted only using HTTPS over a TLS tunnel. Basic HTTP and HTTPS over SSL are not permitted.
- Only SNMP read-only may be enabled.
- Only FIPS-approved algorithms can be used for cryptographic services (such as HTTPS, L2, AES-CBC, SSH, and IKEv1/IKEv2-IPSec), which include AES, Triple-DES, SHA-1, HMAC SHA-1, and RSA signature and verification.
- TFTP can only be used to load backup and restore files. These files are: Configuration files (system setup configuration), the WMS database (radio network configuration), and log files. (FTP and TFTP over IPsec can be used to transfer configuration files.)
- The switch logs must be monitored. If a strange activity is found, the Crypto Officer should take the switch off line and investigate.
- The Tamper-Evident Labels (TELs) must be regularly examined for signs of tampering.
- The Crypto Officer shall not configure the Diffie-Hellman algorithm with 768-bits (Group 1) in FIPS mode for IKEv1/IKEv2-IPSec and SSH.

User Guidance

The User accesses the switch VPN functionality as an IPsec client. The user can also access the switch 802.11i functionality as an 802.11 client. Although outside the boundary of the switch, the User should be directed to be careful not to provide authentication information and session keys to others parties.

Setup and Configuration

The Aruba 620 and 650 Mobility Controllers meet FIPS 140-2 Level 2 requirements. The sections below describe how to place and keep the switch in FIPS-approved mode of operation. The Crypto Officer (CO) must ensure that the switch is kept in a FIPS-approved mode of operation.

The switch can operate in two modes: the FIPS-approved mode, and the standard non-FIPS mode. By default, the switch operates in non-FIPS mode.

Setting Up Your Controller

To set up your controller:

1. Make sure that the controller is not connected to any device on your network.
2. Boot up the controller.
3. Connect your PC or workstation to a line port on the controller.

For further details, see the *ArubaOS 6.1 Quick Start Guide*.

Enabling FIPS Mode

For FIPS compliance, users cannot be allowed to access the switch until the CO changes the mode of operation to FIPS mode. There are two ways to enable FIPS mode:

- Use the WebUI
- Use the Setup Wizard

Enabling FIPS with the Setup Wizard

The Setup Wizard allows you to configure access to the controller, install software licenses, and configure wireless local area networks (WLANs) for internal or guest users.

The Setup Wizard is available the first time you connect to and log into the controller or whenever the controller is reset to its factory default configuration. After you complete the Setup Wizard, the controller reboots using the new configuration information you entered.

For details on running the Setup Wizard, see the *ArubaOS 6.1 Quick Start Guide*.

Enabling FIPS with the WebUI

The default IP address of the controller is 172.16.0.254. When you connect a PC or workstation to a line port on the controller, you can connect to this IP address through a Web browser. The system must be configured to either obtain its IP address via DHCP or have a static IP address on the 172.16.0.0/24 subnetwork.

To log in with the WebUI:

1. Open a Web browser and connect to http://172.16.0.254.
2. Log in.
3. Go to the **Configuration > Network > Controller > System Settings** page (the default page when you click the Configuration tab).
4. Click the **FIPS Mode for Mobility Controller Enable** checkbox.

If you need to enable FIPS mode on a controller that is no longer in the factory default configuration, you can either:

- o Log in through the WebUI as described previously
- o Enable FIPS on the Configuration > Wizards > Controller Wizard page

5. 'FIPS Enable' is shown on SSH command Line Interface (CLI) after issuing the command `show fips`.

Disallowed FIPS Mode Configurations

When you enable FIPS mode, the following configuration options are disallowed:

- All WEP features
- WPA
- TKIP mixed mode
- Any combination of DES, MD5, and PPTP