Aruba 3000 and 6000/M3

Mobility Controllers with ArubaOS FIPS Firmware Non-Proprietary Security Policy

FIPS 140-2 Level 2 Release Supplement

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

Contents

Preface

This security policy document can be copied and distributed freely.

Purpose of this Document

This release supplement provides information regarding the Aruba 3000 and 6000/M3 Mobility Controller 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

Related Documents

Product Manuals

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

- *Aruba 3000 and 6000/M3 Mobility Controllers with ArubaOS FIPS Firmware Non-Proprietary Security Policy (this document)*
- *Aruba 6000 Mobility Controller Installation Guide*
- *Aruba 3000-series Mobility Controller Installation Guide*
- *ArubaOS 3.3.2 User Guide*
- *ArubaOS 3.3.2 CLI Reference Guide*

- *ArubaOS 3.3.2 Quick Start Guide*
- *ArubaOS 3.3.2 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 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 3000 and 6000/M3 Mobility Controllers

1

This chapter introduces the Aruba 3000 and 6000/M3 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 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 3200 (3200-8-AOS-STD-FIPS-US)
- Aruba 3400 (3400-32-AOS-STD-FIPS-US)
- Aruba 3600 (3600-64-AOS-STD-FIPS-US)
- Aruba 6000 (6000-BASE-2PSU-200-FIPS, 6000-BASE-2PSU-400-FIPS, LC-2G-1, LC-2G24F-1, LC-2G24FP-1, and either one or two M3mk1-G10X-10G2X).
- The exact firmware versions tested were A3000_3.3.2.0-FIPS, ArubaOS_MMC_3.3.2.0-FIPS.

Physical Description

See page 29 for a list of what ships with this product.

Dimensions

The Aruba 6000 Mobility Controller has the following physical dimensions:

- 3 RU chassis is designed to fit in a standard 19" rack. A separate mounting kit is needed for a 23" rack.
- Size:
  - Width 17.4" (19" rack width)
  - Height 5.25" (3 RU)—3.5" for the card slots plus 1 RU for the power supply slots
  - Depth 14"
- Maximum weight: Up to 58 lbs (26.5 kg)

The Aruba 3200 Mobility Controller has the following physical dimensions:

- 1 RU chassis is designed to fit in a standard 19" rack with the included mounting kit. A separate mounting kit is needed for a 23" rack.
- Size:
  - Width 13.8"
  - Height 1.75" (1 RU)
  - Depth 11.7"
- Maximum weight: Up to 7.1 lbs (3.2 kg)

The Aruba 3400 and 3600 Mobility Controllers have the following physical dimensions:

- 1 RU chassis is designed to fit in a standard 19" rack with the included mounting kit. A separate mounting kit is needed for a 23" rack.
- Size:
  - Width 13.8"
  - Height 1.75" (1 RU)
  - Depth 11.7"
- Maximum weight: Up to 7.4 lbs (3.4 kg)

Cryptographic Module Boundaries

For FIPS 140-2 Level 2 validation, the Mobility Controller has been validated as a multi-processor standalone cryptographic module. The steel 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.

Chassis

The Aruba 6000 Mobility Controller chassis is designed to be modular. All of the modular components, consisting of the switching supervisor and network line cards, the fan tray, and the power supplies, are accessible from the front of the chassis and are field replaceable and hot-swappable.

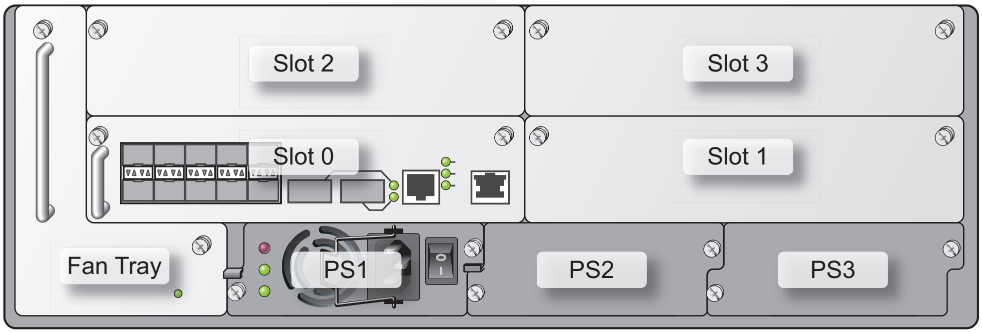

Figure 1-1 The Aruba 6000 Mobility Controller with M3 Mark I

Figure 1-1 shows the front of the Aruba 6000 Mobility Controller, and illustrates the following:

- Slots 2 and 3 are for optional Line Card modules to provide extra port capacity.
- Slots 0 and 1 are for one or two Multi-service Mobility Modules (M3), which combine the Supervisor Card and Line Card functionality in a single module. Note that this validation covers only configurations with one or two M3s.
- M3 indicator LEDs indicate power state, status of the device, and link activity.
- The hot-swappable fan tray cools the switch. The fan tray pulls air from right to left, as viewed from the front of the chassis, across the installed cards.
- PS1, PS2, and PS3 are for Power Supply modules. The number of power supplies required for the system depends on the number and type of Line Cards installed, and whether to include redundancy for fault tolerance.

The Aruba 3000-series Mobility Controller chassis is a 1U not-modular chassis.

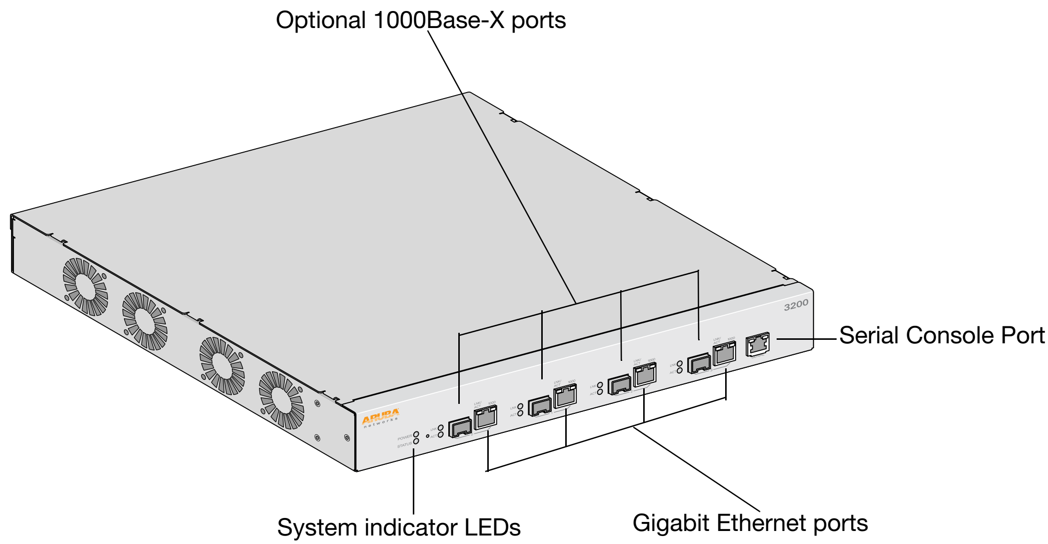

Figure 1-2 The Aruba 3000-series Mobility Controller Chassis

Figure 1-2 shows the front of the Aruba 3000-series Mobility Controller, and illustrates the following:

- System indicator LEDs indicate power state and status of the device.
- Four Gigabit Ethernet ports provide network connectivity.
- Optional 1000Base-X fiber optic ports provide network connectivity.
- Serial Console port is for connecting to a local management console.

This page intentionally left blank.

FIPS 140-2 Level 2 Features

2

Intended Level of Security

The Aruba 3000 and 6000/M3 Mobility Controllers and associated modules are intended to meet overall FIPS 140-2 Level 2 requirements as shown in Table 2-1.

Table 2-1 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.

For the Aruba 6000 the left, top, right, and bottom surfaces are irremovable. The rear panel can be removed by unscrewing fifteen screws. The switch has a number of hot-swappable components at front side, including four slots for supervisor and line cards, one fan tray, and three power supplies. Each of the components is attached with two screws.

For the Aruba 3000-series the left, right, front, rear, and bottom surfaces are irremovable. The top panel can be removed by unscrewing two screws. A metallic opaque shield is installed at the factory during manufacturing and can not be removed by the User.

For physical security, the Aruba 6000 switch requires Tamper-Evident Labels (TELs) to allow the detection of the opening of the chassis covers; the removal or replacement of any module or cover plate, and to block the Serial console port.

The Aruba 3000-series Mobility Controllers require Tamper-Evident Labels (TELs) to allow the detection of the opening of the chassis cover and to block the Serial console port.

To protect the Aruba 3000 and 6000/M3 Mobility Controllers from any tampering with the product, TELs should be applied by the Crypto Officer as covered under "Tamper-Evident Labels" on page 29.

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 2-2 FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input Interface	10/100 Mbps Ethernet port 10/100/1000 Mbps Ethernet ports
Data Output Interface	10/100 Mbps Ethernet port 10/100/1000 Mbps Ethernet ports
Control Input Interface	Power switch (Aruba 6000 only) Reset button (Aruba 6000 only) 10/100 Mbps Ethernet port 10/100/1000 Mbps Ethernet ports 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 (Aruba 6000 only)

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 power and reset through the power and reset switch. 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). 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 (Aruba 6000 only) 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 main roles in the switch (as required by FIPS 140-2 Level 2) that operators may assume: a Crypto Officer role and 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 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 2-3 Crypto-Officer Services

Service	Description	Input	Output	CSP Access
SSH	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), PRNG keys (read access); Crypto Officer's password (read access)
IKE/IPSec	Provide authenticated and encrypted remote management sessions to access the CLI functionality	IKE inputs and data; IPSec inputs, commands, and data	IKE outputs, status, and data; IPSec outputs, status, and data	RSA key pair for IKE (read access), Diffie-Hellman key pair for IKE (read/write access), pre- shared keys for IKE (read access); Session keys for IPSec (read/write access)
Bootrom Monitor Mode	Reboot, update the Bootrom, issue file system-related commands, modify network parameters, and issue various show commands (disabled in FIPS mode)	Commands and configuration data	Status of commands, configuration data	None
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

Table 2-3 Crypto-Officer Services (Continued)

Service	Description	Input	Output	CSP Access
Configuring the VPN	Configure Public Key Infrastructure (PKI); configure the Internet Key Exchange (IKE) Security Protocol; configure the IPSec protocol	Commands and configuration data	Status of commands and configuration data	RSA 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	IKE inputs and data; IPSec inputs, commands, and data	IKE outputs, status, and data; IPSec outputs, status, and data	Preshared key for IKE (read access), Diffie-Hellman key pair for IKE (read/write access), Session keys for IPSec (read/write access)
Self-test	Run firmware/configuration integrity tests, cryptographic algorithm known-answer 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

User Role

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

Table 2-4 User Service

Service	Description	Input	Output	CSP Access
IKE/IPSec	Access the module's IPSec services in order to secure network traffic	IPSec inputs, commands, and data	IPSec outputs, status, and data	RSA key pair for IKE (read access); Diffie-Hellman key pair for IKE (read and write access); pre-shared keys for IKE (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 public key (read) EAP-TLS 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 public key (read) EAP-TLS 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, 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 and SSH or by entering enable command and password in console. Role-based authentication is also performed for User authentication.

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

Table 2-5 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 (IKE)	User	RSA signing and verification is used to authenticate to the module during IKE. This mechanism is as strong as the RSA algorithm using a 1024 bit key pair.
Pre-shared key-based authentication (IKE)	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	32-byte (256-bit) PSK key corresponds to 2^{256} potential combinations.
EAP-TLS authentication	User	1024-bit RSA key corresponds to effective strength of 2^{80}

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, bypass mode processing, and system status indication via LEDs.

The SNMPv1 can be used to remotely perform non-security-sensitive monitoring. SNMP uses a clear text community string for authentication. Also, the Bootrom Monitor mode is disabled in FIPS mode by placing a Tamper Evident Label (TEL) over the serial port.

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. #762) - CBC; 128,192,256 bits - CCM; 128 bits, Assoc. Data Len Range: 15 - 30, Payload Length Range: 0 - 32, Nonce Length(s): 13, Tag Length(s): 8
- TDES (Cert. #667) - CBC; 192 bits (168 used)/1,2,3 keys keying option
- SHA-1 (Cert. #769) - BYTE oriented
- HMAC SHA-1 (Cert. #417)

Hardware encryption is provided for the following non-FIPS-approved algorithms.

- MD5
- RC4
- RSA (key wrapping; key establishment methodology provides 80 bits of encryption strength)

The firmware implementation is performed using OpenSSL crypto library version fips-1.1.1. The firmware implements the following FIPS-approved algorithms:

- AES (Cert. #823) - CBC: 128, 192, 256 bits
- Triple-DES (Cert. #694)- CBC key options Keying Options 1,2,3 used
- SHA-1 (Cert. #823) - BYTE oriented
- HMAC SHA-1 (Cert. #458)
- RSA (Cert. #399)
- RNG (Cert. #475)

The firmware implementation using OpenSSL fips-1.1.1 is also used to implement the following non-FIPS-approved algorithms in the controller firmware:

- MD5
- RC4

- Diffie-Hellman (allowed for key agreement)
- RSA (key wrapping; key establishment methodology provides 80 bits of encryption strength)
- DES

Diffie-Hellman key establishment methodology provides 80-bits of encryption strength; non-compliant less than 80-bits of encryption strength. Note: Only 1024 bit Diffie-Hellman keys are supported by the module in the FIPS mode of operation.

Critical Security Parameters

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

Table 2-6 CSPs Used in Aruba Mobility Controllers

CSPs	CSPs type	Generation	Storage and Zeroization	Use
Key Encryption Key (KEK)	TDES key	Hard Coded	Stored in Flash and zeroized by using the CLI command `wipe out flash`.	Encrypts IKE, pre-shared keys, and database file
Pre-shared keys	64 character pre-shared key	External	Stored encrypted in Flash with the KEK. Zeroized by changing (updating) the pre-shared key through the User interface.	User and module authentication during IKE
RADIUS server shared secret	6-128 character shared secret	External	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	External	A hash is stored in flash. Zeroized by changing (updating) through the user interface.	Administrator authentication
IPSec session keys	168-bit TDES or 128/192/256-bit AES keys; HMAC SHA-1 key	Established during the Diffie-Hellman key agreement	Stored in plaintext in volatile memory. Zeroized when the session is closed.	Secure IPSec traffic

Table 2-6 CSPs Used in Aruba Mobility Controllers (Continued)

CSPs	CSPs type	Generation	Storage and Zeroization	Use
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
IKE 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 IKE negotiations	Stored in the volatile memory. Zeroized after the session is closed.	Used in establishing the session key for an IPSec session
IKE Diffie-Hellman public key	768/1024-bit Diffie-Hellman public key. Note: Key size 768 bits is not allowed in FIPS mode.	Generated internally during IKE negotiations	Stored in plaintext in memory.	Key agreement during IKE
IKE Diffie-Hellman shared secret	128 octet 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 IKE
IKE session authentication key	160-bit HMAC-SHA1 key	Established as a result of Diffie-Hellman key agreement.	Stored in plaintext in volatile memory. Zeroized when session is closed.	IKE payload integrity verification
IKE session encryption key	168-bit TDES or 128/192/256-bit AES keys	Established as a result of Diffie-Hellman key agreement.	Stored in plaintext in volatile memory. Zeroized when session is closed.	IKE payload encryption
SSH session keys	168-bit TDES or 128/192/256-bit AES keys; HMAC SHA-1 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 Diffie-Hellman Public Key	768/1024-bit Diffie-Hellman public 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.

Table 2-6 CSPs Used in Aruba Mobility Controllers (Continued)

CSPs	CSPs type	Generation	Storage and Zeroization	Use
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 session 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
RSA Public Key	RSA 1024 bit key	External	Stored in flash memory.	Used by TLS and EAP-TLS protocols during the handshake, and for firmware load validation
RSA Private Key	RSA 1024 bit key	External	Stored in flash memory encrypted with KEK.	Used by TLS and EAP-TLS protocols during the handshake
skeyid	intermediate 160-bit 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 IKE
skeyid_d	intermediate 160-bit 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 IKE
802.11i Pre-Shared Key (PSK)	802.11i pre-shared secret key (256-bit)	External	Stored in flash memory encrypted with KEK	Used by the 802.11i protocol
802.11i Pair-Wise Master key (PMK)	802.11i secret key (256-bit)	Derived during the EAP-TLS handshake	Stored in the volatile memory. Zeroized on reboot.	Used by the 802.11i protocol
802.11i session key	AES-CCM key (128 bit)	Derived from 802.11 PSK	Stored in plaintext in volatile memory. Zeroized on reboot.	Used for 802.11i encryption

Table 2-6 CSPs Used in Aruba Mobility Controllers (Continued)

CSPs	CSPs type	Generation	Storage and Zeroization	Use
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	Zeroized on reboot.	Used to integrity-prote ct tunneled Layer 2 frames
Passwords	6-character password	External	Stored encrypted in Flash with KEK. Zeroized by either deleting the password configuration file or by overwriting the password with a new one.	Authenticatio n for accessing the management interfaces, RADIUS authentication
PRNG seeds	Seed key (24 bytes, TDES 2-keying option) and seed (8 bytes)	Seeded using non-approved OpenSSL random number generator	In volatile memory only. Zeroized on reboot.	Seed PRNGs
TLS pre-master secret	48 byte secret	Externally generated	Stored in plaintext in volatile memory. Zeroized when the session is closed.	Key agreement during TLS

Encryption Keys and Passwords

- Key Encryption Key (KEK)–The KEK is hard-coded in the image. The KEK encrypts IKE RSA keys pairs, pre-shared keys, and User database. The KEK can be zeroized by erasing the image.
- Preshared keys can be used instead of certificates during IKE authentication. The preshared key must be entered by the Crypto Officer with the username being the IP address and the password being the preshared key. The preshared keys are stored encrypted in flash and can be zeroized by either overwriting them with new ones or by erasing the flash.

- IPSec Session key are used to protect IKE phase 1 & 2 protocol messages. Session keys are generated using the Diffi-Hellman key agreement. IPSec session keys is visible only in process space, and zeroized when the session is closed, in a matter of a few milliseconds.
- The IKE Diffie-Hellman private key is generated during IKE for use for the key establishment during IKE. The key is generated internally and is an ephemeral key that is stored in plaintext in memory. The IKE Diffie-Hellman key pair can be zerorized by using the OPENSSL_cleanse() function, followed by OPENSSL_free() to free up the memory. The key pairs also can be zeroized in a few milliseconds by rebooting the module.
- The IKE User Diffie-Hellman public key is used during the IKE key establishment. The public key is used by the module to establish a shared secret with the user. The public key is an ephemeral key and is stored in plaintext in memory. It can be zeroized by rebooting the module. IKE Diffie-Hellman key pairs can be zerorized in a few milliseconds by using the OPENSSL_cleanse() function, followed by OPENSSL_free() to free up the memory.
- SSH Session keys are used to protect SSH protocol messages. Session keys are generated using the Diffi-Hellman key agreement. SSH session keys are visible only in the process space, and zeroized in a matter of a few milliseconds when the session is closed.
- The SSH Diffie-Hellman private key is generated internally and is used during the SSH key establishment. This key is an ephemeral key and is stored in plaintext in memory. It can be zeroized by rebooting the module. The SSH Diffie-Hellman key pair is zerorized in a few milliseconds by using the OPENSSL_cleanse() function, followed by OPENSSL_free() to free up the memory.
- The SSH User Diffie-Hellman public key is used during the SSHv2 key establishment. The public key is used by the module to establish a shared secret with the user. The public key is an ephemeral key and is stored in plaintext in memory. It can be zeroized by rebooting the module.
- The TLS session keys are derived at the end of EAP-TLS handshake between the wireless client (User role) and RADIUS server. After that, the RADIUS server uses TLS session keys to derive the 802.11i Pairwise Master Key (PMK) and then transport the PMK to the controller encrypted with an IPSec session key. TLS keys are stored in plaintext in memory. They can be zeroized by rebooting the module. Upon closing a session, the session keys are zerorized by using the OPENSSL_cleanse() function, followed by OPENSSL_free() to free up the memory.
- The RSA public key is used primarily for user EAP-TLS authentication. The public key is externally generated and stored in flash memory encrypted with KEK.

- The RSA private key is used primarily for user EAP-TLS authentication. The private key is externally generated and stored in flash memory encrypted with KEK.
- The 802.11i Pre-Shared Key (PSK) is a pre-shared key used to derive session keys for the 802.11i wireless security protocol. The key is stored in flash memory encrypted with KEK.
- The 802.11i Pair-Wise Master Key (PMK) is established during the EAP-TLS handshake and is used to derive session keys for the 802.11i wireless security protocol. The key is stored in volatile memory in plaintext. It can be zeroized in a few milliseconds by rebooting the switch.
- The 802.11i session key is used to encrypt 802.11i communications and is derived from the PSK using the key derivation function specified in the IEEE 802.11i standard. The key is stored in volatile memory in plaintext and is zeroized in a few milliseconds on reboot.
- The data link (Layer 2) encryption key is established during the EAP-TLS handshake and is used to encrypt Layer 2 tunneling frames. It is stored in volatile memory in plaintext. It can be zeroized by rebooting the switch.
- Passwords are used for authentication. The Crypto Officer will not be able to access the CLI and management interfaces until authenticated successfully. SNMPv1 can be used to remotely perform non-security-sensitive monitoring. SNMP uses a clear text community string for authentication. Passwords are also used to remotely authenticate users during RADIUS and to authenticate AAA users.
- All passwords are stored encrypted (database files are encrypted with the key encryption key) in flash, except for the Crypto Officer passwords. The Crypto Officer password is stored encrypted in the configuration file (default.cfg).
- All passwords can be zeroized by overwriting them with new ones or erasing the flash.
- PRNG Seeds are used to seed PRNGs, stored as plaintext in volatile memory and zeroized on reboot in a few milliseconds.
- The RADIUS server shared secret is used to authenticate the module to the RADIUS server.
- The enable secret is used to authenticate the administrator.

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 switch performs the following power-up self-tests:

- Firmware Integrity Test - the switch validates the integrity of its firmware using 2 methods. First, a CRC-32 checksum is calculated for the image and compared to a value in the image header. If these values do not match, the firmware is rejected. Second, an RSA signature is included with the image, and the module maintains a trust anchor chain with which this signature is validated. If the RSA signature validation fails, the image is rejected.
- Cryptographic Algorithm Tests–These tests are run at power-up for the Triple-DES encryption/decryption, AES and AES-CCM encryption/decryption, HMAC SHA-1 calculation/verification, RSA signing/verifying, and the PRNG random data generation.
- RSA Pair-wise Consistency Test (sign/verify)–The RSA pair-wise consistency test takes a RSA private key and signs the hash of some data. The resulting signed data is compared to the hashed data before it was signed. If the two values are equal, then the test fails. If the two values differ, the public key is used to verify the signed data and the resulting value is compared to the original hashed data. If the two values are not equal the test fails.
- RSA Pair-wise Consistency Test (encrypt/decrypt) - The RSA pair-wise consistency test takes a RSA private key and encrypts some data. The resulting cipher is compared to the hashed data before it was encrypted. If the two values are equal, then the test fails. If the two values differ, the public key is used to decrypt the cipher and the resulting value is compared to the original plaintext. If the two values are not equal the test fails.

Following Conditional Self-tests are performed in the switch:

- Continuous Random Number Generator Test—This test is run upon generation of random data by the switch's random number generators to detect failure to a constant value. The module stores the first random number for subsequent comparison, and the module compares the value of the new random number with the random number generated in the previous round and enters an error state if the comparison is successful. The test is performed for approved as well as non-approved RNGs.
- The controller implements alternating bypass test.
- RSA pairwise consistency test.
- Firmware Load Test.

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. The status can be view by using the show log crypto all CLI command.

In the event of a hardware KATs failure, the log file records one of the following messages depending on the algorith 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 3

This chapter covers the physical installation of the Aruba 3000 and 6000/M3 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

You will need the following during installation:

- Aruba 3000 and 6000/M3 Mobility Controller components.
- Aruba 3000 and 6000/M3 rack mounting kit.
- Phillips or cross-head screwdriver.
- 19-inch equipment rack, or equivalent.
- 3U rack space for the Aruba 6000 and 1U rack space for the Aruba 3000-Series with 10 cm (4 inches) clearance to the left, right, front, and rear of the rack.
- Another person to help position the switch.
- Aruba power cord for each power supply, rated to at least 10 A with IEC320 connector.
- Adequate power supplies and electrical power.
- Cool, non-condensing air 0 to 40 °C (32 to 104 °F). May require air conditioning.
- Management Station (PC) with 10/100 Mbps Ethernet port and SSH software.
- A 4- or 8-conductor Category 5 UTP Ethernet cable.

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 Crypto Officer receives the switch in a carton. 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 3000 and 6000/M3 Mobility Controller
- Rack mounting kit
- Aruba User Documentation CD
- Tamper-Evident Labels

Minimum Configuration for the Aruba 6000

The Aruba 6000 Mobility Controller must include the following basic components:

- One modular switch chassis
- One fan tray
- One M3 card in slot 0
- Power Supply

Note: The number and type of power supplies required depends on the number and type of line cards installed in the chassis (refer to the *Aruba 6000 Mobility Controller Installation Guide*).

The switch is shipped with all required modules installed.

Note: The Aruba 3000-Series do not have minimum configurations, as they are fixed configuration chassis.

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).

Reading TELs

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

Figure 3-1 Tamper-Evident Labels

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

Required TEL Locations

The Aruba 6000 Mobility Controller requires a minimum of 11 TELs to be applied as follows:

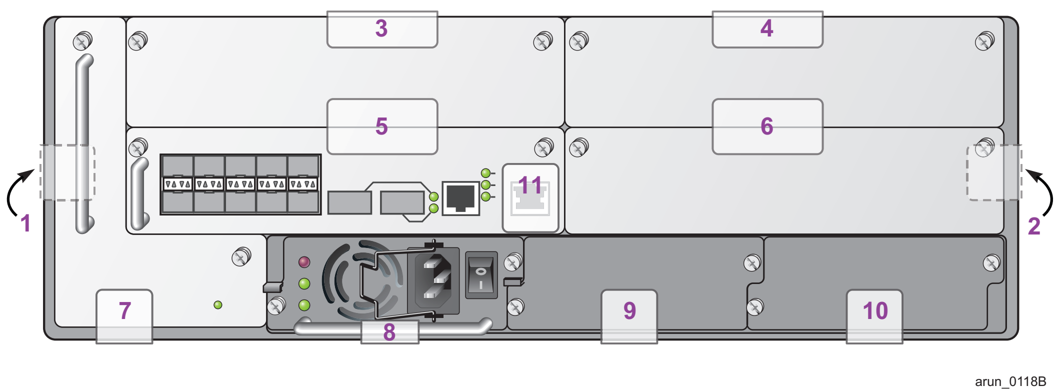

Figure 3-2 Required TELs for the Aruba 6000 Mobility Controller

To Detect Opening the Chassis Cover

1. Spanning the left side and rear of the chassis
2. Spanning the right side and rear of the chassis

To Detect the Removal of Any Module or Cover Plate

3. Spanning the Slot 2 faceplate or blank and the top of the chassis
4. Spanning the Slot 3 faceplate or blank and the top of the chassis
5. Spanning the Slot 0 faceplate or blank and the Slot 2 faceplate or blank

6. Spanning the Slot 1 faceplate or blank and the Slot 3 faceplate or blank
7. Spanning the fan tray faceplate and the bottom of the chassis
8. Spanning the PS1 handle (or blank faceplate) and the bottom of the chassis
9. Spanning the PS2 handle (or blank faceplate) and the bottom of the chassis
10. Spanning the PS3 handle (or blank faceplate) and the bottom of the chassis

To Detect Access to Restricted Ports

11. Spanning the Serial port on the M3

The Aruba 3000-series Mobility Controller requires a minimum of 3 TELs to be applied as follows:

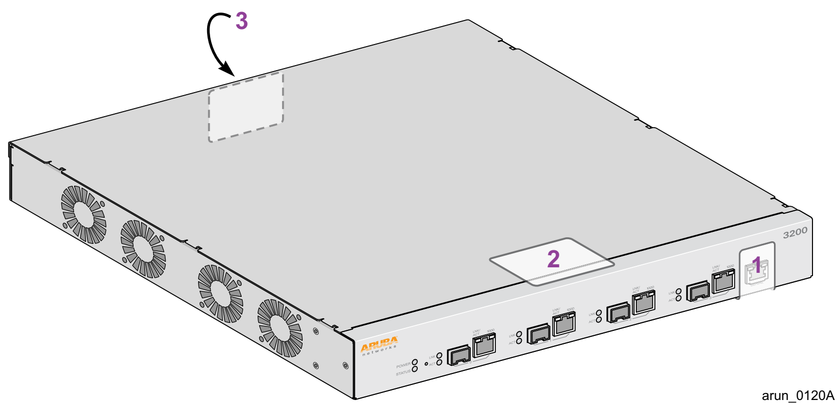

Figure 3-3 Required TELs for the Aruba 3000-series Mobility Controller

To Detect Access to Restricted Port

1. Spanning the Serial port

To Detect Opening the Chassis Cover

2. Spanning the top of the faceplate and top of the chassis
3. Spanning the back and top of the chassis

Applying TELs

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 4

The Aruba 3000 and 6000/M3 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 35)
- 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 IKE/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.
- When installing expansion or replacement modules for the Aruba 6000, use only FIPS-approved modules, replace TELs affected by the change, and record the reason for the change, along with the new TEL locations and serial numbers, in the security log.

- The Crypto Officer shall not configure the Diffie-Hellman algorithm with 768-bits (Group 1) in FIPS mode for IKE/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.

Set Up and Configuration 5

The Aruba 3000 and 6000/M3 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 3.3.2 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 3.3.2 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:

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

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