Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches by Cisco Systems, Inc.

FIPS 140-2 Non Proprietary Security Policy
Level 1 Validation

Version 0.3

March 17, 2015

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches with firmware version IOS XE 03.06.00aE, that form part of the NGWC (Next Generation Wiring Closet) product portfolio, referred to in this document as switches, controllers or the module. This security policy describes how the modules meet the security requirements of FIPS 140-2 Level 1 and how to run the modules in a FIPS 140-2 mode of operation and may be freely distributed.

1.2 Models

- Cisco Catalyst 3650 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Field Replaceable Uplink network modules for the 3850 switches

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 NIST website at http://csrc.nist.gov/groups/STM/index.html.

1.3 Module Validation Level

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

No.	Area Title	3650/3850 Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	2
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A
	Overall module validation level	**1**

Table 1 - Module Validation Level

1.4 References

This document deals only with operations and capabilities of the Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches by Cisco Systems, Inc. in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the routers from the following sources:

The Cisco Systems website contains information on the full line of Cisco Systems Security. Please refer to the following website:
http://www.cisco.com/en/US/products/

For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.

The NIST Validated Modules website (http://csrc.nist.gov/groups/STM/cmvp/validation.html) contains contact information for answers to technical or sales-related questions for the module.

1.5 Terminology

In this document, the Cisco Systems Catalyst 3650 and 3850 are referred to as switches, controllers, or the modules.

1.6 Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

Vendor Evidence document
Finite State Machine
Other supporting documentation as additional references

This document provides an overview of the Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the appliances. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

2 Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches

The Next Generation Wiring Closet (NGWC) program is a game changing architecture for converged services at the access layer. Wireless is one of the many services being integrated within the switch. The wireless service ensures that the access layer terminates the data plane, delivering on the promise of Cisco's unified architecture. Unification implies that services are provided to both wireless and wired stations. The introduction of wireless in the system means that the system must also support an integrated mobility architecture.

The 3650 and the 3850 are the first set of NG3k switches, the next-generation of the successful Catalyst 3k switching product line - the first Doppler ASIC-based switch family that will be a component of the NGWC architecture and instrumental in making the vision of NGWC a reality. The Doppler ASIC is the most important component of the NG3K solution enabling new switching features, providing higher scalability for a large set of switching features and enabling new services such as wireless and context based networking in the wiring closet. The Doppler ASIC provides 24 ports of 1 GE downlinks, 2 ports of 10 GE/1GE uplinks and 2 ports of 1GE uplinks with an integrated 240G stack.

The switches include cryptographic algorithms implemented in IOS software as well as hardware ASICs. The module supports RADIUS, TACACS+, IKE/IPSec, TLS, DTLS, SESA (Symmetric Early Stacking Authentication), SNMPv3, 802.11i, and SSHv2.

In addition to features relevant to the wired network, the 3650 and the 3850 switches also provide functionality that supports the wired-wireless convergence. These features provide the ability to terminate Access Point (AP) tunnels at the access switch port that enables common wired-wireless policies and high capacity for ubiquitous wireless deployments.

2.1 Cryptographic Module Physical Characteristics

The module is a multiple-chip standalone cryptographic module. The cryptographic boundary is defined as encompassing the "top," "front," "left," "right," and "bottom" surfaces of the chassis for the switches and the casing for the switch.

2.2 Module Interfaces

The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The logical interfaces and their mapping are described in the following tables.

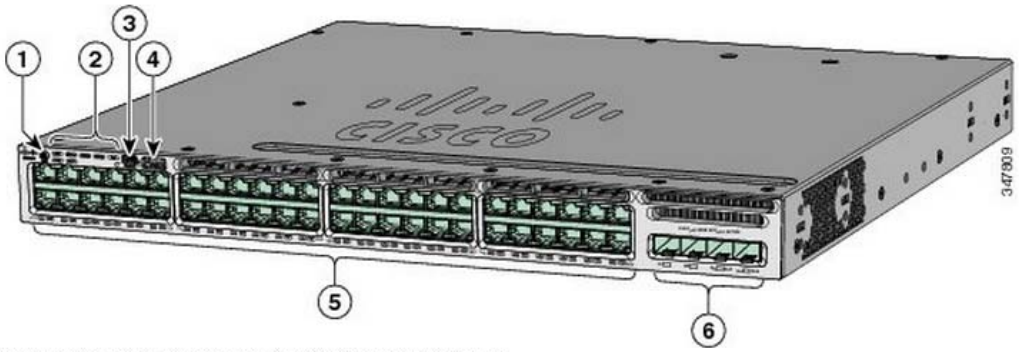
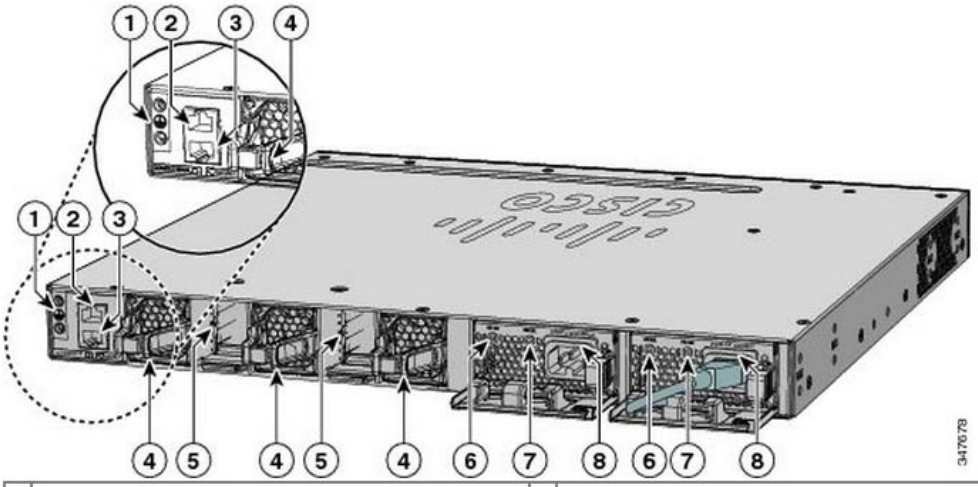


Figure 1-2 Catalyst 3650-24PS-L Switch Front Panel

1	Mode button	4	USB Type A storage port
2	Status LEDs	5	10/100/1000 PoE+ Ethernet ports
3	USB mini-Type B (console) port	6	Uplink ports

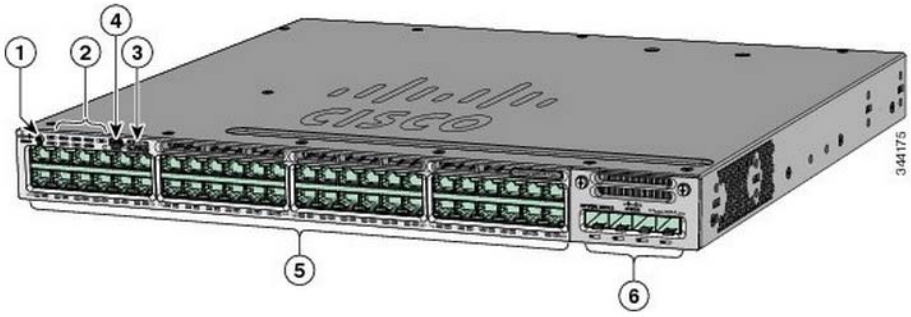


1	Ground connector	5	StackWise port connector
2	CONSOLE (RJ-45 console port)	6	AC OK (input) status LED
3	MGMT (RJ-45 10/100/1000 management port)	7	PS OK (output) status LED
4	Fan module	8	Power supply modules (AC power supply modules shown)

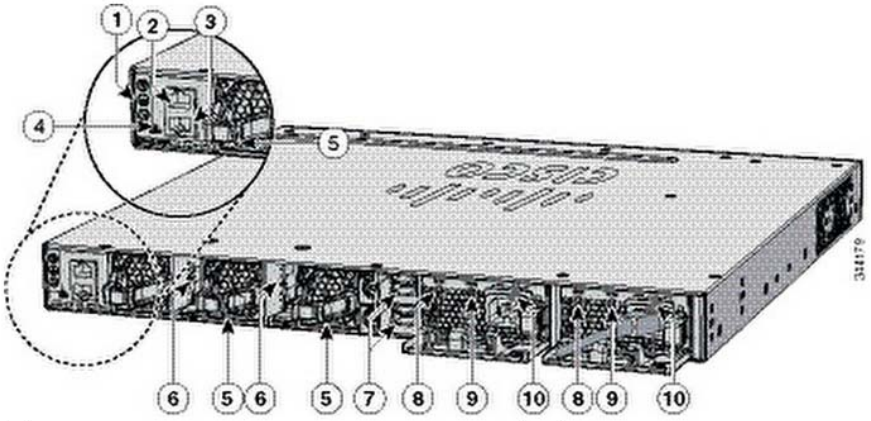
Figure 1 - Catalyst 3650 Front Panel, Rear Panel diagrams

Physical Interface	FIPS 140-2 Logical Interface
10/100/1000 Mbps Ethernet Ports Management port Console port USB port	Data Input Interface
10/100/1000 Mbps Ethernet Ports Management port Console port USB port	Data Output Interface
10/100/1000 Mbps Ethernet Ports Management port Console port Reset switch	Control Input Interface
10/100/1000 Mbps Ethernet Ports Management port Console port USB port LED Displays for system and port status	Status Output Interface
Power/RPS (Redundancy Power Supply) AC/DC Power	Power Interface

Table 2 - Catalyst 3650 Physical Interface/Logical Interface Mapping



1	Mode button	4	USB mini-Type B (console) port
2	Status LEDs	5	10/100/1000 PoE+ ports
3	USB Type A storage port	6	Network module



1	Ground connector	6	StackWise port connector
2	CONSOLE (RJ-45 console port)	7	StackPower connector
3	MGMT (RJ-45 10/100/1000 management port)	8	AC OK (input) status LED
4	RESET button	9	PS OK (output) status LED
5	Fan module	10	Power supply modules (AC power supply modules shown)

Figure 2 - Catalyst 3850 Front Panel, Rear Panel diagrams

Physical Interface	FIPS 140-2 Logical Interface
10/100/1000 Mbps Ethernet Ports FRUlink 1G SFP Ports, FRUlink 10G SFP+ Ports Stack Interfaces Management port Console port USB port	Data Input Interface
10/100/1000 Mbps Ethernet Ports FRUlink 1G SFP Ports, FRUlink 10G SFP+ Ports Stack Interfaces Management port Console port USB port	Data Output Interface
10/100/1000 Mbps Ethernet Ports Management port Stack Interfaces Console port Reset switch	Control Input Interface

Physical Interface	FIPS 140-2 Logical Interface
10/100/1000 Mbps Ethernet Ports FRUlink 1G SFP Ports, FRUlink 10G SFP+ Ports Stack Interfaces Management port Console port USB port LEDs	Status Output Interface
Power/RPS (Redundancy Power Supply) AC/DC Power	Power Interface

Table 3 - Catalyst 3850 Physical Interface/Logical Interface Mapping

2.3 Roles, Services and Authentication

The module supports these four roles:

- AP Role—This role is filled by an access point associated with the controller.
- Client Role—This role is filled by a wireless client associated with the controller.
- User Role—This role performs general security services including cryptographic operations and other approved security functions. The product documentation refers to this role as a management user with read-only privileges.
- Crypto Officer (CO) Role—This role performs the cryptographic initialization and management operations. In particular, it performs the loading of optional certificates and key-pairs and the zeroization of the module. The product documentation refers to this role as a management user with read-write privileges.

Authentication is role-based. Each role is authenticated upon initial access to the module. The module also supports RADIUS or TACACS+ for authentication.

All passwords must be 8 characters up to 25 characters with a minimum of one letter and one number. If six (6) integers, one (1) special character and one (1) alphabet are used without repetition for an eight (8) digit PIN, the probability of randomly guessing the correct sequence is one (1) in 251,596,800 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 10 x9 x 8 x 7 x 6 x 5 x 32 x 52 = 251, 596, 800). Therefore, the associated probability of a successful random attempt is approximately 1 in 251,596,800, which is less than 1 in 1,000,000 required by FIPS 140-2.

When using RSA based authentication, RSA key pair has modulus size of 2048 bit, thus providing 112 bits of strength. Therefore, an attacker would have a 1 in 2^112 chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2.

This Module does not support a Maintenance Role.

User Services

The services available to the User role consist of the following:

Services	Description	CSPs and Access - read (r)/write (w)/delete (d)
System Status	The LEDs show the network activity and overall operational status and the command line status commands output system status.	N/A
TACACS+	User & CO authentication to the module using TACACS+.	User Password – r TACACS+ secret – r
IPSec	Secure communications between controller and RADIUS	skeyid, skeyid_d, IKE session encryption key, IKE session authentication key, ISAKMP preshared, skeyid, skeyid_d, IPSec session encryption key, IPSec session authentication key - r
RADIUS Key Wrap	Establishment and subsequent receive 802.11i PMK from the RADIUS server.	RADIUS secret, RADIUS Key wrap key – r

Table 4 - User Services

Crypto Officer Services

The Crypto Officer services consist of the following:

Services	Description	CSPs and Access – read (r) / write (w) / delete (d)
Self-Test and Initialization	Cryptographic algorithm tests, firmware integrity tests, module initialization.	N/A
System Status	The LEDs show the network activity and overall operational status and the command line status commands output system status.	N/A
TACACS+	User & CO authentication to the module using TACACS+.	User Password – r, w, d TACACS+ secret – r, w, d
IPSec	Secure communications between controller and RADIUS.	skeyid, skeyid_d, IKE session encryption key, IKE session authentication key, ISAKMP preshared, skeyid, skeyid_d, IPSec session encryption key, IPSec session authentication key – r, w, d
Key Management	Key and parameter entry, output, and Zeroization	DH public key, DH private key, SSH RSA public key, SSH RSA private key – r, w, d
TLS	Establishment and subsequent data transfer of a TLS session for use	TLS Server RSA public key, TLS Server RSA private key, TLS pre-master secret,

	between the module and the CO. Protection of syslog messages.	TLS session key – r, w, d
DTLS Data Encrypt	Enabling optional DTLS data path encryption for Office Extended APs.	DTLS Master Secret, CAPWAP session keys, DTLS Session Integrity Keys – r, w, d
RADIUS Key Wrap	Establishment and subsequent receipt of 802.11i PMK from the RADIUS server.	RADIUS secret, RADIUS Key wrap key – r, w, d
SSH	Establishment and subsequent data transfer of a SSH session for use between the module and the CO.	Diffie-Hellman (DH) public key, DH private key, SSH RSA public key, SSH RSA private key – r DH Shared Secret, , SSH session key, SSH session authentication key – r, w, d
SNMPv3	Non-security related monitoring by the CO using SNMPv3	snmpEngineID, SNMPv3 Password, SNMP session key – r, w, d
SESA (Symmetric Early Stacking Authentication)	Setting secure stacking.	SESA Authorization Key, SESA Master Session Key, SESA Derived Session Keys – r, w, d
Module Configuration	Selection of non-cryptographic configuration settings.	N/A
Zeroization	Zeroize cryptographic keys	All Keys and CSPs will be destroyed

Table 5 - Crypto Officer Services

AP and Client Services

The AP and the client services are listed in tables 6 and 7, respectively. Both the roles make use of 802.11i standard.

Services	Description	CSPs and Access – read (r) / write (w) / delete (d)
MFP	Generation and subsequent distribution of MFP key to the AP over a CAPWAP session.	Management Frame Protection (MFP) key – r
802.11i	Establishment and subsequent data transfer of an 802.11i session for use between the client and the access point	802.11i Pairwise Transient Key, 802.11i Pairwise Master Key, 802.11i Temporal Key, 802.11i Group Master Key, 802.11i Group Temporal Key – r, w
RADIUS Key Wrap	Establishment and subsequent receipt of 802.11i PMK from the RADIUS server.	RADIUS secret, RADIUS Key wrap key – r

Table 6 - AP Services

Services	Description	CSPs and Access – read (r) / write (w) / delete (d)
EAP Authenticator	Establishment of EAP-TLS or EAP-FAST based authentication between the client and the Controller.	802.11i Pairwise Transient Key, 802.11i Pairwise Master Key, 802.11i Temporal Key, 802.11i Group Master Key, 802.11i Group Temporal Key – r, w
RADIUS Key Wrap	Establishment and subsequent receipt of 802.11i PMK from the RADIUS server.	RADIUS secret, RADIUS Key wrap key – r

Table 7 – Client Services

2.4 Unauthenticated Services

An unauthenticated operator may observe the System Status by viewing the LEDs on the module, which show network activity and overall operational status. A solid green LED indicates normal operation and the successful completion of self-tests.

2.5 Services Available in a Non-FIPS Mode of Operation

- SSL 3.0
- IPSec/IKE with Diffie-Hellman 768-bit/1024-bit modulus

2.6 Cryptographic Algorithms

The module implements a variety of approved and non-approved algorithms.

Approved Cryptographic Algorithms
The switches support the following FIPS-2 approved algorithm implementations:

Algorithms	IOS Common Cryptographic Module (IC2M)	CiscoSSL FIPS Object Module (Assembler)	(Doppler ASIC)	IOS XE
AES	2817	2685	2879	N/A
CVL	253	N/A	N/A	N/A
DRBG	481	435	N/A	N/A
HMAC	1764	1672	1815	N/A
KBKDF	N/A	N/A	N/A	28
RSA	1471	N/A	N/A	N/A
SHS	2361	2256	2420	N/A
Triple-DES	1688	N/A	N/A	N/A

Table 8 - Algorithm Certificates

Non-FIPS Approved Algorithms Allowed in FIPS Mode

- Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides between 112 and 128 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- AES (Cert. #2817, key wrapping; key establishment methodology provides 128 bits of encryption strength)

Non-FIPS Approved Algorithms

The cryptographic module implements the following non-Approved algorithms:

- MD5
- HMAC-MD5
- RC4

2.7 Cryptographic Key/CSP Management

The module securely administers both cryptographic keys and other critical security parameters such as passwords. All keys are also protected by the password-protection on the CO role login, and can be zeroized by the CO. Keys are exchanged and entered electronically. Persistent keys are entered by the CO via the console port CLI, transient keys are generated or established and stored in DRAM.

Note that the command '**fips zeroize'** will zeroize all Keys/CSPs stored in DRAM. This command essentially results in a device reboot and therefore forces a power cycle, zeroizing all the CSPs/Keys listed below with "Power cycle" in the Zeroization Method column.

Table 8 lists the secret and private cryptographic keys and CSPs used by the module.

ID	Algorithm	Size	Description	Storage	Zeroization Method
General Keys/CSPs					
DRBG V	800-90 CTR_DRBG	128-bits	Generated by entropy source via the CTR_DRBG derivation function. It is stored in DRAM with plaintext form	DRAM (plaintext)	'fips zerozie' command or Power cycle
DRBG key	SP 800-90 CTR_DRBG	256-bits	This is the 256-bit DRBG key used for SP 800-90 CTR_DRBG	DRAM (plaintext)	'fips zerozie' command or Power cycle
DRBG entropy input	SP 800-90 CTR_DRBG	256-bits	HW based entropy source output used to construct seed	DRAM (plaintext)	'fips zerozie' command or Power cycle
DRBG seed	SP 800-90 CTR_DRBG	384-bits	Input to the DRBG that determines the internal state of the DRBG	DRAM (plaintext)	'fips zerozie' command or Power cycle
User password	Password	Variable (8+ characters)	Used to authenticate local users	NVRAM (plaintext)	Zeroized by overwriting with new password

Enable secret	Password	Variable (8+ characters)	Used to authenticate local users at a higher privilege level	NVRAM (plaintext)	Zeroized by overwriting with new password
RADIUS secret	Shared Secret	Variable (8+ characters)	The RADIUS Shared Secret	NVRAM (plaintext)	'# no radius-server key'
RADIUS key wrap key	AES	128 bits	Used to protect SAK	NVRAM (plaintext)	Zeroized by overwriting with new key
TACACS+ secret	Shared Secret	Variable (8+ characters)	The TACACS+ shared secret	NVRAM (plaintext)	'# no tacacs-server key'
Diffie-Hellman public key	DH	2048-4096 bits	The public exponent used in Diffie-Hellman (DH) exchange.	DRAM (plaintext)	'fips zerozie' command or Power cycle
Diffie-Hellman private key	DH	224-379 bits	The private exponent used in Diffie-Hellman (DH) exchange.	DRAM (plaintext)	'fips zerozie' command or Power cycle.
Diffie-Hellman shared secret	DH	2048-4096 bits	This is the shared secret agreed upon as part of DH exchange	DRAM (plaintext)	'fips zerozie' command or Power cycle
SSH					
SSH RSA public key	RSA	2048-3072 bits modulus	SSH public key used in SSH session establishment	DRAM (plaintext)	'fips zerozie' command or Power cycle
SSH RSA private key	RSA	2048-3072 bits modulus	SSH private key used in SSH session establishment	NVRAM (plaintext)	'# crypto key zeroize rsa'
SSH session key	Triple-DES/AES	168-bits/256-bits	This is the SSH session symmetric key.	DRAM (plaintext)	'fips zerozie' command or Power cycle
TLS					
TLS server RSA public key	RSA	2048-3072 bits modulus	RSA public key used in TLS negotiations.	DRAM (plaintext)	'fips zerozie' command or Power cycle
TLS server RSA private key	RSA	2048-3072 bits modulus	Identity certificates for module itself and also used in TLS negotiations.	NVRAM (plaintext)	'# crypto key zeroize rsa'
TLS pre-master secret	Shared Secret	384-bits	Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created.	DRAM (plaintext)	'fips zerozie' command or Power cycle
TLS session key	Triple-DES/AES	168-bits/256-bits	This is the TLS session key	DRAM (plaintext)	'fips zerozie' command or Power cycle

SESA					
SESA authorization key	AES	128 bits	Used to authorize members of a single stack on Incredible Units. Used as input to SP800-108 derivation methods to derive four additional 128 fields to transfer the Master Session Key and additional aggressive exchange material	NVRAM (plaintext)	'no fips authorization-key'
SESA master session Key	AES	128 bits	Used to derive SESA session key	DRAM (plaintext)	'fips zerozie' command or Power cycle
SESA derived session key	AES	128 bits and 192 bits	Used to protect traffic over stacking ports	DRAM (plaintext)	'fips zerozie' command or Power cycle
DTLS					
DTLS master secret	DTLS	384-bits	Generated by approved DRBG for generating the DTLS encryption key	DRAM (plaintext)	'fips zerozie' command or Power cycle
DTLS session encryption/ decryption key (CAPWAP session key)	AES-CBC	128-256 bits	Session Keys used to e/d CAPWAP control messages	DRAM (plaintext)	'fips zerozie' command or Power cycle
DTLS session integrity key	HMAC-SHA1	160 bits	Session keys used for integrity checks on CAPWAP control messages	DRAM (plaintext)	'fips zerozie' command or Power cycle
SNMPv3					
snmpEngine ID	Shared secret	32-bits	Unique string to identify the SNMP engine	NVRAM (plaintext)	'# no snmp-server engineID local engineid-string', overwriitten with new engine ID
SNMPv3 password	shared secret	256 bits	This secret is used to derive HMAC-SHA1 key for SNMPv3 Authentication	DRAM (plaintext)	'fips zerozie' command or Power cycle
SNMPv3 session key	AES	128-bit	Encrypts SNMPv3 traffic	DRAM (plaintext)	P'fips zerozie' command or ower cycle
802.11i					
802.11i Pre-shared Key (PSK)	Shared secret	Variable (8+ characters)	The PSK is used to derive the PMK for 802.11i communications	NVRAM (plaintext)	Zeroized by overwriting with new key
802.11i Pairwise Master Key	HMAC SHA-1	512-bits	The PMK is a secret shared between an 802.11 supplicant and authenticator, and is used to	DRAM (plaintext)	'fips zerozie' command or Power cycle

(PMK)			establish the other 802.11i keys.		
802.11i Pairwise Transient Key (PTK)	AES-CCM	256-bits	The PTK, also known as the CCMP key, is the 802.11i session key for unicast communications.	DRAM (plaintext)	'fips zerozie' command or Power cycle
802.11i Temporal Key (TK)	AES-CCM	128-bits	Encrypt/decrypt unicast traffic	DRAM (plaintext)	'fips zerozie' command or Power cycle
802.11i Group Master Key (GTK)	HMAC SHA-1	256 bits	The secret shared between an 802.11 supplicant and authenticator for broadcast or multicast communications.	DRAM (plaintext)	'fips zerozie' command or Power cycle
802.11i Group Temporal Key (GTK)	AES-CCM	128-bits	802.11i session key for broadcast or multicast traffic	DRAM (plaintext)	'fips zerozie' command or Power cycle
IPSec					
skeyid	Shared Secret	160 bits	Used for key agreement in IKE. This key was derived in the module	DRAM (plaintext)	'fips zerozie' command or Power cycle
skeyid_d	Shared Secret	160 bits	Used for key agreement in IKE	DRAM (plaintext)	'fips zerozie' command or Power cycle
IKE session encryption key	TRIPLE-DES/AES	168-bit TRIPLE-DES or a 256-bit AES	Derived in the module used for IKE payload integrity verification	DRAM (plaintext)	'fips zerozie' command or Power cycle
IKE session authentication key	HMAC-SHA1	160 bits	HMAC-SHA1 key	DRAM (plaintext)	'fips zerozie' command or Power cycle
ISAKMP preshared	pre-shared key	Variable (8+ characters)	This key was configured by CO and used for User role authentication using IKE Pre-shared key based authentication mechanism	NVRAM (plaintext)	'fips zerozie' command or Power cycle
IPSec session encryption key	TRIPLE-DES/AES	168-bit TRIPLE-DES or a 256-bit AES	Derived in the module used for IKE payload integrity verification	DRAM (plaintext)	'fips zerozie' command or Power cycle
IPSec session authentication key	HMAC-SHA1	160 bits	HMAC-SHA1 key	DRAM (plaintext)	'fips zerozie' command or Power cycle

Table 9 - Cryptographic Keys and CSPs

2.8 Self-Tests

The modules include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to insure all components are functioning correctly.

2.7.1 Power-On Self-Tests (POSTs)

- IC2M Algorithm Implementation Known Answer Tests:
  - AES (encrypt/decrypt) KATs
  - AES-GCM KAT
  - DRBG KAT
  - Firmware Integrity Test (RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256)
  - HMAC (SHA-1/256) KATs
  - RSA (sign/verify) KATs
  - Triple-DES (encrypt/decrypt) KATs
- CiscoSSL FIPS Object Module Algorithm Implementation Known Answer Tests:
  - AES (encrypt/decrypt) KATs
  - DRBG KAT
  - HMAC (SHA-1/256) KATs
- Doppler ASIC Hardware Algorithm Implementation Known Answer Tests:
  - AES (encrypt/decrypt) KATs
  - HMAC-SHA1 KAT

2.7.2 Conditional Tests

- Conditional Bypass test
- Conditional Random Number Generation test for approved RNGs
- Conditional Random Number Generation test for non-approved RNG
- Pairwise consistency test for RSA

The devices perform all power-on self-tests automatically at boot. All power-on self-tests must be passed before each role starts to perform services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of the LAN's interfaces; this prevents the AP's from passing any data during a power-on self-test failure.

3 Secure Operation

The switches meet all the overall Level 1 requirements for FIPS 140-2. Follow the setup instructions provided below to place the module in FIPS-approved mode. Operating this Switch without maintaining the following settings will remove the module from the FIPS approved mode of operation.

3.1 System Initialization and Configuration

1. The value of the boot field must be 0x0102. This setting disables break from the console to the ROM monitor and automatically boots. From the "configure terminal" command line, the CO enters the following syntax:

   config-register 0x0F

2. The CO must create the "enable" password for the CO role. Procedurally, the password must be at least 8 characters, including at least one letter and at least one number, and is entered when the CO first engages the "enable" command. The CO enters the following syntax at the "#" prompt:

   Switch(config)# enable secret [PASSWORD]

3. The CO must always assign passwords (of at least 8 characters, including at least one letter and at least one number) to users. Identification and authentication on the console/auxiliary port is required for Users. From the "configure terminal" command line, the CO enters the following syntax:

   Switch(config)# line con 0
   Switch(config)# password [PASSWORD]
   Switch(config)# login local

4. To ensure all FIPS 140-2 logging is received, set the log level:

   Switch(config)# logging console error

5. The CO enables secure stacking (SESA) but configuring the Authorization key:
   Switch(config)# fips authorization-key <128 bit, i.e, 16 hex byte key>

6. The CO may configure the module to use RADIUS or TACACS+ for authentication. If the module is configured to use RADIUS, the Crypto Officer must define RADIUS or shared secret keys that are at least 8 characters long, including at least one letter and at least one number.

7. The CO shall only assign users to a privilege level 1 (the default).

8. The CO shall not assign a command to any privilege level other than its default.