



FIPS 140-2 Security Policy for Cisco Catalyst 6506, 6506-E, 6509, and 6509-E Switches with Wireless Services Modules (WiSMs)

May 3, 2011
Version 2.4

Contents

This security policy contains these sections:

- [Overview, page 2](#)
- [Secure Configuration, page 5](#)
- [Roles, Services, and Authentication, page 9](#)
- [Ports and Interfaces, page 11](#)
- [Cryptographic Key Management, page 12](#)
- [Disallowed Security Functions, page 20](#)
- [Self Tests, page 20](#)
- [Installing the Opacity Shield on Catalyst 6506, 6506-E, 6509 and 6509-E Switches, page 20](#)
- [Physical Security, page 23](#)
- [Mitigation of Attacks, page 26](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 26](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© Cisco Systems, Inc. 2010-2011. May be reproduced only in its original entirety (without revision).

Overview

The Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches together with the Wireless Services Module (WiSM) provide unparalleled security, mobility, redundancy, and ease of use for mission-critical wireless LANs (WLANs). The WiSM works in conjunction with Cisco Aironet® Series lightweight access points operating in CAPWAP mode to deliver a secure and unified wireless solution that supports data, voice, and video applications.

The Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches are multi-chip, standalone cryptographic modules containing WiSM Modules to perform the cryptographic operations and a supervisor blade to manage overall chassis configuration. The module meets all Level 2 FIPS 140-2 requirements and Level 3 requirements for Design Assurance.

The WiSM module in conjunction with Cisco Aironet Series Access Points support Control and Provisioning of Wireless Access Points (CAPWAP) and Wi-Fi Protected Access 2 (WPA2) security. CAPWAP uses DTLS to provide a secure link over which CAPWAP control messages are sent. DTLS is essentially TLS over datagram (UDP) transport. WPA2 is the approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i standard. The WiSM module automatically detects, authorizes and configures access points, setting them up to comply with the centralized security policies of the wireless LAN. In a wireless network operating in this mode, WPA2 protects all wireless communications between the wireless client and other trusted networked devices on the wired network with AES-CCM encryption. CAPWAP protects all control and bridging traffic between trusted network access points and the module with DTLS encryption. In the FIPS mode of operation, the WiSM supports WPA2 (802.11i), HTTPS using TLS, CAPWAP, MFP, RADIUS KeyWrap (using AES Key wrapping), IPSec, Local-EAP, EAP-FAST, TACACS+ and SNMP, and uses the following cryptographic algorithm implementations:

- AES (AES Cert. #1344, key wrapping; key establishment methodology provides 128 bits of encryption strength)
- AES-CBC (firmware)
- AES-ECB (firmware)
- AES-CCM (firmware)
- SHA-1 (firmware)
- HMAC SHA-1 (firmware)
- FIPS 186-2 Random Number Generator (firmware)
- RSA signature generation and verification (firmware)
- RSA (key wrapping; key establishment methodology provides 96 bits of encryption strength)
- TDES (firmware)
- Diffie Hellman key establishment (firmware, key establishment methodology provides 112 bits of encryption strength)
- NDRNG (used to seed the Approved RNG)

HTTPS using TLS uses 1536 bit modulus RSA keys to wrap 128 bit AES symmetric keys, and RADIUS KeyWrap uses 128 bit AES keys as key encrypting keys.

This document details the security policy for the Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches with Wireless Services Modules (WiSMs). This security policy may be freely distributed.

The evaluated platform consists of the following:

- Chassis Hardware Version
 - Catalyst 6506 switch

- Catalyst 6506-E switch
- Catalyst 6509 switch
- Catalyst 6509-E switch
- Backplane Hardware Version
 - WS-C6506-E
 - WS-C6509-E
 - WS-C6506
 - WS-C6509
- FIPS Kit (includes opacity shield and tamper labels)
 - P/N 800-27009 (Catalyst 6506 and Catalyst 6506-E switch chassis)
 - P/N 800-26335 (Catalyst 6509 and Catalyst 6509-E switch chassis)
- Supervisor Blade Hardware Version
 - WS-SUP720-3BXL
 - WS-SUP720-3B
- Supervisor Blade Firmware Version
 - Cisco IOS Release 12.2.33-SXI3
 - Cisco IOS Release 12.2.33-SXH5
- WiSM Module Hardware Version WS-SVC-WISM-1-K9
- WiSM Module Firmware Version 7.0.98.0, 7.0.98.213, or 7.0.116.0

This security policy describes how the listed Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches with WiSM Modules meet the security requirements of FIPS 140-2, and describes how to operate the hardware devices in a secure FIPS 140-2 mode. The addition of any component not addressed by this FIPS 140-2 validation and not included in the boundary definition is considered out of scope and may affect the correct operation of the module. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the listed Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches with Wireless Services Modules (WiSMs). This Security Policy document is non-proprietary and can be freely distributed.

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 this URL:

<http://csrc.nist.gov/cryptval/>

Cisco Catalyst 6506, 6506-E, 6509, and 6509-E Switches with WiSM Cryptographic Modules

The cryptographic boundary is defined as encompassing the following:

- The entire outer enclosure of the chassis
- Four WiSM Modules
- One Supervisor Blade (either a SUP720-3B or a SUP720-3BXL)
- Opacity shield

- Slot covers

Figure 1 and Figure 2 below show the cryptographic boundary as the dark border around the module. The service modules require that a special opacity shield be installed over the intake-side air vents to operate in FIPS-approved mode. The shield decreases the surface area of the vent holes, reducing visibility within the cryptographic boundary to FIPS-approved specifications. The tamper-evident seals and opacity shield included in the FIPS Kit shall be installed for the module to operate in a FIPS Approved mode of operation. Detailed installation instructions for the opacity shield and the application of the tamper evident seals are provided in this publication.

Figure 1 *Cryptographic Boundary on Catalyst 6506 and Catalyst 6506E Switches*

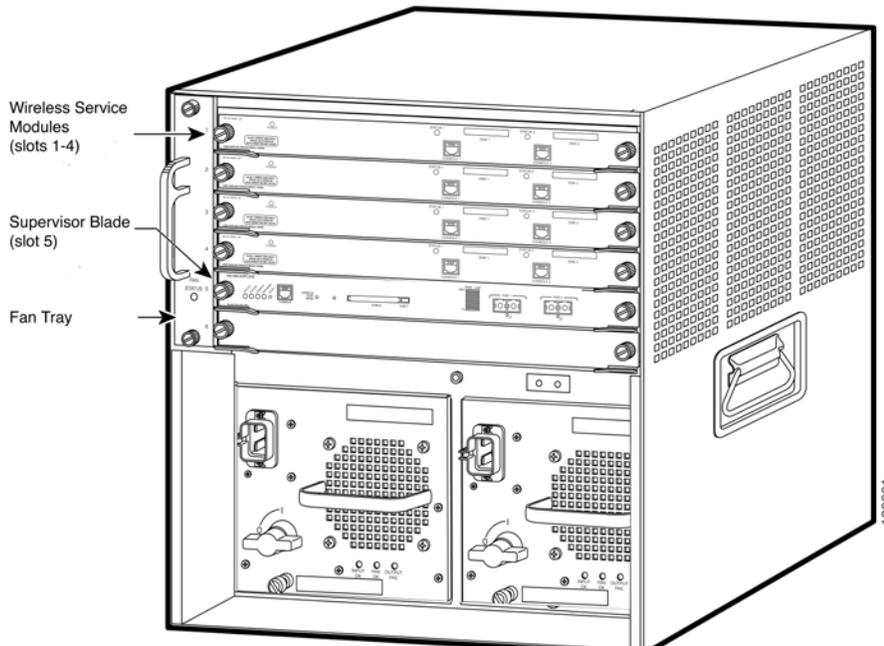
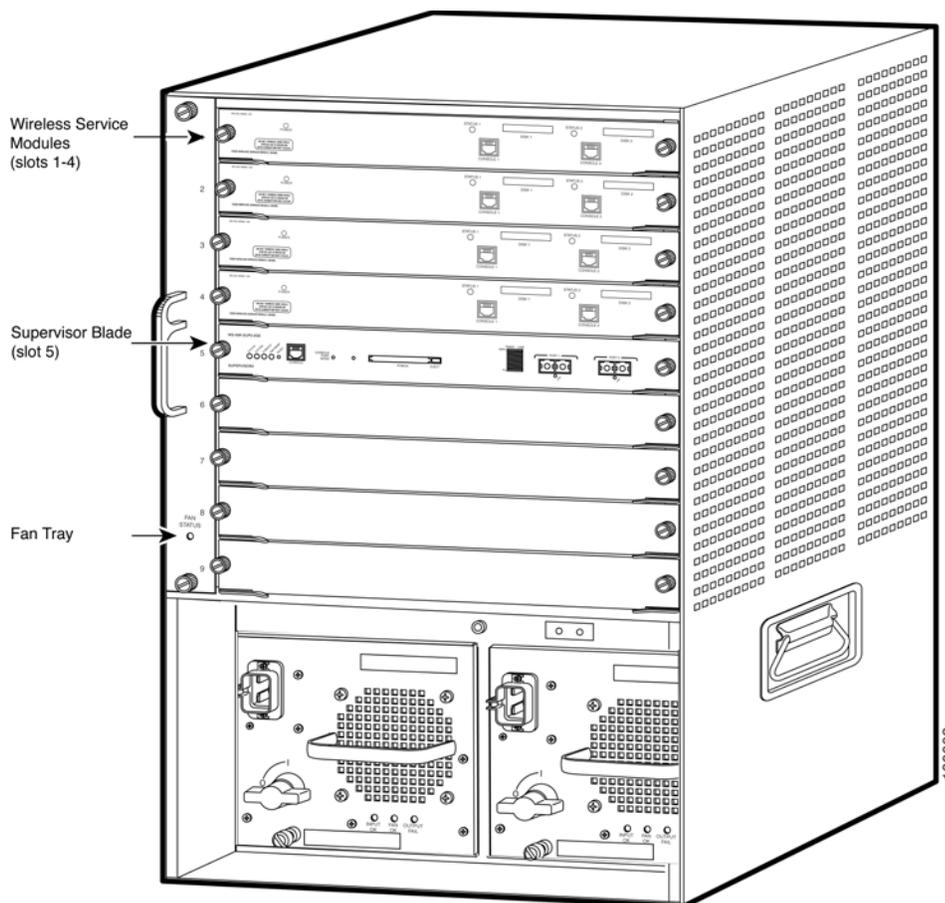


Figure 2 Cryptographic Boundary on Catalyst 6509 and Catalyst 6509E Switches



Secure Configuration

The initial configuration of the Supervisor card is accomplished by creating a VLAN that defines the connection between the Supervisor card and the WiSM card and by creating authentication data as explained in the Configure Supervisor Authentication Data section.

The initial configuration of the WiSM is performed through the local access of CLI of the Supervisor and by initiating a session from the supervisor CLI to each of the controllers in the WiSM. The rest of the configuration shall be performed over a local link through the console connection of each of the controllers in the WiSM. After the first three steps below, remote access through HTTPS may be used for subsequent configuration. For connecting using HTTPS, the Crypto Officer shall configure their web browsers so that only TLS v1.0 is used. The HTTPS client must be configured to use AES_128_CBC_SHA based cipher suites.

Only the 7.0.98.0, 7.0.98.213, or 7.0.116.0 CAPWAP firmware release may be contained on the wireless LAN controllers for distribution to access points.

Configure Supervisor Authentication Data

The Supervisor crypto officer (this role is defined in the Roles, Services and Authentication section) must create the enable password for the supervisor crypto officer role. The password must be at least eight characters (all digits, all lower and uppercase letters, and all special characters except '?' are accepted) and is entered when the crypto officer first engages the **enable** command. The crypto officer enters the following syntax at the # prompt:

```
# enable secret password
```

The crypto officer must always assign passwords (of at least eight characters) to users. Enter this command to set user passwords:

```
# username name password password
```

Follow these steps on each WiSM controller to securely configure the module:

1. [Enable FIPS Mode of Operations](#)
2. [Disable Boot Break](#)
3. [Configure HTTPS Certificate](#)
4. [Configure WiSM Authentication Data](#)
5. [Configure Communications with RADIUS](#)
6. [Configure Pre-shared Keys for 802.11i](#)
7. [Configure Ciphersuites for 802.11i](#)
8. [Configure SNMP](#)
9. [Configure TACACS+ secret](#)
10. [Configure MFP \(Management Frame Protection\)](#)
11. [Configure Local EAP](#)
12. [Configure EAP-FAST](#)
13. [Configure EAP-TLS](#)
14. [Save and Reboot](#)

Enable FIPS Mode of Operations

The following CLI command places the controller in the WiSM in FIPS mode of operations, enabling all necessary self tests and algorithm restrictions:

```
> config switchconfig fips-prerequisite enable
```

Disable Boot Break

The following CLI command prevents breaking out of the boot process. It must be executed after enabling FIPS mode of operations.

```
> config switchconfig boot-break disable
```

Configure HTTPS Certificate

The following command configures the controller in the module to use the manufacture-installed Cisco device certificate for the HTTPS server. It must be executed after enabling FIPS mode of operations:

```
> config certificate use-device-certificate webadmin
```

Configure WiSM Authentication Data

All users shall have a password containing 8 or more characters, including numbers and letters. A crypto officer can use the following CLI command to set user passwords:

```
>config mgmtuser password username password
```

Note that this and all subsequent configuration steps may also be performed through HTTPS. However, only the CLI commands are included in this document.

Configure Communications with RADIUS

Communications between the controller and RADIUS may be configured for RADIUS KeyWrap or IPSec.

RADIUS KeyWrap and MACK Keys

The following CLI commands configure the RADIUS secret and AES-key wrap KEK and MACK:

```
> config radius auth add index ip-address port hex secret
> config radius auth keywrap add hex kek mack index
> config radius auth keywrap enable
```

IPSec

Optionally, the controller may be configured to communicate with RADIUS via IPSec. Refer to the document at the following link for additional instructions:

http://www.cisco.com/en/US/products/ps6366/products_tech_note09186a0080a829b8.shtml

Configure Pre-shared Keys for 802.11i

WPA2 Pre-shared key (WPA2-PSK) is an optional mode permitted by this security policy. Generation of pre-shared keys is outside the scope of this security policy, but you should entered them as 64 hexadecimal values (256 bits) using the following command syntax:

```
> config wlan security wpa akm psk set-key hex key index
> config wlan security wpa akm psk enable index
```

Configure Ciphersuites for 802.11i

The following CLI commands create a wireless LAN, configure it to use WPA2, associate it with a RADIUS server, and enable it:

```
> config wlan create index profile_name ssid
> config wlan radius_server auth add index radius-server-index
> config wlan enable index
```

Configure SNMP

Non-security related remote monitoring and management of the Controllers can be done via SNMP. Only SNMPv3 with HMAC-SHA-1 is permitted by this security policy. The user passwords shall be selected to be 8 or more characters, including numbers and letters.

The following CLI commands enable SNMPv3 with HMAC-SHA1:

```
> config snmp version v1 disable
> config snmp version v2c disable
> config snmp version v3 enable
> config snmp v3user create username [ro|rw] hmacsha [none|des] authkey encryptkey
```

Configure TACACS+ secret

The crypto officer may configure the module to use TACACS+ for authentication, authorization and accounting. Configuring the module to use TACACS+ is optional. If the module is configured to use TACACS+, the Crypto-Officer must define TACACS+ shared secret keys that are at least 8 characters long. The following CLI command configures TACACS+ for authentication (auth), authorization (athr) and accounting (acct):

```
> config tacacs [auth | athr | acct] add index ip port [ascii | hex] secret
```

Refer to the Cisco Wireless LAN Controller Configuration Guide for additional instructions.

Configure MFP (Management Frame Protection)

Infrastructure MFP enables one access point to validate a neighboring access point's management frames. Configuring the module to use MFP is optional. The following CLI command is used to enable infrastructure MFP:

```
> config wps mfp infrastructure enable
```

Client MFP is used to encrypt and sign management frames between the AP and the client. The following CLI command is used to enable client MFP:

```
> config wlan mfp client enable index required
```

Refer to the Cisco Wireless LAN Controller Configuration Guide for additional instructions.

Configure Local EAP

The module can be optionally configured as a local EAP authentication server to authenticate wireless clients. Both EAP-TLS and EAP-FAST are supported and permitted by this security policy.

Refer to the Cisco Wireless LAN Controller Configuration Guide for instructions on configuring the Local EAP server to authenticate wireless clients without a RADIUS server.

Configure EAP-FAST

EAP-FAST is an Extensible Authentication protocol and can be used as an authentication method between the Controller and the wireless client. When a RADIUS server is used to authenticate clients, no extra EAP-FAST configuration is required.

The following CLI command is used by the crypto officer to enter a new EAP-FAST server key, where hex-key can be up to 32 hex digits or 16 bytes.

```
>config local-auth method fast server-key hex-key
```

Refer to the Cisco Wireless LAN Controller Configuration Guide for instructions on configuring Local EAP server with EAP-FAST as the authentication method for the wireless clients.

Configure EAP-TLS

EAP-TLS is an Extensible Authentication protocol and can be used as an authentication method between the Controller and the wireless client. It requires configuration based on certificates issued from a PKI. Refer to the *Cisco EAP-TLS Deployment Guide for Wireless LAN Networks* configuration instructions to use EAP-TLS as the authentication method for the wireless clients.

Click this URL for an example configuration:

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a0080851b42.shtml

Save and Reboot

After executing the above commands, you must save the configuration and reboot the system:

```
> save config
> reset system
```

Roles, Services, and Authentication

This section describes the roles, services, and authentication types in the security policy.

Roles

The module supports these six roles:

- AP Role—This role is filled by an access point associated with the controller in the WiSM.

- Client Role—This role is filled by a wireless client associated with the controller in the WiSM.
- 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 Crypto Officer must maintain security and control at all times of any unused tamper-evident labels. The product documentation refers to this role as a management user with read-write privileges.
- Supervisor Crypto Officer (CO) Role—This role performs the initial WiSM configuration by initiating a session to the WiSM through the local access of the switch (Supervisor) CLI. The Supervisor CO can zeroize the user passwords stored in the supervisor blade.
- Supervisor User Role—This role can perform basic supervisor user services and can view the status of the WiSM configuration from the Supervisor CLI by issuing the show commands.

The module does not support a maintenance role.

Services

The services provided are summarized in [Table 1](#).

Table 1 *Module Services*

Service	Role	Purpose
Self Test and Initialization	Any role except AP and Client role	Cryptographic algorithm tests, firmware integrity tests, module initialization.
System Status	Any role except AP and Client role	The LEDs show the network activity and overall operational status, and the command-line status commands output system status.
Key Management	CO	Key and parameter entry, key zeroization.
Module Configuration	CO, Supervisor CO	Selection of non-cryptographic configuration settings.
Supervisor Authentication data Zeroization	Supervisor CO	Supervisor User passwords zeroization.
SNMPv3	CO	Non security-related monitoring by the CO using SNMPv3.
TACACS+	CO, User	User and CO Authentication to the module using TACACS+
IPSec	CO, User	Secure communication between the controller and RADIUS.
CAPWAP	AP	Establishment and subsequent data transfer of a CAPWAP session for use between the module and an AP ¹ .
MFP	AP	Generation and subsequent distribution of MFP key to the AP over a CAPWAP session.

Table 1 **Module Services (continued)**

Service	Role	Purpose
TLS	CO	Establishment and subsequent data transfer of a TLS session for use between the module and the CO.
Local EAP Authenticator	Client	Establishment of EAP-TLS or EAP-FAST based authentication between the client and the Controller in the WiSM.
802.11i	AP	Establishment and subsequent data transfer of an 802.11i context for use between the client and the access point.
RADIUS KeyWrap	CO, User	Establishment and subsequent receive 802.11i PMK from the RADIUS server.

1. CAPWAP uses RSA key wrapping which provides 96 bits of effective symmetric key strength.

An unauthenticated operator may observe the System Status by viewing the LEDs on the module which show network activity and overall operational status. The module does not support a bypass capability in the approved mode of operations. The only services available to an unauthenticated user are Self Test and Initialization (by power cycling the unit) and viewing System Status (by observing the LEDs).

Ports and Interfaces

The Cisco Catalyst series switch module has the following physical ports and interfaces:

- 1 console port on the Supervisor front panel
- 2 console ports on each front panel of the WiSMs
- 2 Gigabit Ethernet ports on the Supervisor front panel
- 1 10/100/1000 Ethernet port on the Supervisor front panel
- Power, status LEDs on the WiSM and Disk, Link and Status LEDs on the Supervisor

Supervisor User and Supervisor CO Authentication

When a Supervisor User tries to connect to the CLI of the Supervisor via the Console port, the module prompts the Supervisor User to enter a password. The Supervisor User is authenticated based on the password provided. Once the user has been authenticated, the module provides a basic set of services to that user.

The Supervisor Crypto Officer must first assume the Supervisor User role and then enter the "enable" command. The Supervisor CO will be prompted to enter another password in order to receive additional services that are reserved for the Supervisor Crypto Officer. The Supervisor CO will be authenticated if a correct password is provided to the module.

User and CO Authentication

When a user first connects to the controllers in the WiSM module through the console ports, the module prompts the user to enter a username and password. The user is authenticated based on the password provided. Once the user has been authenticated, the module provides services based on whether they have read-only privileges (the User role) or read-write privileges (the CO role).

The "*" characters are used to mask the password when the users authenticate. If the incorrect password is entered, the module will re-prompt the user to login.

After the module power cycles, a user must reauthenticate.

The module supports password based local authentication for access via the CLI or HTTPS, as well as remote authentication using RADIUS and TACACS+. The module also supports non-crypto related remote access via the SNMPv3. RADIUS, TACACS+ and SNMPv3 may be used in the FIPS mode.

The security policy stipulates that all user passwords must be 8 alphanumeric characters, so the password space is 2.8 trillion possible passwords (for a character set of 36). The possibility of randomly guessing a password is thus far less than one in one million. To exceed a one in 100,000 probability of a successful random password guess in one minute, an attacker would have to be capable of 28 million password attempts per minute, which far exceeds the operational capabilities of the module to support.

AP Authentication

Each controller of the WiSM module in the Cisco Catalyst series switch performs mutual authentication with an access point through the CAPWAP protocol, using an RSA key pair with 1536 bit modulus, which has an equivalent symmetric key strength of 96 bits. An attacker would have a 1 in 2^{96} chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 7.9×10^{23} attempts per minute, which far exceeds the operational capabilities of the module to support.

Client Authentication

The module performs mutual authentication with a wireless client through EAP-TLS or EAP-FAST protocols. EAP-FAST is based on EAP-TLS and uses EAP-TLS key pair and certificates. The RSA key pair for the EAP-TLS credentials has modulus size of 1024 bit to 2048 bit, thus providing between 80 bits and 112 bits of strength. Assuming the low end of that range, an attacker would have a 1 in 2^{80} chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 1.8×10^{21} attempts per minute, which far exceeds the operational capabilities of the modules to support.

Cryptographic Key Management

Cryptographic keys are stored in plaintext form in flash for long term storage and in SDRAM (for active keys) of the controllers in the WiSM module. The AES key wrap KEK, AES key wrap MAC keys and the Pre shared key (PSK) are input by the CO in plaintext over a local console connection or in encrypted form when sent over the TLS session. The PMK is input from the RADIUS server encrypted with the AES key wrap protocol or via IPSec. RSA public keys are output in plaintext in the form of X.509 certificates.

The DTLS (CAPWAP) pre-master key is output wrapped with the AP's RSA key, and the MFP MIC key and 802.11i PTK, 802.11i GTK are output encrypted with the DTLS (CAPWAP) encryption key. PAC key is output wrapped with the Client's RSA key. Asymmetric key establishment (RSA key transport) is used in the creation of session keys during EAP-TLS and EAP-FAST. Any keys not explicitly mentioned are not input or output.

[Table 2](#) lists the secret and private cryptographic keys and CSPs used by the module. [Table 3](#) lists the public keys used by the module. [Table 4](#) lists the access to the keys by service.

The module uses RSA key wrapping with 1536 bit modulus and provides 96 bits of encryption strength in key establishment.

Table 2 Secret and Private Cryptographic Keys and CSPs

Name	Algorithm	Storage	Description
PRNG seed key	FIPS 186-2	Flash	This is the seed key for the PRNG. It is statically stored in the code.
PRNG seed	FIPS 186-2	SDRAM	This is the seed for the PRNG. It is generated using an un-approved RNG based on the controller's /dev/urandom device.
User Password	Shared secret	Flash	Identity based authentication data for a user.
SNMPv3 user password	Shared secret	Flash	This secret is used to derive HMAC-SHA1 key for SNMPv3 authentication.
Supervisor user password	Shared secret	Supervisor NVRAM	The plaintext password for the Supervisor User.
Enable password	Shared secret	Supervisor NVRAM	The plaintext password for the Supervisor Crypto Officer.
TACACS+ authentication secret	Shared secret	Flash	This TACACS+ shared secret is used to obfuscate the Crypto-Officer's authentication requests and responses between the module and the TACACS+ server. Entered by the Crypto-Officer in plaintext form and stored in plaintext form. Note that encryption algorithm is not FIPS compliant and the Crypto-Officer must ensure a strong user password.
TACACS+ authorization secret	Shared secret	Flash	This TACACS+ shared secret is used to obfuscate the Crypto-Officers' operation's authorization requests and responses between the module and the TACACS+ server. Entered by the Crypto-Officer in plaintext form and stored in plaintext form. Note that encryption algorithm is not FIPS compliant.

Table 2 Secret and Private Cryptographic Keys and CSPs (continued)

Name	Algorithm	Storage	Description
TACACS+ accounting secret	Shared secret	Flash	This TACACS+ shared secret is used to obfuscate accounting requests and responses between the module and the TACACS+ server. Entered by the Crypto-Officer in plaintext form and stored in plaintext form. Note that encryption algorithm is not FIPS compliant.
bsnOldDefaultIdCert	RSA	Flash	1536-bit RSA private key used to authenticate to the access point, generated during the manufacturing process.
bsnDefaultIdCert	RSA	Flash	1536-bit RSA private key, not used in FIPS mode.
bsnSslWebadminCert	RSA	Flash	1536-bit RSA private key used for HTTPS-TLS, generated during the manufacturing process.
bsnSslWebauthCert	RSA	Flash	1024-bit RSA private key, not used in FIPS mode.
VendorDeviceCert	RSA	Flash	Certificate to authenticate controller to EAP clients during EAP authentication. It may be used in EAP-TLS or EAP-FAST authentication method.
Pre-shared key (PSK)	Shared secret	Flash	The 802.11i preshared key (PSK). This key is optionally used as a PMK.
HTTPS TLS Pre-Master Secret	Shared secret	SDRAM	Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created.
HTTPS TLS Encryption Key	AES-CBC	SDRAM	128-bit AES key used to encrypt session data.
HTTPS TLS Integrity Key	HMAC- SHA-1	SDRAM	HMAC-SHA-1 key used for HTTPS integrity protection.
DTLS Pre-Master Secret	Shared secret	SDRAM	Shared secret generated by an AP and entered wrapped by the AP's RSA key. Used to derive the DTLS Master Secret.
DTLS Master Key	Shared secret	SDRAM	Used to create the DTLS Encryption and Integrity Keys
DTLS Encryption Key (CAPWAP Session Key)	AES-CBC	SDRAM	Session key used to encrypt and decrypt CAPWAP control messages.
DTLS Integrity Key	HMAC- SHA-1	SDRAM	Session key used for integrity checks on CAPWAP control messages.
AAA Shared Secret	TDES	Flash	Used to derive IPsec encryption keys and IPsec HMAC keys.

Table 2 Secret and Private Cryptographic Keys and CSPs (continued)

Name	Algorithm	Storage	Description
RadiusOverIPSec EncryptionKey	TDES	SDRAM	TDES encryption/decryption key, used in IPSec tunnel between module and RADIUS to encrypt/decrypt EAP keys.
RadiusOverIPSec IntegrityKey	HMAC	SDRAM	Integrity/authentication key, used in IPSec tunnel between module and RADIUS.
Infrastructure MFP MIC Key	AES-CMAC	Flash	This 128-bit AES key is generated in the controller using FIPS 186-2 approved RNG. This key is sent to the AP encrypted with the DTLS Encryption Key. This key is used by AP to sign management frames when infrastructure MFP is enabled.
802.11i Pairwise Master Key (PMK)	Shared secret	SDRAM	The PMK is a secret shared between an 802.11 supplicant and authenticator, and is used to establish the other 802.11i keys.
802.11i Key Confirmation Key (KCK)	HMAC- SHA-1	SDRAM	The KCK is used by IEEE 802.11i to provide data origin authenticity in the 4-Way Handshake and Group Key Handshake messages.
802.11i Key Encryption Key (KEK)	AES-KeyWrap	SDRAM	The KEK is used by the EAPOL-Key frames to provide confidentiality in the 4-Way Handshake and Group Key Handshake messages.
802.11i Pairwise Transient Key (PTK)	AES-CCM	SDRAM	The PTK, also known as the CCMP Key, is the 802.11i session key for unicast communications.
802.11i Temporal Key (TK)	AES-CCM	SDRAM	AES-CCM key used in 802.11i unicast communications.
802.11i Group Temporal Key (GTK)	AES-CCM	SDRAM	The GTK is the 802.11i session key for broadcast communications.
RADIUS AES KeyWrap KEK	AES-KeyWrap	Flash	The key encrypting key used by the AES Key Wrap algorithm to protect the PMK for the 802.11i protocol.
RADIUS AES KeyWrap MACK	AES-KeyWrap	Flash	The MAC key used by the AES Key Wrap algorithm to authenticate RADIUS conversation.
EAP-TLS Pre-Master Secret	Shared secret	SDRAM	Shared secret created using asymmetric cryptography from which new EAP-TLS session keys can be created.
EAP-TLS Encryption Key	AES-CBC	SDRAM	AES key used to encrypt EAP-TLS session data.
EAP-TLS Integrity Key	HMAC- SHA-1	SDRAM	HMAC-SHA-1 key used for EAP-TLS integrity protection.

Table 2 Secret and Private Cryptographic Keys and CSPs (continued)

Name	Algorithm	Storage	Description
EAP-TLS Peer Encryption Key	Shared Secret	SDRAM	This 32-byte key is master session key of the EAP-TLS authentication algorithm. It is the PMK for 802.11i.
EAP-FAST Server Key	AES-CCM	Flash	EAP-FAST server master key to generate client protected access credential (PAC).
EAP-FAST PAC-Key	Shared Secret	SDRAM	Shared secret between the local EAP authenticator and the wireless client. For EAP-FAST authentication. It is created by PRNG and is used to derive EAP-FAST tunnel master secret.
EAP-FAST tunnel master secret	Shared Secret	SDRAM	This is the master secret for EAP-FAST. It is used to derive EAP-FAST Encryption key, EAP-FAST Integrity key, EAP-FAST Session Key Seed.
EAP-FAST Encryption Key	AES-CBC	SDRAM	Encryption Key for EAP-FAST tunnel.
EAP-FAST Integrity Key	HMAC- SHA-1	SDRAM	Integrity Key for EAP-FAST tunnel.
EAP-FAST Session-Key Seed	Shared Secret	SDRAM	This secret is used to derive the EAP-FAST master session key by mixing with the EAP-FAST Inner Method Session Key.
EAP-FAST Inner Method Session Key	Shared Secret	SDRAM	This 32-byte key is the session key generated by the EAP handshake inside the EAP-FAST tunnel.
EAP-FAST Master Session Key	Shared Secret	SDRAM	This 64-byte key is the session key generated by the EAP-FAST authentication method. It is then used as PMK for 802.11i.

Table 3 Public Keys

Name	Algorithm	Storage	Description
bsnOldDefaultCaCert	RSA	Flash	Verification certificate, used for CAPWAP authentication.
bsnDefaultRootCaCert	RSA	Flash	Verification certificate, used for CAPWAP authentication.
bsnDefaultCaCert	RSA	Flash	Verification certificate, used for CAPWAP authentication.
bsnDefaultBuildCert	RSA	Flash	Verification certificate, used to validate the controller's firmware image.
cscDefaultNewRootCaCert	RSA	Flash	Verification certificate, not used in FIPS mode of operations.

Table 3 *Public Keys (continued)*

Name	Algorithm	Storage	Description
cscDefaultMfgCaCert	RSA	Flash	Verification certificate, used with CAPWAP to authenticate the access point.
cscDefaultDevCaCert	RSA	Flash	Verification certificate, used with CAPWAP to authenticate the access point.
cscDefaultR3CaCert	RSA	Flash	Verification certificate, not used in FIPS mode of operations.
bsnOldDefaultIdCert	RSA	Flash	Authentication certificate, used to authenticate to the access point.
bsnSslWebadminCert	RSA	Flash	Server certificate used for HTTPS-TLS.
VendorCACert	RSA	Flash	Certificate to validate wireless client certificates during EAP authentication. It may be used in EAP-TLS or EAP-FAST authentication method.

Table 4 *Key/CSP Access by Service*

Service	Key Access
Self Test and Initialization	<ul style="list-style-type: none"> Initializes PRNG seed
System Status	<ul style="list-style-type: none"> None
Key Management	<ul style="list-style-type: none"> Read/Write AAA Shared Secret, PSK, RADIUS AES KeyWrap KEK, RADIUS AES KeyWrap MACK, EAP-FAST Server Key Destroy all keys (with Key Zeroization command)
Module Configuration	<ul style="list-style-type: none"> Modify user passwords Modify TACACS+ shared secret
Supervisor Authentication Data Zeroization	<ul style="list-style-type: none"> Supervisor user passwords
SNMPv3	<ul style="list-style-type: none"> Authenticate using SNMPv3 user password
TACACS+	<ul style="list-style-type: none"> Authenticate, authorize and accounting using TACACS+ shared secrets
IPSec	<ul style="list-style-type: none"> Use AAA Shared Secret, RadiusOverIPSecEncryptionKey, RadiusOverIPSecIntegrityKey
CAPWAP	<ul style="list-style-type: none"> Verify with cscDefaultNewRootCaCert and cscDefaultMfgCaCert Sign with bsnOldDefaultIdCert Private Key Read (and transmit) bsnOldDefaultCert Certificate Establish and then encrypt/decrypt with CAPWAP Session Key

Table 4 **Key/CSP Access by Service**

Service	Key Access
MFP	<ul style="list-style-type: none"> • Derive Infrastructure MFP MIC key from PRNG and distribute to connected access points
HTTPS TLS	<ul style="list-style-type: none"> • Sign with bsnSslWebadminCert Private Key • Read (and transmit) bsnSslWebadminCert Public Key • Establish TLS Pre-Master Key • Establish and then perform cryptographic operations with TLS Encryption Key and TLS Integrity Key
Local EAP Authenticator (EAP-TLS)	<ul style="list-style-type: none"> • Sign with VendorDeviceCert Private Key • Read (and transmit) VendorCACert • Establish EAP-TLS tunnel Pre-master secret • Derives EAP-TLS Master secret and tunnel encryption & integrity keys • Derives EAP-TLS peer encryption Key

Table 4 Key/CSP Access by Service

Service	Key Access
Local EAP Authenticator (EAP-FAST)	<p>In-band PAC Provisioning without certificates:</p> <ul style="list-style-type: none"> Establish EAP-TLS pre-master secret using anonymous Diffie Hellman key exchange Derive EAP-TLS master secret and EAP-TLS tunnel encryption and integrity keys Read EAP-FAST Server Key and generate EAP-FAST PAC-Key for the client <p>In-band PAC Provisioning with certificates:</p> <ul style="list-style-type: none"> Sign with VendorDeviceCert Private Key Read (and transmit) VendorCACert Read and verify Client certificate Establish EAP-TLS pre-master secret using authenticated Diffie Hellman key exchange Derive EAP-TLS master secret and EAP-TLS tunnel encryption and integrity keys Read EAP-FAST Server Key and generate EAP-FAST PAC-Key for the client <p>EAP-FAST Tunnel Establishment:</p> <ul style="list-style-type: none"> Read EAP-FAST Server Key Decrypt client PAC to recover client EAP-FAST PAC-Key Derive EAP-FAST Master secret and tunnel encryption/integrity keys and EAP-FAST Session-Key Seed. <p>Authentication:</p> <ul style="list-style-type: none"> Derive EAP-FAST Inner Method Session Key according to the inner EAP algorithm Derive EAP-FAST Master Session Key using the Session-Key Seed and Inner Method Session Key(s)
802.11i	<ul style="list-style-type: none"> Compute 802.11i KCK, 802.11i KEK, 80211.i TK, and 802.11i PTK from 802.11i PMK or 802.11i PSK Generate 802.11i GTK Encrypt/decrypt using 802.11i KEK Authenticate data using 802.11i KCK
RADIUS	<ul style="list-style-type: none"> Decrypt 802.11i PMK using KeyWrap KEK Authenticate data using KeyWrap MACK

Key Establishment

The module uses RSA key wrapping which provides 96 bits of effective key strength to establish 128-bit AES keys for DTLS. Keys are output from the module encrypted with the DTLS Encryption Key.

Key Zeroization

All keys in the WiSM controllers can be zeroized by entering this CLI command from a PC connected to the console port:

```
> config switchconfig key-zeroize controller
```

After you enter the command, power cycle the module and hold down the **Esc** key to initiate a memory test that clears residual keys from the RAM.

Disallowed Security Functions

These cryptographic algorithms are not approved and may not be used in FIPS mode of operations:

- RC4
- MD5 (MD5 is allowed for use in DTLS)
- HMAC MD5
- AES-CTR (non-compliant)
- CCKM

Self Tests

The following self tests are performed by the module:

- Firmware integrity test on the IOS and CAPWAP firmware.
- Power on self test of AES-ECB, AES-CCM, SHA-1, HMAC SHA-1, RNG, TDES, EAP-FAST KDF, and RSA algorithms.
- Continuous random number generator test for Approved and non-Approved RNGs.

Self Tests are performed automatically when power is applied to the module. Self Tests may be run on-demand at any time by cycling power to the module.

Installing the Opacity Shield on Catalyst 6506, 6506-E, 6509 and 6509-E Switches

The Catalyst 6500 series opacity shield is designed to be installed while the system is operating without creating an electrical hazard or damage to the system. You will need some clearance between adjacent racks in order to perform this procedure. This procedure is applicable to the following Catalyst 6500 series switches:

- Catalyst 6506 switch
- Catalyst 6506-E switch
- Catalyst 6509 switch
- Catalyst 6509-E switch

**Note**

To operate in FIPS Approved mode the physical security devices shall be installed as indicated.

Follow these steps to install an opacity shield on the Catalyst 6506, 6506-E, 6509 and 6509-E Switches:

- Step 1** The opacity shield is designed to be installed on a Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switch chassis that is already rack-mounted. If your Catalyst 6500 series switch chassis is not rack-mounted, install the chassis in the rack using the procedures contained in the *Catalyst 6500 Series Switches Installation Guide*. If your Catalyst 6500 series switch chassis is already rack-mounted, proceed to [Step 2](#).
- Step 2** Open the FIPS kit packaging. The kit contains the following items:
- A packaged opacity shield assembly with installation hardware for the Catalyst 6506 and Catalyst 6506-E switch chassis (part number 800-27009).
 - A packaged opacity shield assembly with installation hardware for the Catalyst 6509 and Catalyst 6509-E switch chassis (part number 800-26335).
 - An envelope with 60 FIPS tamper-evidence labels.
 - An envelope containing a disposable ESD wrist strap.
- Step 3** Select the appropriate opacity shield kit for your system and set the other opacity shield kit aside.
- Step 4** Open the protective packaging and remove the opacity shield and the two bags of installation hardware. The bag with the part number 69-1482 contains the installation hardware for non-E chassis; the other bag (part number 69-1497) contains the installation hardware for -E chassis. Select the bag of installation hardware appropriate for your installation. Set the second bag of fasteners aside; you will not need them for this installation.
- Step 5** Open the bag of installation hardware and remove the following items:
- (Bag with part number 69-1482)—Two M3 thumbscrews, four M3 snap rivet fasteners. The snap rivet fasteners come assembled; you need to separate the two pieces of the snap rivet fastener by removing the snap rivet pin from the snap rivet sleeve before you install them in the opacity shield.
 - (Bag with part number 69-1497)—Two M4 thumbscrews, four M4 snap rivet fastener sleeves, and four M4 snap rivet pins.
- Step 6** Start the two thumbscrews in the corresponding threaded holes in the opacity shield; two or three turns is sufficient. Do not thread the screws too far into the opacity shield. The opacity shield for the Catalyst 6509 or Catalyst 6509-E chassis is identified by a 6509-E that is silk-screened adjacent to several of the threaded holes; the opacity shield for the Catalyst 6506 or Catalyst 6506-E chassis is identified by a 6506-E that is silk-screened adjacent to several of the threaded holes.
- [Figure 3](#) shows how opacity shield is positioned on the 6506 or 6506-E switch. [Figure x](#) shows how opacity shield is positioned on the 6509 or 6509-E switch.
- Step 7** Open the envelope containing the disposable ESD wrist strap. Attach the disposable ESD wrist strap to your wrist. Attach the other end of the wrist strap to exposed metal on the chassis.
- Step 8** Position the opacity shield over the air intake side of the chassis so that the two thumbscrews on the opacity shield are aligned with the unused L-bracket screw holes on the chassis.
- Step 9** Press the opacity shield firmly against the air intake side of the chassis and hand tighten the two thumbscrews to secure the opacity shield to the chassis.
- Step 10** Position the rivet sleeve over either one of the square cutouts on the opacity shield (non-E chassis) or over the one of the round cutouts on the opacity shield (-E chassis). Press the rivet sleeve through the cutout, through the opacity shield material, and through one of the chassis air vent perforations.

- Step 11** Take the rivet pin and push it through the rivet sleeve until you hear a click.
- Step 12** Repeat step 10 and step 11 for the remaining three snap rivet fasteners.

Figure 3 *Installing the Opacity Shield on the Catalyst 6506 or Catalyst 6506E Switch*

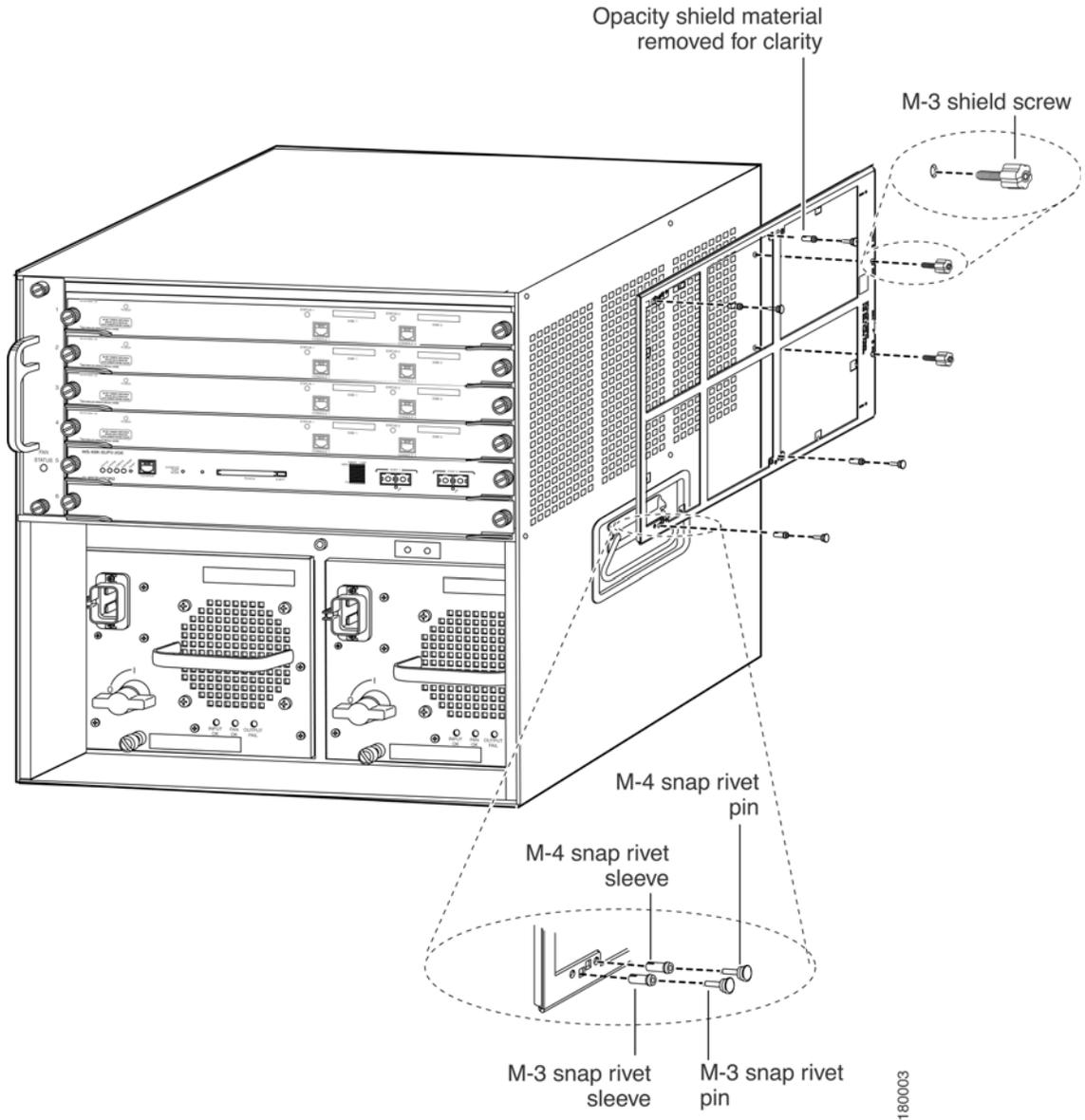
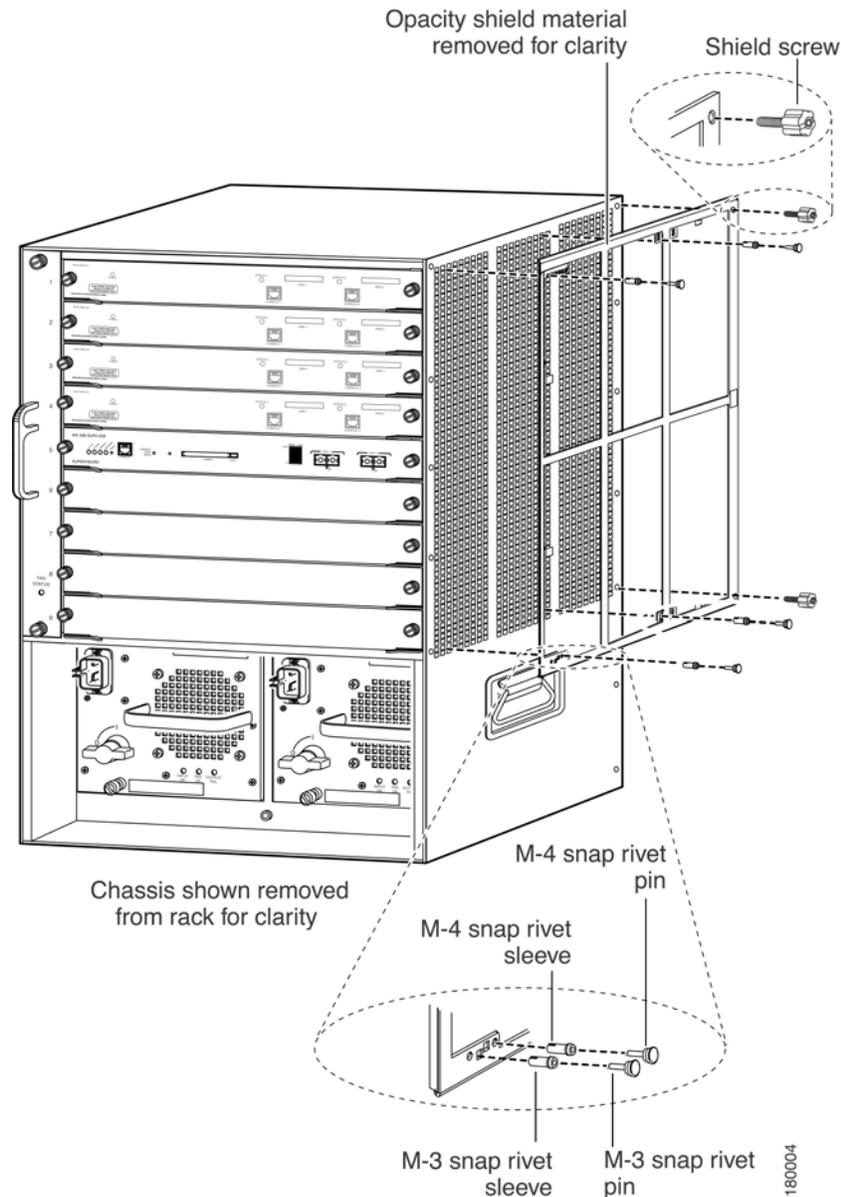


Figure 4 Installing the Opacity Shield on the Catalyst 6509 or Catalyst 6509E Switch



Physical Security

The Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches are entirely encased by a thick steel chassis. Nine module slots are provided on the Catalyst 6509 switch and Catalyst 6509-E switch and six module slots are provided on the Catalyst 6506 switch and Catalyst 6506-E switch. On-board LAN connectors and console connectors are provided on the supervisor blades, and console connectors are provided on the WiSMs. The power cable connection and a power switch are provided on the power supply of all the models.

The Crypto Officer is responsible for the application and maintenance of the physical security policy. Verify that the Supervisor Blade is installed in chassis slot 5 and the four WiSMs are installed in chassis slots 1, 2, 3, and 4. Install slot covers over the remaining chassis slots. The slot covers are included with each chassis, and additional slot covers may be ordered from Cisco. Use the procedure described here to apply tamper-evidence labels to the network modules and the service modules.

After the switch has been configured to meet FIPS 140-2 Level 2 requirements, the switch cannot be accessed without indicating signs of tampering. To seal the system with tamper-evidence labels, follow these steps:

-
- Step 1** Remove any grease, dirt, or oil from the cover by using alcohol-based cleaning pads before applying the tamper-evidence labels. The chassis temperature should be above 10° C (50° F).
- Step 2** Place labels on the chassis as shown in [Figure 5](#) and [Figure 6](#).
- a. Fan tray—The tamper-evidence label should be placed so that one half of the label adheres to the front of the fan tray and the other half adheres to the left side of the chassis. Any attempt to remove the fan tray will damage the tamper seal, which indicates tampering has occurred.
 - b. Modules—For each Supervisor Blade 720, WiSM Module or blank module cover installed in the chassis, place a tamper-evidence label so that one half of the label adheres to the module and the other half adheres to the right side of the chassis. Place another tamper-evidence label so that one half of the label adheres to the module and the other half adheres to the fan tray on the left side. Any attempt to remove a supervisor blade, WiSM Module, or blank module cover will damage a tamper seal, which indicates tampering has occurred.
 - c. Power supply—For each power supply or power supply blank cover installed in the chassis, place a tamper-evidence label so that one half of the label adheres to the front of the power supply or power supply blank cover and the other half adheres to the chassis. Any attempt to remove a power supply will damage the tamper seal, which indicates tampering has occurred.
 - d. Opacity shield—Four labels should be applied to the opacity shield (mounted on the right side of the chassis) as follows:
 - Place one label so that one half of the label adheres to the top of the opacity shield and the other half adheres to the chassis.
 - Place one label so that one half of the label adheres to the left side of the opacity shield and the other half adheres to the chassis.
 - Place one label so that one half of the label adheres to the right side of the opacity shield and the other half adheres to the chassis.
 - For the Catalyst 6509 switch chassis only, place one label so that one half of the label adheres to the bottom of the opacity shield and the other half adheres to the right side of the chassis.
- Step 3** Place labels on each supervisor blade installed in the chassis as shown in the figures below.
- a. Place a tamper-evidence label so that one half of the label adheres to the PCMCIA slot and the other half adheres to the supervisor blade faceplate. Any attempt to install or remove a Flash PC card will damage the tamper seal, which indicates tampering has occurred.
 - b. Place a tamper-evidence label so that one half of the label adheres to the GBIC transceiver installed in the supervisor blade network interface uplink port and the other half adheres to the supervisor blade 2 faceplate. Any attempt to remove a GBIC transceiver will damage the tamper seal, which indicates tampering has occurred.
 - c. Place a tamper-evidence label so that it completely covers an unpopulated network interface uplink port. Any attempt to install a GBIC transceiver in the network interface uplink port will damage the tamper seal, which indicates tampering has occurred.

- Step 4** Place labels on each WiSM installed in the chassis as shown in the figures below.
- Place tamper-evidence labels on both the PCMCIA slots such that one half of the label adheres to the PCMCIA slots and the other half adheres to the WiSM faceplate. Any attempt to install or remove the Compact Flash cards will damage the tamper seals, which indicates tampering has occurred.



Note The tamper seal label adhesive completely cures within five minutes.

Figure 5 Catalyst 6506 and Catalyst 6506E Switch Chassis Tamper-Evidence Label Placement

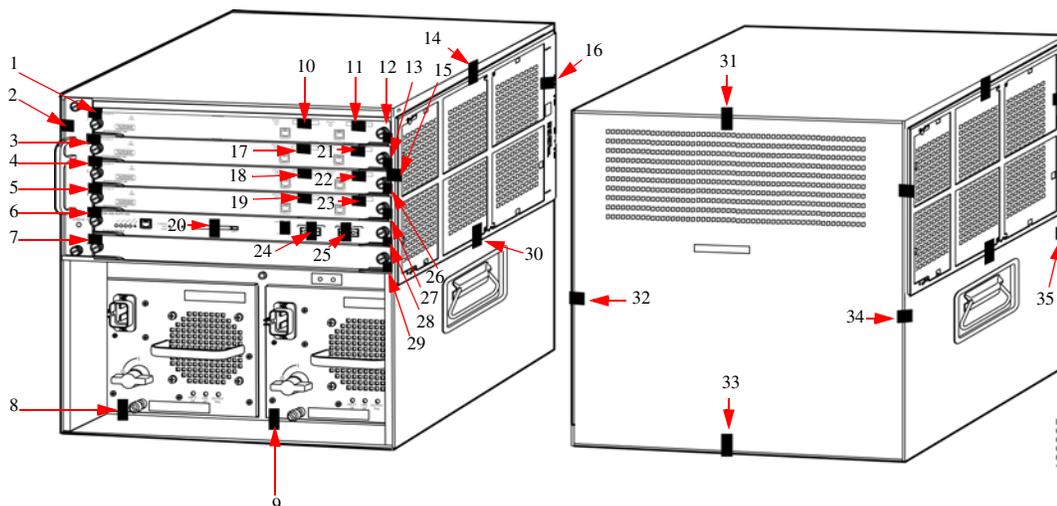
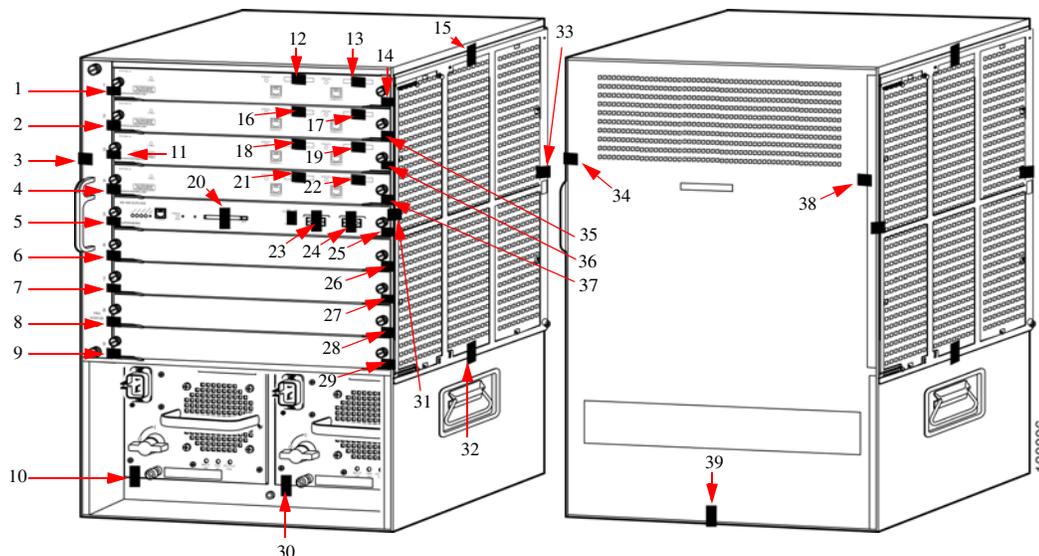


Figure 6 Catalyst 6509 and Catalyst 6509E Switch Chassis Tamper-Evidence Label Placement



The tamper-evidence seals are made from a special thin-gauge vinyl with self-adhesive backing. Any attempt to open the chassis, remove the modules or power supplies, or remove the opacity shield will damage the tamper-evidence seals or the painted surface and metal of the chassis. The tamper-evidence seals must be inspected for damage to verify that the module has not been tampered with.

Tamper-evidence seals can also be inspected for signs of tampering, which include the following: curled corners, bubbling, crinkling, rips, tears, and slices. The word OPEN may appear if the label was peeled back. If it is deemed necessary by the Crypto Officer to replace the tamper evident stickers, please reference FIPS kit CVPN6500FIPS/KIT=, version D0.

Mitigation of Attacks

The Controllers in the WiSM module provide mitigation against the following attacks:

- Protection against wireless denial of service attacks due to forged 802.11 management frames. When wireless clients and wireless infrastructure are enabled with MFP (Management Frame Protection) the system is protected against DoS attacks from exploited 802.11 management frames.
- Protection against rogue or unauthorized access points in joining the trusted network. The Cisco access points and Controllers support mutual authentication via x.509 certificates that are installed from the factory.
- Protection against MiTM attacks against access point control traffic. All control and bridging traffic between Controllers and access points is protected with AES-CCM encryption.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

© 2010-2011 Cisco Systems, Inc. All rights reserved.