Cisco Catalyst 6506, Catalyst 6506-E, Catalyst 6509 and Catalyst 6509-E Switch with Catalyst 6500 Series VPN Services Port Adapter (ws-ipsec-2 and ws-ipsec-3) Security Policy version 1.6 May 27, 2009

This is the non-proprietary Cryptographic Module Security Policy for the Catalyst 6506, Catalyst 6506-E, Catalyst 6509, Catalyst 6509-E switches with the VPN Services Port Adapter:

- Chassis Hardware Version
  - Catalyst 6506 switch
  - Catalyst 6506-E switch
  - Catalyst 6509 switch
  - Catalyst 6509-E switch
- Backplane Hardware Version
  - 1.1 (Catalyst 6506-E switch)
  - 1.4 (Catalyst 6509-E switch)
  - 3.0 (Catalyst 6506 switch, Catalyst 6509 switch)
- Supervisor Blade Hardware Version
  - SUP720-3B version 5.7
  - SUP720-3BXL version 5.7
  - SUP720-10GbE version 2.1
- VPN Services Port Adapter Version
  - ws-ipsec-2 version 1.0
  - ws-ipsec-3 version 1.0
- Firmware version — Cisco IOS 12.2(33)SXI, IOS 12.2(33)SXI1, Modular IOS 12.2(33)SXI and Modular IOS 12.2(33)SXI1, image filename
  - s72033-adventerprisek9_wan_dbg-mz.122-33.SXI for IOS
  - s72033-adventerprisek9_wan_dbg-mz.122-33.SXI1 for IOS

CISCO SYSTEMS

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

- s72033-adventerprisek9_wan_dbg-vz.122-33.SXI for Modular IOS
- s72033-adventerprisek9_wan_dbg-vz.122-33.SXI1 for Modular IOS

This security policy describes how the listed Catalyst 6500 series switches with the VPN Services Port Adapter (ws-ipsec-2 and ws-ipsec-3) meet the security requirements of FIPS 140-2, and describes how to operate the hardware devices in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the listed Catalyst 6500 series switches with the VPN Services Port Adapter. This document 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 http://csrc.nist.gov/cryptval/.

Contents

This document contains the following sections:

References

This publication deals only with operations and capabilities of the listed Catalyst 6500 series switches with VPN Services Port Adapter in the technical terms of a FIPS 140-2 Cryptographic Module Security Policy. More information is available on the Catalyst 6500 series switches from the following source:

- The Catalyst 6500 series switch product descriptions can be found at:

  http://www.cisco.com/en/US/products/hw/switches/ps708/index.html
- For answers to technical or sales related questions, refer to the contacts listed on the Cisco Systems website at www.cisco.com.
- For answers to technical or sales-related questions for the module, refer to the NIST Validated Modules website at http://csrc.nist.gov/cryptval.

Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. The Submission Package also contains the following documents:

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

This publication provides an overview of the Catalyst 6506, Catalyst 6506-E, Catalyst 6509, Catalyst 6509-E switches and explains the secure configuration and operation of the modules. This introduction section is followed by the “Catalyst 6500 Series Switches” section which details the general features and functionality of the applicable Catalyst 6500 series switches. The “Secure Operation of the Catalyst 6500 Series Switches” section specifically addresses the required configuration for the FIPS-approved 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, contact Cisco Systems.

Catalyst 6500 Series Switches

Branch office networking requirements are dramatically evolving, driven by web and e-commerce applications to enhance productivity and merging the voice and data infrastructure to reduce costs. The Catalyst 6500 series switches with the VPN Services Port Adapter offer versatility, integration, and security to branch offices. With numerous network modules and service modules available, the modular architecture of the Cisco switches easily allows interfaces to be upgraded to accommodate network expansion. The Catalyst 6500 series switches provide a scalable, secure, manageable remote access server that meets FIPS 140-2 Level 2 requirements, as a multi-chip standalone module.

Each chassis is a multi-chip, standalone cryptographic system containing a VPN Services Port Adapter to perform the cryptographic operations and a supervisor engine to manage overall chassis configuration.

Each chassis is a multi-chip, standalone cryptographic system containing a VPN Services Port Adapter Module to perform the cryptographic operations, a Services Port Adapter carrier card and a supervisor engine to manage overall chassis configuration.

All cryptographic operations including AES and Triple-DES encryption, SHA-1 hashing, HMAC-SHA-1 message authentication, and random number generation are performed by the VPN Services Port Adapter.

This section describes the general features and functionality provided by the Catalyst 6506 and Catalyst 6506-E switches (see Figure 1), and the Catalyst 6509 and Catalyst 6509-E switches (see Figure 2).

Figure 1 Catalyst 6506 and Catalyst 6506-E Switches

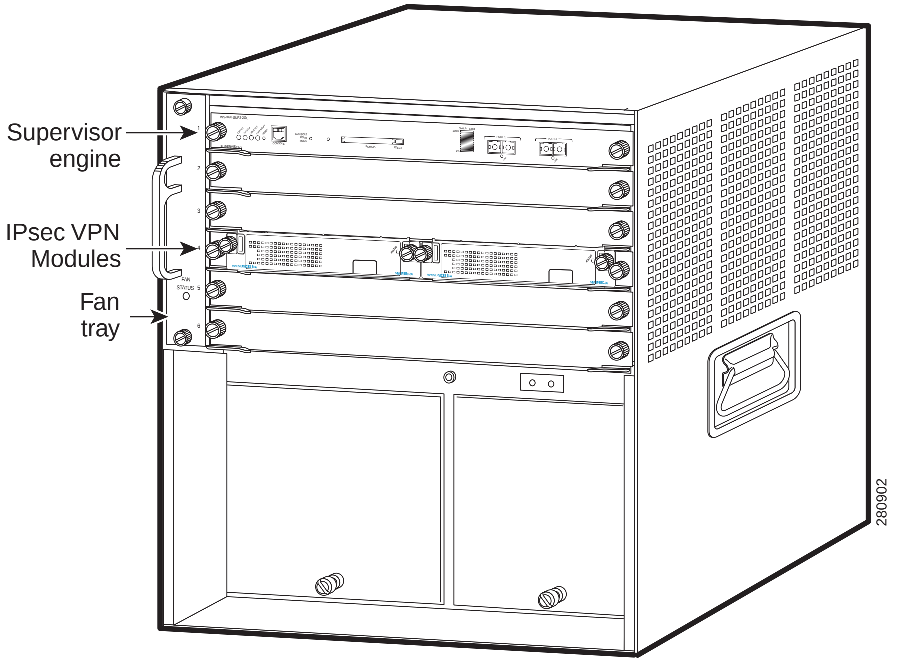
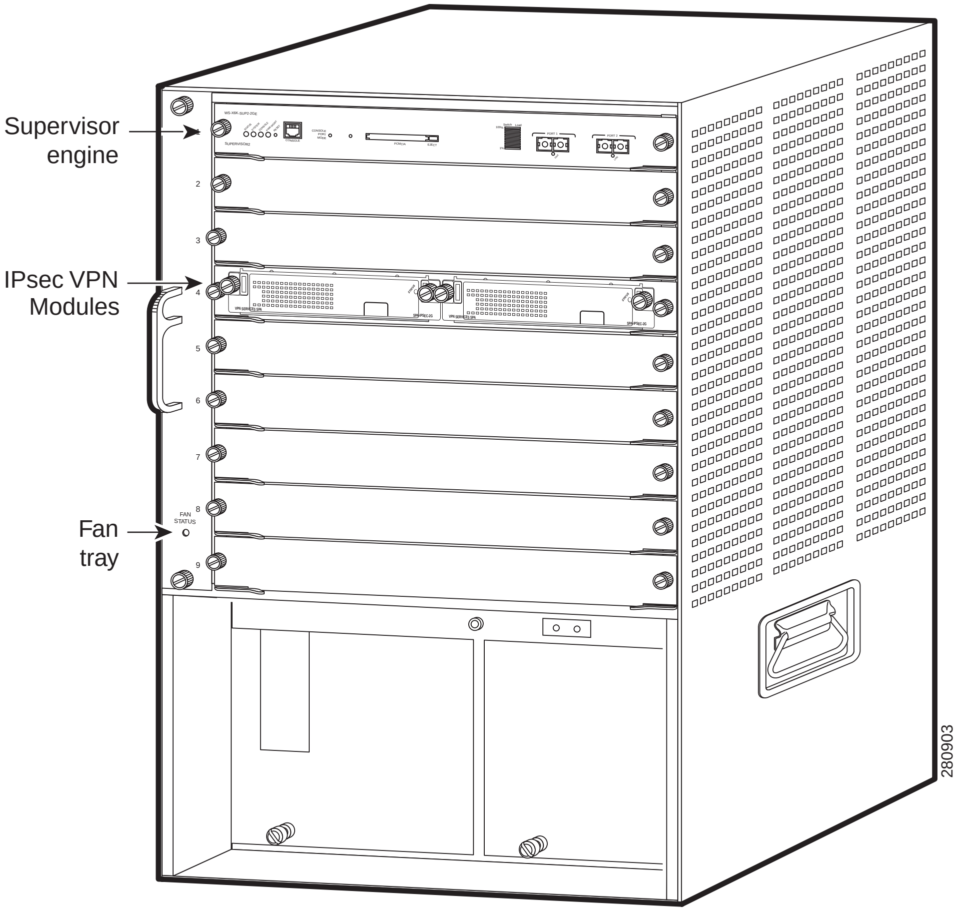


Figure 2 Catalyst 6509 and Catalyst 6509-E Switches



Catalyst Catalyst 6506, 6506-E, 6509 and 6509-E Switches Cryptographic Module

The cryptographic boundary is defined as encompassing the following:

- Top, front, left, right, and bottom surfaces of the chassis.
- All portions of the backplane of the chassis that are not designed to accommodate a network module or a service module.
- The inverse of the three-dimensional space within the chassis that would be occupied by any installed network module or a service module which does not perform approved cryptographic functions, or any installed power supply.
- The connection apparatus between the network module or service module and the motherboard and daughterboard that hosts the network module or service module.

The cryptographic boundary is illustrated in Figures 1 and 2 above as the dark border around the module.

The cryptographic boundary does not include the network module or service module itself unless it performs approved cryptographic functions. In other words, the cryptographic boundary encompasses all hardware components within the chassis except any installed non approved cryptographic network modules or service modules and the power supply sub modules. The service and network modules currently included in the cryptographic boundary are theVPN Services Port Adapter, Services Port Adapter carrier card and one supervisor board (either a SUP720-3B, SUP720-3BXL or a SUP720-10GbE).

The Catalyst 6500 series switches incorporate one or more VPN Services Port Adapter cryptographic accelerator cards and one or more supervisor blades. The VPN Services Port Adapter is installed in a Services Port Adapter carrier that occupies a chassis module slot.

Cisco IOS and Modular IOS features such as tunneling, data encryption, and termination of remote access WANs using IPsec, Layer 2 forwarding and Layer 2 tunneling protocols make the Catalyst 6500 series switches with VPN Services Port Adapter an ideal platform for building virtual private networks or outsourced dial solutions.

The service modules require that a special opacity shield be installed over the intake-side air vents in order 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. Detailed installation instructions for the shield are provided in this publication

Module Interfaces

The switch chassis physical interfaces are located on the Supervisor Engine 720 front panel. The Supervisor Engine 720-3B and 3BXL have one console port, one RJ-45 10/100/1000 Ethernet port (with link LEDs), two Gigabit Ethernet ports utilizing SFP transceiver modules, two PCMCIA slots to hold compact flash memory devices, and status LEDs. The Supervisor Engine 720-10GbE has one console port, one RJ-45 10/100/1000 Ethernet port, two Gigabit Ethernet ports utilizing SFP transceiver modules, two 10Gigabit Ethernet uplink ports, two USB ports, PCMCIA slots to hold compact flash memory devices and status LEDs

Figure 3 Supervisor Engine 720-3B and 720-3BXLPhysical Interfaces

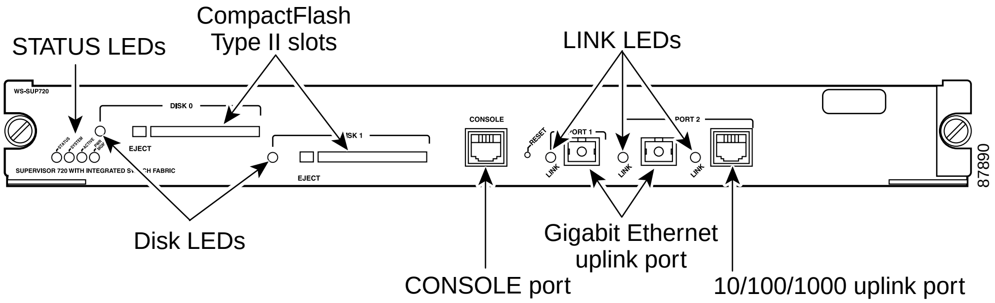
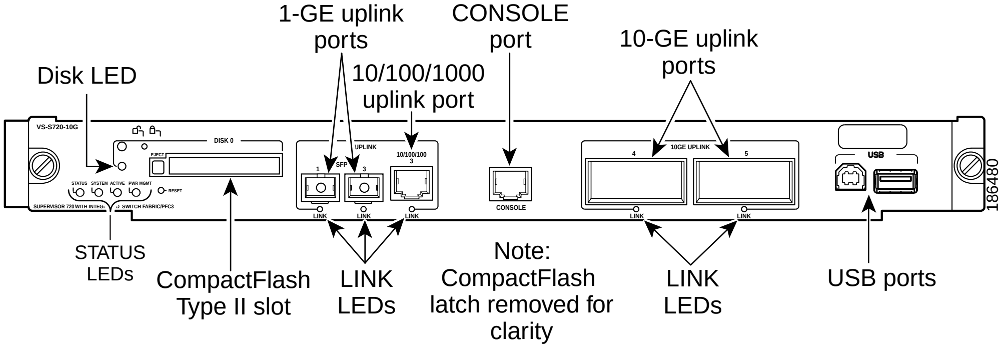


Figure 4 Supervisor Engine 720-10GbE Physical Interfaces



The Catalyst 6500 series switches provide console ports, fixed Ethernet interfaces, six network and service module slots on the Catalyst 6506 and Catalyst 6506-E switch chassis and nine network and service module slots on the Catalyst 6509 and Catalyst 6509-E switch chassis. Network modules support a variety of LAN and WAN connectivity interfaces, such as the following: Ethernet, ATM, serial, ISDN BRI, and integrated CSU/DSU options for primary and backup WAN connectivity.

An network module or a service module is installed in one of the chassis slots, which are located on the front panel of the chassis. The modules interface directly with the supervisor engine, and cannot perform cryptographic functions; they only serve as a data input and data output physical interface.

The supervisor engine has three Ethernet uplink ports, with only two active at any time: either two Gigabit Ethernet SFP-based ports or one Gigabit Ethernet SFP-based port and one 10/100/1000 RJ-45 port. The supervisor engine also has an RJ-45 connector for a console terminal for local system access. The Ethernet ports have LINK LEDs. Power is supplied to the module from the power supply through the backplane. The figure below shows the LED locations on the supervisor engine front panel. Table 1 describes the LEDs.

Table 1 Supervisor Engine LED Descriptions

LED	Color/State	Description
STATUS	Green	All diagnostics pass. The module is operational (normal initialization sequence).
	Orange	The module is booting or running diagnostics (normal initialization sequence). An over-temperature condition has occurred. (A minor temperature threshold has been exceeded during environmental monitoring.)
	Red	The diagnostic test failed. The module is not operational because a fault occurred during the initialization sequence. An over-temperature condition has occurred. (A major temperature threshold has been exceeded during environmental monitoring.)
SYSTEM[1]	Green	All chassis environmental monitors are reporting OK.
	Orange	The power supply has failed or the power supply fan has failed. Incompatible power supplies are installed. The redundant clock has failed. One VTT[2] module has failed or the VTT module temperature minor threshold has been exceeded.

Table 1 Supervisor Engine LED Descriptions (continued)

LED	Color/State	Description
	Red	Two VTT modules fail or the VTT module temperature major threshold has been exceeded. The temperature of the supervisor engine major threshold has been exceeded.[3]
ACTIVE	Green	The supervisor engine is operational and active.
	Orange	The supervisor engine is in standby mode.
POWER MGMT	Green	Sufficient power is available for all modules.
	Orange	Sufficient power is not available for all modules.
PCMCIA		The PCMCIA LED is lit when no Flash PC card is installed in the slot, and it goes off when you insert a Flash PC card.
LINK	Green	The port is operational.
	Orange	The link has been disabled by software.
	Flashing Orange	The link is bad and has been disabled due to a hardware failure.
	Off	No signal is detected.
VPN Services Port Adapter		
STATUS	Green	All non-FIPS-related diagnostic tests pass. The module is operational.[4]
	Red	A diagnostic test other than an individual port test failed.
	Orange	Indicates one of three conditions: • The module is running through its boot and self-test diagnostic sequence. • The module is disabled. • The module is in the shutdown state.
	Off	The module power is off.

[1] The SYSTEM and PWR MGMT LED indications on a redundant supervisor engine are synchronized to the active supervisor engine.

[2] VTT = voltage termination module. The VTT module terminates signals on the Catalyst switching bus.

[3] If no redundant supervisor engine is installed and there is a VTT module minor or major over-temperature condition, the system shuts down.

[4] Enter the **show crypto eli** command to determine whether the FIPS-related self-tests passed.

All of these physical interfaces are separated into the logical interfaces from FIPS 140-2 as described in Table 2.

Table 2 FIPS 140-2 Logical Interfaces

Switch Physical Interfaces	FIPS 140-2 Logical Interface
Gigabit Ethernet (1-GE, 10/100/1000 or 10-GE) ports SFP ports Backplane interface Console port	Data input interface
Gigabit Ethernet (1-GE, 10/100/1000 or 10-GE) ports SFP ports Backplane interface Console port	Data output interface
Gigabit Ethernet (1-GE, 10/100/1000 or 10-GE) ports SFP ports Backplane interface Console port Power switch	Control input interface
Gigabit Ethernet (1-GE, 10/100/1000 or 10-GE) ports Network and service module interfaces Backplane interface Console port LEDs	Status output interface
Power plug	Power interface

Roles and Services

Authentication is role-based. There are two main roles in the switch that operators may assume: the crypto officer role and the user role. The administrator of the switch assumes the crypto officer role in order to configure and maintain the switch using crypto officer services, while the users only use the basic user services. Both roles are authenticated by providing a valid username and password. The configuration of the encryption and decryption functionality is performed only by the crypto officer after authentication to the crypto officer role by providing a valid crypto officer username and password. After the crypto officer configures the encryption and decryption functionality, the user can use this functionality after authentication to the user role by providing a valid user username and password. The crypto officer can also use the encryption and decryption functionality after authentication to the crypto officer role.

User and crypto officer passwords are required to be at least 8 characters in length, using both letters and digits. This provides a potential password space of approximately 5,595 trillion passwords. In order to have a one in 100,000 chance of randomly guessing a password in a space of a minute, an attacker would have to be able to enter 93 billion passwords per second, which far exceeds the operational capabilities of the module or its interfaces.

The module supports RADIUS and TACACS+ for authentication and they are used in the FIPS mode.

Crypto Officer Services

During initial configuration of the switch, the crypto officer password (the “enable” password) is defined. A crypto officer may assign permission to access the crypto officer role to additional accounts, which creates additional crypto officers.

The crypto officer role is responsible for the configuration and maintenance of the switch. The crypto officer services consist of the following:

- Configuring the switch—Defines network interfaces and settings, creates command aliases, sets the protocols the switch will support, enables interfaces and network services, sets system date and time, and loads authentication information.
- Defining rules and filters—Creates packet filters that are applied to user data streams on each interface. Each filter consists of a set of rules, which define a set of packets to permit- or deny-based characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
- Status functions—Views the switch configuration, routing tables, and active sessions, uses the **Get** commands to view SNMP MIB II statistics, health, temperature, memory status, voltage, and packet statistics, reviews accounting logs, and views physical interface status.
- Managing the switch or the switch—Logs off users, shuts down or reloads the switch, manually backs up switch configurations, views complete configurations, manages user rights, and restores switch configurations.
- Setting encryption and bypass—Sets up the configuration tables for IP tunneling. Sets keys and algorithms to be used for each IP range or allow plaintext packets to be set from a specified IP address.
- Changing port adapters—Inserts and removes adapters in a port adapter slot.

User Services

A user enters the system by accessing the console port with a terminal program or through IPsec protected telnet. The supervisor blade firmware prompts the user for their password. If the password is correct, the user is allowed entry to the Cisco IOS/Modular IOS executive program. The user services consist of the following:

- Status functions—Views state of interfaces, state of Layer 2 protocols, and version of Cisco IOS or Modular IOS currently running.
- Network functions—Connects to other network devices (using outgoing TELNET or PPP) and initiates diagnostic network services (that is, ping, mtrace).
- Terminal functions—Adjusts the terminal session (for example, locks the terminal, adjusts flow control).
- Directory Services—Displays the directory of files kept in flash memory.

Installing the Opacity Shield on the Catalyst 6500 Series 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 The opacity shield part number is located on the outside of the protective packaging.

To install an opacity shield on the Catalyst 6500 series switches, follow these steps:

Step 1 The opacity shield is designed to be installed on a Catalyst 6500 series 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 (part number CVPN6500FIPS/KIT=). 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. 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:

- (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.

Note Extra snap fasteners are included in the bags of installation hardware in case of loss or damage.

Note Installation hardware from one bag is not interchangeable with the installation hardware from the second bag.

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. (See Figure 5 for the Catalyst 6506 and Catalyst 6506-E switches, or Figure 6 for the Catalyst 6509 and Catalyst 6509-E switches.) 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

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). Refer to Figure 5 or Figure 6 for snap rivet fastener placement. Press the rivet sleeve through the cutout, through the opacity shield material, and through one of the chassis air vent perforations.

Note You might need to try different cutouts to find the one cutout that aligns correctly with a chassis air vent perforation.

Step 11 Take the rivet pin and push it through the rivet sleeve until you hear a click.

Note If you do not hear a click, remove and inspect the snap rivet fastener. If the rivet sleeve appears expanded or damaged, discard the snap rivet fastener and use a new one from the extras supplied in the bag of installation hardware.

Step 12 Repeat step 10 and step 11 for the remaining three snap rivet fasteners. Refer to Figure 5 (Catalyst 6506 and Catalyst 6506-E) or Figure 6 (Catalyst 6509 and Catalyst 6509-E) for snap rivet fastener placement.

Caution Due to decreased airflow when using the opacity shield, which is required for FIPS 140-2 validation, short-term operation as specified by GR-63-CORE at 55º C is impacted. Short-term operation requirements will only be met at 40º C. Without the opacity shield installed, the system will meet the short-term operations requirements at 55º C.

Caution We recommend that you replace the opacity shield every three months to prevent dust build-up and the possibility of overheating the chassis. If the environment is especially dusty, inspect and replace the opacity shield more often.

Note If you need to remove the chassis from the rack, you must first remove the opacity shield. With the opacity shield installed, the chassis is too wide to slide out of the rack.

Figure 5 Installing the Opacity Shield on the Catalyst 6506 or Catalyst 6506-E Switch

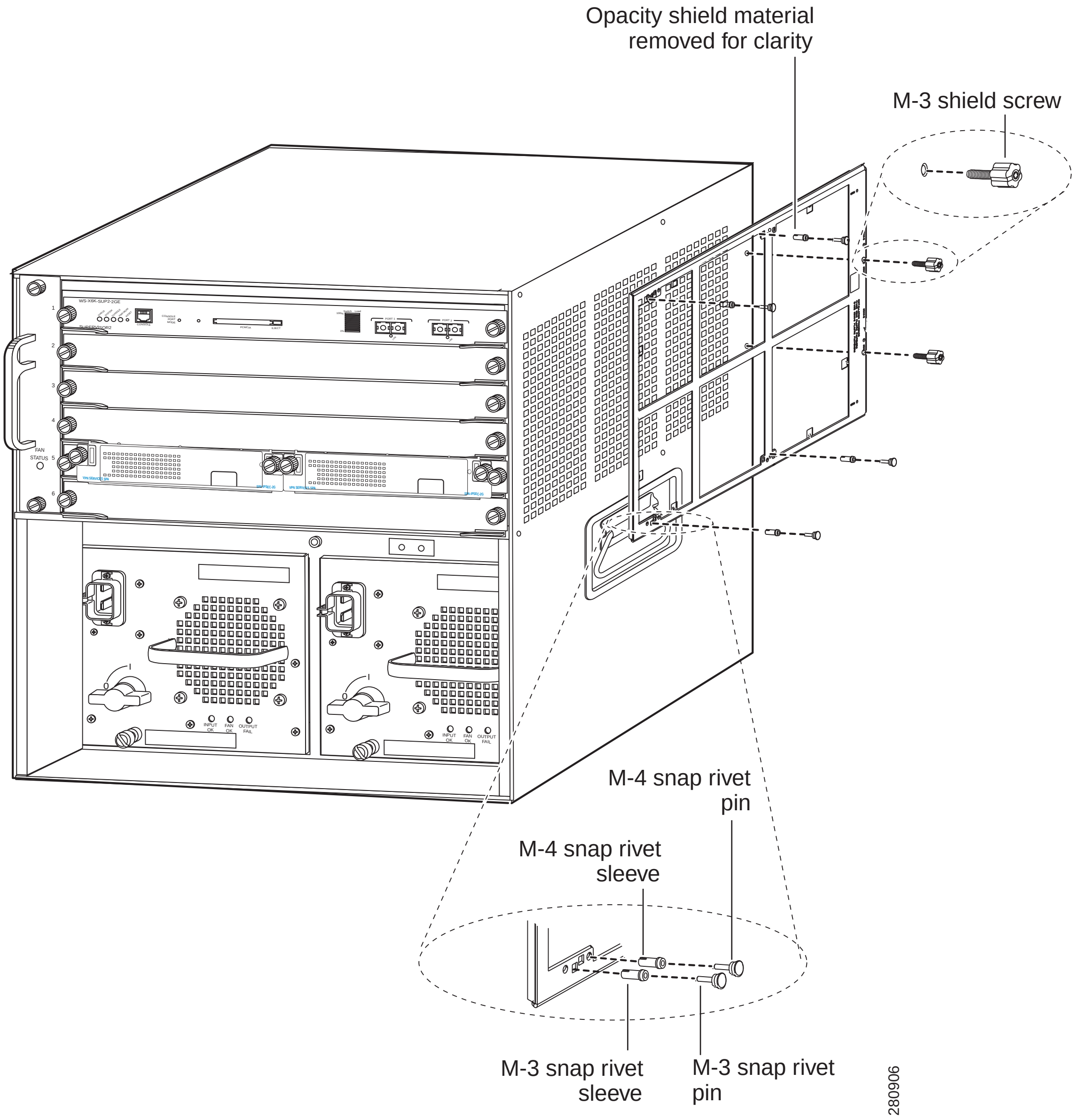
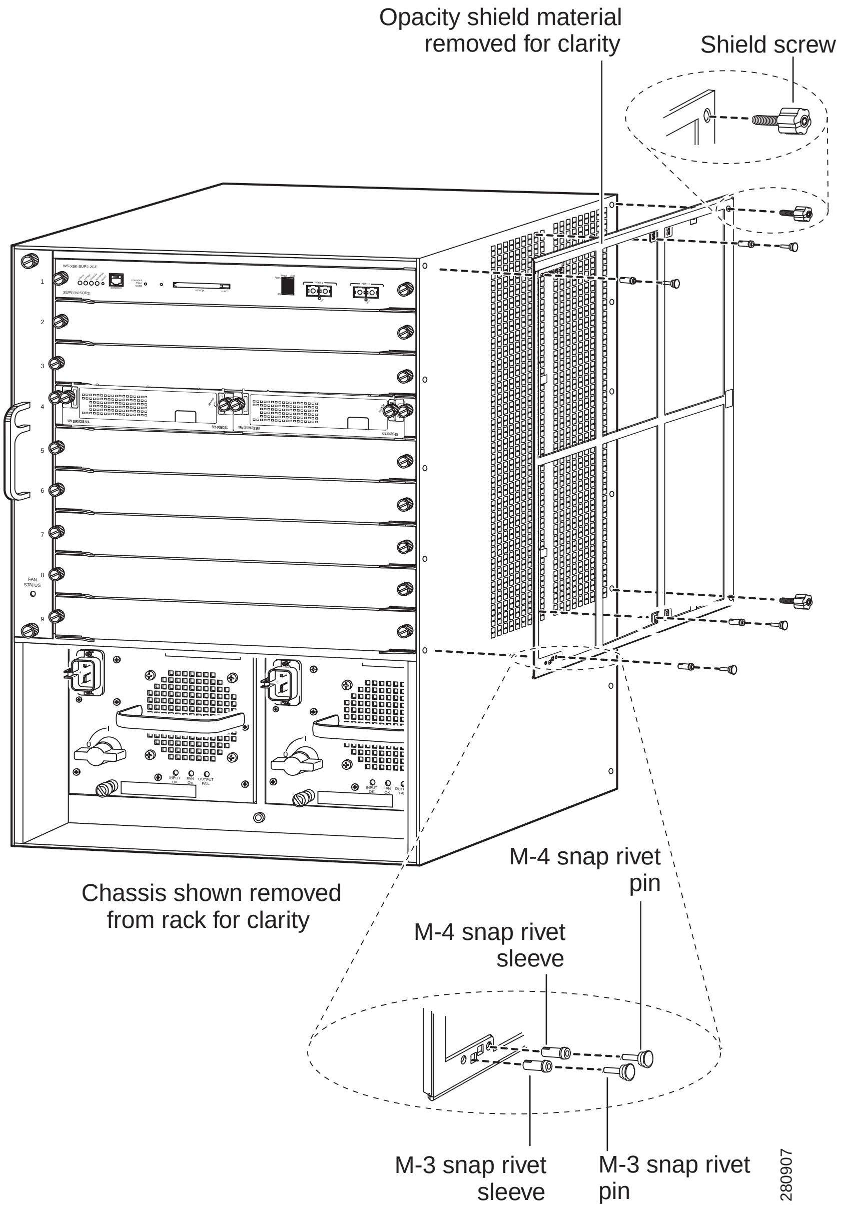


Figure 6 Installing the Opacity Shield on the Catalyst 6509 or Catalyst 6509-E Switch



Physical Security

The switch is entirely encased by a thick steel chassis. Nine module slots are provided on the Catalyst 6509 switch, Catalyst 6509-E switch, 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 engines, and the power cable connection and a power switch are provided on the power supply of both models. The individual modules that comprise the switch may be removed to allow access to the internal components of each module.

Any chassis slot that is not populated with a module must have a slot cover installed in order to operate in a FIPS compliant mode. 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.

Note Use the same procedure to apply tamper evidence labels to the slot covers.

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 serialized 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 either Figure 9 (Catalyst 6506), or Figure 10 (Catalyst 6509 switch).

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 Engine 720, VPN Services Port Adapter, network module, or blank module cover installed in the chassis, place a tamper evidence label so that one half of the label adheres to the right side of the module and the other half adheres to the right side of the chassis. Any attempt to remove the fan tray will damage the 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 the fan tray 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 engine installed in the chassis as shown in either Figure 7 (Catalyst 6506 and Catalyst 6506-E switches), or Figure 8 (Catalyst 6509 and Catalyst 6509-E switches).

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 Engine 2 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 engine 2 network interface uplink port and the other half adheres to the Supervisor Engine 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.

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

Figure 7 ***Catalyst 6506 and Catalyst 6506-E Switch Chassis Tamper Evidence Label Placement***

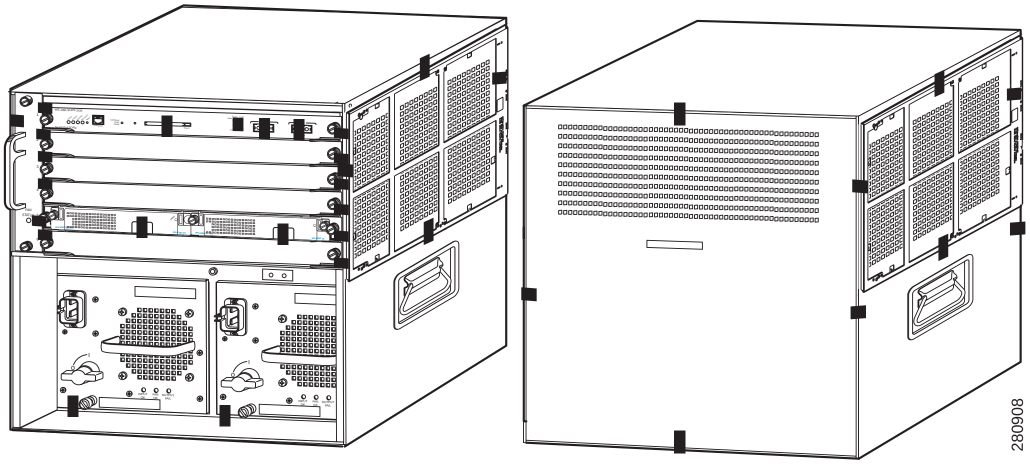
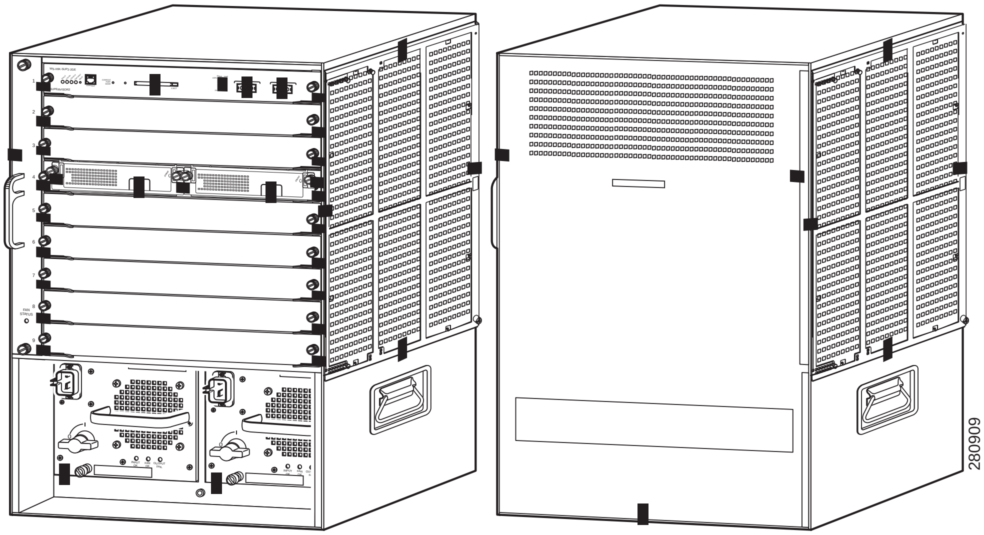


Figure 8 Catalyst 6509 and Catalyst 6509-E Switch Chassis Tamper Evidence Label Placement



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. Because the tamper evidence seals have nonrepeated serial numbers, they may be inspected for damage and compared against the applied serial numbers 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.

Cryptographic Key Management

The switch securely administers both cryptographic keys and other critical security parameters such as passwords. The tamper evidence seals provide physical protection for all keys. Keys are also password protected and can be zeroized by the crypto officer. Keys are exchanged manually and entered electronically using manual key exchange or Internet Key Exchange (IKE).

The modules support the following FIPS 140-2 approved algorithms: AES and Triple-DES encryption, SHA-1 hashing for IKE and IPSec, HMAC-SHA-1, and ANSI X9.31 Random Number Generation. The switch is in the approved mode of operation only when FIPS 140-2 approved algorithms are used. The following are not FIPS 140-2 approved algorithms: DES, MD5, HMAC-MD5, and DH. However, DH is allowed in FIPS mode of operations for use in key establishment, providing 80 or 96 bits of encryption strength. The IOS and Modular IOS implementations of AES and Triple-DES shall not be used in FIPS mode of operations.

The module supports the following types of key management schemes:

- Pre-shared key exchange through electronic key entry. AES and Triple-DES keys are exchanged manually and entered electronically.
- The IKE method with support for exchanging preshared keys manually and entering electronically.
  - The preshared keys are used with Diffie-Hellman key agreement technique to derive AES or Triple-DES keys.

The system supports commercially available methods of key establishment including Diffie-Hellman and IKE. Refer to the *Cisco IOS Reference Guide* for further information.

All preshared keys are associated with the CO role that created the keys and the CO role is protected by a password. Therefore, the CO password is associated with all the pre-shared keys. The crypto officer needs to be authenticated to store keys. All Diffie-Hellman (DH) keys agreed upon for individual tunnels are directly associated with that specific tunnel only through the IKE protocol.

The module supports the critical security parameters (CSPs) as described in Table 3.

Table 3 Critical Security Parameters

Name	Algorithm	Description	Storage	Zeroization Method
PRNG seed	X9.31	This is the seed for the ANSI X9.31 PRNG.	DRAM (plaintext)	Automatically every 400 bytes or turn off the switch.
Diffie Hellman private exponent	DH	The private exponent used in Diffie-Hellman (DH) exchange.	DRAM (plaintext)	Automatically after a DH shared secret has been generated, or turn off the switch.
skeyid	Keyed SHA-1	The value derived from the shared secret within IKE exchange.	DRAM (plaintext)	Automatically after the IKE session is terminated, or turn off the switch.
skeyid_d	Keyed SHA-1	The IKE key derivation key for non-ISAKMP security associations.	DRAM (plaintext)	Automatically after the IKE session is terminated, or turn off the switch.
skeyid_a	SHA-1 HMAC	The ISAKMP security association authentication key.	DRAM (plaintext)	Automatically after the IKE session is terminated, or turn off the switch.
skeyid_e	AES/ Triple-DES	The ISAKMP security association encryption key.	DRAM (plaintext)	Automatically after the IKE session is terminated, or turn off the switch.
IKE session encrypt key	AES/ Triple-DES	The IKE session encryption key.	DRAM (plaintext)	Automatically after the IKE session is terminated, or turn off the switch.
ISAKMP preshared	Secret	The key used to generate IKE skeyid during preshared-key authentication. This key can have two forms based on whether the key is related to the hostname or the IP address.	NVRAM (plaintext)	**# no crypto isakmp key**
IPsec encryption key	AES/ Triple-DES	The IPsec encryption key.	DRAM (plaintext)	Automatically after the IPSec session is terminated, or turn off the switch.
Router authentication key 1	Shared secret	This key is used by the switch to authenticate itself to the peer. The switch gets the password (that is used as this key) from the AAA server and sends it onto the peer. The password retrieved from the AAA server is zeroized upon completion of the authentication attempt.	DRAM (plaintext)	Automatically after the completion of the authentication attempt.

Table 3 Critical Security Parameters (continued)

Name	Algorithm	Description	Storage	Zeroization Method
PPP authentication key	RFC 1334	The authentication key used in PPP.	DRAM (plaintext)	Turn off the switch.
Router authentication key 2	Shared secret	This key is used by the switch to authenticate itself to the peer. The key is identical to Router authentication key 1 except that it is retrieved from the local database (on the switch).	NVRAM (plaintext)	**# no username password**
User password	Shared secret	The password of the user role.	NVRAM (plaintext or encrypted)	Set a new password
Enable password	Shared secret	The plaintext password of the cryptographic officer (CO) role.	NVRAM (plaintext)	Set a new password
Enable secret	Shared secret	The ciphertext password of the cryptographic officer (CO) role. The algorithm used to encrypt this password is not FIPS approved; this password is considered plaintext for FIPS purposes.	NVRAM (plaintext)	Set a new password
RADIUS secret	Shared secret	The RADIUS shared secret.	NVRAM (plaintext) DRAM (plaintext)	# **no radius-server key**
TACACS+ secret	Shared secret	The TACACS+ shared secret.	NVRAM (plaintext) DRAM (plaintext)	# **no tacacs-server key**

Note All RSA operations are prohibited by policy and the commands that can be executed by the cryptographic officer are shown as a command in the zeroization method column.

Table 4 lists the services accessing the CSPs, the type of access and which role accesses the CSPs. R, W, and D refer to read, write, and delete access, respectively.

Table 4 Role and Service Access to Critical Security Parameters (CSPs)

Role	Service	Critical Security Parameters
User Role	Status Functions	—
User Role	Network Functions	• PRNG Seed, DH private exponent, skeyid, skeyid_d, skeyid_a, skeyid_e, IKE session encrypt key, ISAKMP preshared, IPsec encrypt key, Router authentication key 1, PPP authentication key, Router authentication key 2, user password (R)
User Role	Terminal Functions	—
User Role	Directory Services	—
Crypto-Officer Role	Configure the Switch	• Router authentication key 2 (R/W/D)
Crypto-Officer Role	Define Rules and Filters	—
Crypto-Officer Role	Status Functions	—
Crypto-Officer Role	Manage the Switch	• PRNG Seed (R) • Router authentication key 1 (R/W/D) • PPP authentication key (D) • User password, Enable password, Enable secret, RADIUS secret, TACACS+ secret (R/W/D)
Crypto-Officer Role	Set Encryption/Bypass	• PRNG Seed, DH private exponent, skeyid, skeyid_d, skeyid_a, skeyid_e, IKE session encrypt key, IKE session authentication key, ISAKMP preshared, IKE hash key, IPsec encrypt key, IPsec authentication key, SSH session key (R/W/D) • PPP authentication key (R/W)
Crypto-Officer Role	Change WAN Interface Cards	—

Key Zeroization

All of the keys and CSPs of the module can be zeroized. Refer to the description column of Table 3 for information on methods to zeroize each key and CSP.

Self-Tests

To prevent any secure data from being released, it is important to test the cryptographic components of a security module to ensure that all components are functioning correctly. The switch includes an array of self-tests that are run during startup and periodically during operations. An example of the self-tests is the Cryptographic Known Answer test (KAT) on each of the FIPS 140-2 approved cryptographic algorithms and on the Diffie-Hellman algorithm. In addition, a software integrity test is performed power-up. If any of the self-tests fail, the switch transitions into an error state. Within the error state, all secure data transmission is halted and the switch outputs status information indicating the failure.

Examples of errors that cause the system to transition to an error state include:

- Firmware image integrity checksum failed
- Microprocessor overheats and burns out.
- Known answer test failed
- NVRAM module malfunction
- High temperature warning

VPN Services Port Adapter Self-Tests

- Power-up self-tests (POST)
  - AES Known Answer Test (KAT)
  - Triple-DES KAT
  - RNG KAT
  - SHA-1 KAT
  - HMAC SHA-1 KAT
  - Diffie-Hellman test
- Conditional self-tests
  - Continuous random number generation test

Cisco IOS/Modular IOS Software Self-Tests

- Power-up tests
  - Software/firmware test
  - Power up bypass test
  - AES KAT (not compliant)
  - Triple-DES KAT (not compliant)
  - SHA-1 KAT
  - HMAC SHA-1
- Conditional tests
  - Conditional bypass tests
  - Continuous random number generation test

Secure Operation of the Catalyst 6500 Series Switches

The Catalyst 6500 series switches with the VPN Services Port Adapter meets all the Level 2 requirements for FIPS 140-2. Follow the setting guidelines provided in the following sections to place the module in a FIPS-approved mode of operation. Operating this switch without maintaining the following settings will remove the module from the FIPS-approved mode of operation.

Initial Setup

Before configuring the switch, note these requirements:

- The crypto officer must ensure that the VPN Services Port Adapter cryptographic accelerator card is installed in the chassis by visually confirming the presence of the VPN Services Port Adapter.
- The crypto officer must apply tamper evidence labels as described in the "Physical Security" section on page 18 of this document.
- Only the crypto officer may add and remove network modules. When removing the tamper evidence label, the crypto officer should remove the entire label from the chassis and clean the cover of any grease, dirt, or oil with an alcohol-based cleaning pad. The crypto officer must reapply tamper evidence labels on the switch as described in the "Physical Security" section on page 18.
- The crypto officer must apply the opacity shield as described in the "Physical Security" section on page 18 of this document.

Initializing and Configuring the System

To initialize and configure the system, the crypto officer must perform the following operations:

- The crypto officer must perform the initial configuration. Cisco IOS or Modular IOS Release 12.2(33)SXI or 12.2(33)SXI1, Advanced security build (advsecurity) are the only allowable images; no other image may be loaded.
- The value of the boot field must be 0x0102 (the factory default). This setting disables the break from the console to the ROM monitor and automatically boots the Cisco IOS/Modular IOS image. From the **configure terminal** command line, the crypto officer enters the following syntax:

  ```
  config-register 0x0102
  ```

- The crypto officer must create the enable password for the 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.
- Identification and authentication on the console port is required for users. From the **configure terminal** command line, the crypto officer enters the following syntax:

  ```
  line con 0
  password [PASSWORD]
  login local
  ```

- The crypto officer shall only assign users to a privilege level 1 (the default).
- The crypto officer shall not assign a command to any privilege level other than its default.

- The crypto officer shall enable the module with the following command:

```
power enable module [slot]
```

- The crypto officer shall confirm that the VPN Services Port Adapter is enabled with the following command:

```
show mod
```

- The crypto officer may configure the module to use RADIUS or TACACS+ for authentication. Configuring the module to use RADIUS or TACACS+ for authentication is optional. If the module is configured to use RADIUS or TACACS+, the Crypto-Officer must define RADIUS or TACACS+ shared secret keys that are at least 8 characters long.
- If the crypto officer loads any Cisco IOS/Modular IOS image onto the switch, this will put the switch into a non-FIPS mode of operation.

IPsec Requirements and Cryptographic Algorithms

The only type of key management method allowed in FIPS mode is Internet Key Exchange (IKE).

Although the Cisco implementation of IKE allows a number of algorithms, only the following algorithms are allowed in a FIPS 140-2 configuration:

- ah-sha-hmac
- esp-sha-hmac
- esp-3des
- esp-aes

The following algorithms are not FIPS approved (or are non-compliant) and should not be used during FIPS-approved mode:

- DES
- MD-5 for signing
- HMAC MD-5
- RSA
- Software implementations of AES and Triple-DES

Protocols

SNMP v3 over a secure IPsec tunnel can be employed for authenticated, secure SNMP gets and sets. Since SNMP v2C uses community strings for authentication, only gets are allowed under SNMP v2C. If the SSP protocol is used to support high-availability relationships between modules, the SSP connections must be configured to operate over an authenticated and encrypted IPsec tunnel.

Remote Access

Telnet access to the system is only allowed through a secure IPsec tunnel between the remote system and the module. The Crypto officer must configure the module so that any remote connections using Telnet are secured through IPsec using FIPS-approved algorithms.

Note All users must authenticate after remote access is granted.

Disable Console Access

Once the module is configured, access to the console port must be disabled to prevent a user from accessing ROMMON and disabling the password. This is done by placing a tamper evidence label over the console port.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

By printing or making a copy of this document, the user agrees to use this information for product evaluation purposes only. Sale of this information in whole or in part is not authorized by CiscoSystems.