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

This security policy contains these sections:

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

Overview

The Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches together with the Wireless Services Module (WiSM) provides 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 LWAPP 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 a WiSM Module to perform the cryptographic operations and a supervisor engine to manage overall chassis configuration. The module meets all Level 2 FIPS 140-2 requirements.

The WiSM module in conjunction with Cisco Aironet Series Access Points support Wi-Fi Protected Access 2 (WPA2) security. 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-CCMP encryption. LWAPP protects all control and bridging traffic between trusted network access points and the module with AES-CCM encryption. In the FIPS mode of operation, the WiSM supports WPA2 (802.11i), HTTPS using TLS, LWAPP and RADIUS KeyWrap (using AES Key wrapping) for network communications, and uses the following cryptographic algorithm implementations:

- AES (software)
- AES-CCM (software)
- SHA-1 (software)
- HMAC SHA-1 (software)
- FIPS 186-2 Random Number Generator (software)
- RSA signature generation and verification (software)

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 Module (WiSM). 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
  - 1.0 (Catalyst 6506-E switch)
  - 1.1 (Catalyst 6509-E switch)
  - 3.0 (Catalyst 6506 switch, Catalyst 6509 switch)
- Supervisor Blade Hardware Version
  - SUP720-3B version 4.1
  - SUP720-3BXL version 4.0

- Supervisor Blade Firmware Version
  - Cisco IOS 12.2(18)SXF4, adventerprisek9 build
- WiSM Module Hardware Version 1.2
- WiSM Module Firmware Version 3.2.116.21

This security policy describes how the listed Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches with the WiSM Module 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 Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches with the Wireless Services Module (WiSM). 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:

- 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.

Figure 1 and Figure 2 below show the cryptographic boundary 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 one WiSM module and one supervisor board (either a SUP720-3B or a SUP720-3BXL).

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. Detailed installation instructions for the shield are provided in the "Installing the Opacity Shield on Catalyst 6506, 6506-E, 6509 and 6509-E Switches" section on page 15.

Figure 1 Cryptographic Boundary on Catalyst 6506 Switches

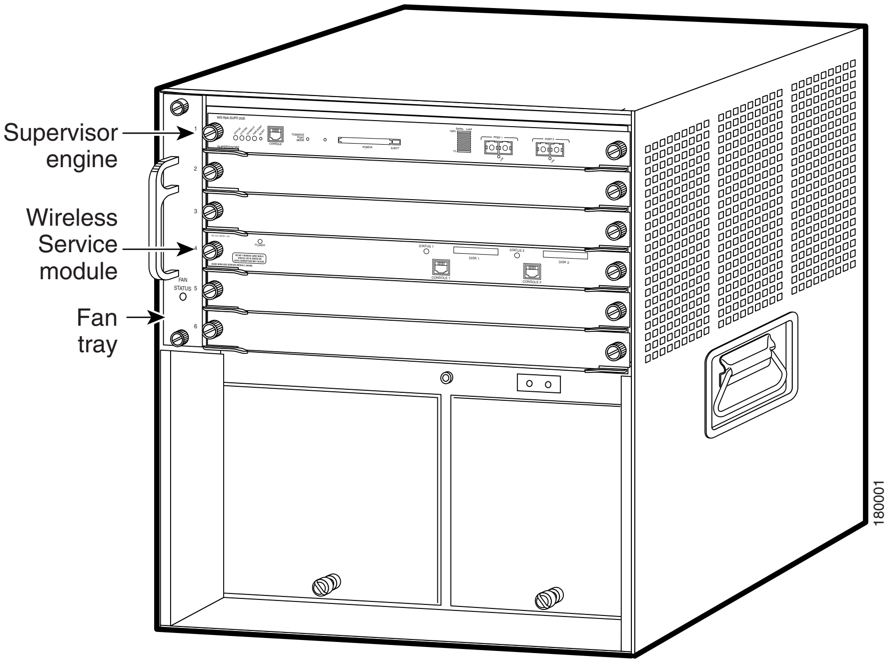
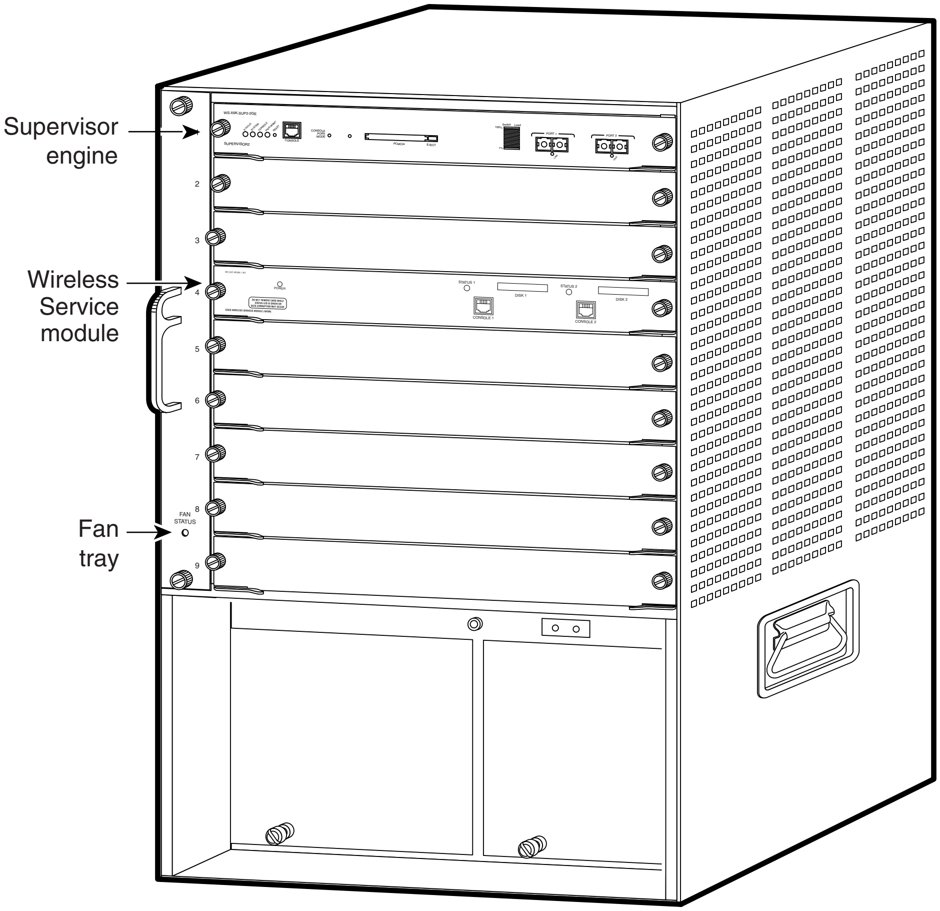


Figure 2 Cryptographic Boundary on Catalyst 6506E Switches



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 controller in the WiSM. The rest of the configuration shall be performed over a local link through the console connection of each of the controller 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.

Only the 3.2.116.21 LWAPP software may reside 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 Key
4. Configure WiSM Authentication Data
5. Configure RADIUS KeyWrap KEK and MACK Keys
6. Configure Ciphersuites for 802.11i
7. Configure Pre-shared Keys for 802.11i
8. Configure SNMP
9. 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 Key

The following command configures the controller to use device keys 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 RADIUS KeyWrap KEK and MACK Keys

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

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

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 wlan-index ssid
> config wlan security 802.1x disable wlan-index
> config wlan security wpa2 enable wlan-index
> config wlan radius_server auth add wlan-index radius-index
> config wlan enable wlan-index
```

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 wpa2 pre-shared-key enable wlan-index hex key
```

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
```

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 five roles:

- AP Role—This role is filled by an access point 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 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 Engine.
- 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

All services can be viewed by typing **?** from within the appropriate roles. This command shows all the services available to the role currently logged in. The services provided are summarized in Table 1.

Table 1 Module Services

Service	Role	Purpose
Self Test and Initialization	Any role except AP role	Cryptographic algorithm tests, software integrity tests, module initialization.
System Status	Any role except AP 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.

Table 1 Module Services (continued)

Service	Role	Purpose
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.
LWAPP	CO, User	Establishment and subsequent data transfer of an LWAPP session for use between the module and an AP[1].
TLS	CO	Establishment and subsequent data transfer of a TLS session for use between the module and the CO.
802.11i	CO, User	Establishment and subsequent data transfer of an 802.11i context for use between the module and wireless clients.
RADIUS KeyWrap	CO, User	Establishment and subsequent receive 802.11i PMK from the RADIUS server.
AP Association	AP role	Association of the AP with the WiSM.

[1] LWAPP uses RSA key wrapping which provides between 80 and 128 bits of effective symmetric key strength.

The module does not support a bypass capability in the approved mode of operations.

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 the WiSM front panel
- 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 CO Authentication

When a Supervisor user tries to connect to the CLI of the Supervisor through 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 is prompted to enter another password to receive additional services that are reserved for the Supervisor Crypto Officer. The Supervisor CO is 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 to that user based on whether they have read-only privileges (the user role) or read-write privileges (the CO role).

No characters are output to the terminal when users authenticate. If the incorrect password is entered, the module will re-prompt for the password with the message Access Denied.

After the module power cycles, a user must reauthenticate.

The WiSM module supports password based authentication for local access via the CLI as well as remote access via the SNMPv3.

The security policy stipulates that all user passwords must contain 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 LWAPP 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 7.9x10^23 attempts per minute, which far exceeds the operational capabilities of the module 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 and AES key wrap MAC keys 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. RSA public keys are output in plaintext in the form of X.509 certificates. The LWAPP session key is output wrapped with the AP's RSA key, and the TK and GTK are output encrypted with the LWAPP session key. 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 and Zeroization
PRNG seed key	FIPS 186-2	Flash	This is the seed key for the PRNG. It is statically stored in the code. It is zeroized during the zeroization procedure.
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. It is zeroized during the zeroization procedure.
User Password	Shared secret	Flash	Identity based authentication data for a user. Zeroized by overwriting it with a new password.
SNMPv3 user password	Shared secret	Flash	This secret is used to derive HMAC-SHA1 key for SNMPv3 authentication. Zeroized by the zeroization process.
Supervisor user password	Shared secret	Supervisor NVRAM	The plaintext password for the Supervisor User. Zeroized by overwriting it with a new password.
Enable password	Shared secret	Supervisor NVRAM	The plaintext password for the Supervisor Crypto Officer. Zeroized by overwriting it with a new password.
bsnOldDefaultIdCert	RSA	Flash	1536-bit RSA private key used to authenticate to the access point, generated during the manufacturing process. Zeroized by the zeroization process.
bsnDefaultIdCert	RSA	Flash	1536-bit RSA private key, not used in FIPS mode. Zeroized by the zeroization process.
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. Zeroized by the zeroization process.
Pre-shared key (PSK)	Shared secret	Flash	The 802.11i preshared key (PSK). This key is optionally used as a PMK. Zeroized by overwriting with a new value.
TLS Pre-Master Secret	Shared secret	SDRAM	Shared secret created using asymmetric cryptography from which new TLS session keys can be created. Zeroized at the end of the TLS session.
TLS Encryption Key	AES	SDRAM	128-bit AES key used to encrypt session data. Zeroized at the end of the TLS session.

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

Name	Algorithm	Storage	Description and Zeroization
TLS Integrity Key	HMAC- SHA-1	SDRAM	HMAC-SHA-1 key used for integrity protection. Zeroized at the end of the TLS session.
LWAPP Session Key	AES-CCM	SDRAM	The session key used to encrypt and integrity check LWAPP traffic. Zeroized when the controller disconnects from the access point or when the module resets.
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. Zeroized when the RSNA terminates.
802.11i Key Encryption Key (KEK)	AES	SDRAM	The KEK is used by the EAPOL-Key frames to provide confidentiality in the 4-Way Handshake and Group Key Handshake messages. Zeroized when the RSNA terminates.
802.11i Temporal Key (TK)	AES-CCM	SDRAM	The TK, also known as the CCMP key, is the 802.11i session key for unicast communications. Zeroized when the RSNA terminates.
802.11i Group Temporal Key (GTK)	AES-CCM	SDRAM	The GTK is the 802.11i session key for broadcast communications. Zeroized when the RSNA terminates.
Radius secret	Shared secret	Flash	Used to authenticate to a RADIUS server. Zeroized during the zeroization procedure.
AES KeyWrap KEK	AES	Flash	The key encrypting key used by the AES Key Wrap algorithm to protect the PMK. Zeroized during the zeroization procedure.
AES KeyWrap MACK	AES	Flash	The MAC key used by the AES Key Wrap algorithm to authenticate RADIUS conversation. Zeroized during the zeroization procedure.

Table 3 Public Keys

Name	Algorithm	Storage	Description and Zeroization
bsnOldDefaultCaCert	RSA	Flash	Verification certificate, used for LWAPP authentication. Zeroized during the zeroization procedure.
bsnDefaultRootCaCert	RSA	Flash	Verification certificate, used for LWAPP authentication. Zeroized during the zeroization procedure.
bsnDefaultCaCert	RSA	Flash	Verification certificate, used for LWAPP authentication. Zeroized during the zeroization procedure.
bsnDefaultBuildCert	RSA	Flash	Verification certificate, used to validate the controller’s firmware image. Zeroized during the zeroization procedure.
cscoDefaultNewRootCaCert	RSA	Flash	Verification certificate, not used in FIPS mode of operations. Zeroized during the zeroization procedure.
cscoDefaultMfgCaCert	RSA	Flash	Verification certificate, used with LWAPP to authenticate the access point. Zeroized during the zeroization procedure.
cscoDefaultDevCaCert	RSA	Flash	Verification certificate, used with LWAPP to authenticate the access point. Zeroized during the zeroization procedure.
cscoDefaultR3CaCert	RSA	Flash	Verification certificate, not used in FIPS mode of operations. Zeroized during the zeroization procedure.
bsnOldDefaultCaCert	RSA	Flash	Verification certificate, not used in FIPS mode of operations. Zeroized during the zeroization procedure.
bsnOldDefaultIdCert	RSA	Flash	Authentication certificate, used to authenticate to the access point. Zeroized during the zeroization procedure.

Table 3 Public Keys (continued)

Name	Algorithm	Storage	Description and Zeroization
bsnDefaultIdCert	RSA	Flash	Authentication certificate, not used in FIPS mode of operations. Zeroized during the zeroization procedure.
bsnSslWebadminCert	RSA	Flash	Server certificate used for HTTPS-TLS. Zeroized during the zeroization procedure.

Table 4 Key/CSP Access by Service

Service	Key Access
Self Test and Initialization	• Initializes PRNG seed
System Status	• None
Key Management	• Read/Write PSK
Module Configuration	• Modify user passwords
Supervisor Authentication Data Zeroization	• Supervisor user passwords
SNMPv3	• SNMPv3 user password
LWAPP	• Verify with cscoDefaultNewRootCaCert and cscoDefaultMfgCaCert • Sign with bsnOldDefaultIdCert Private Key • Read (and transmit) bsnOldDefaultIdCert Certificate • Establish and then encrypt/decrypt with LWAPP Session Key
TLS	• 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
802.11i	• Compute KCK, KEK, and PTK from PMK • Generate GTK • Encrypt/decrypt using KEK • Authenticate data using KCK
RADIUS	• Decrypt 802.11i PMK using KeyWrap KEK • Authenticate data using KeyWrap MACK

Key Zeroization

All keys in the WiSM controllers can be zeroized by entering this CLI command:

```
> 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
- HMAC MD5

Self Tests

The following self tests are performed by the module:

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

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

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

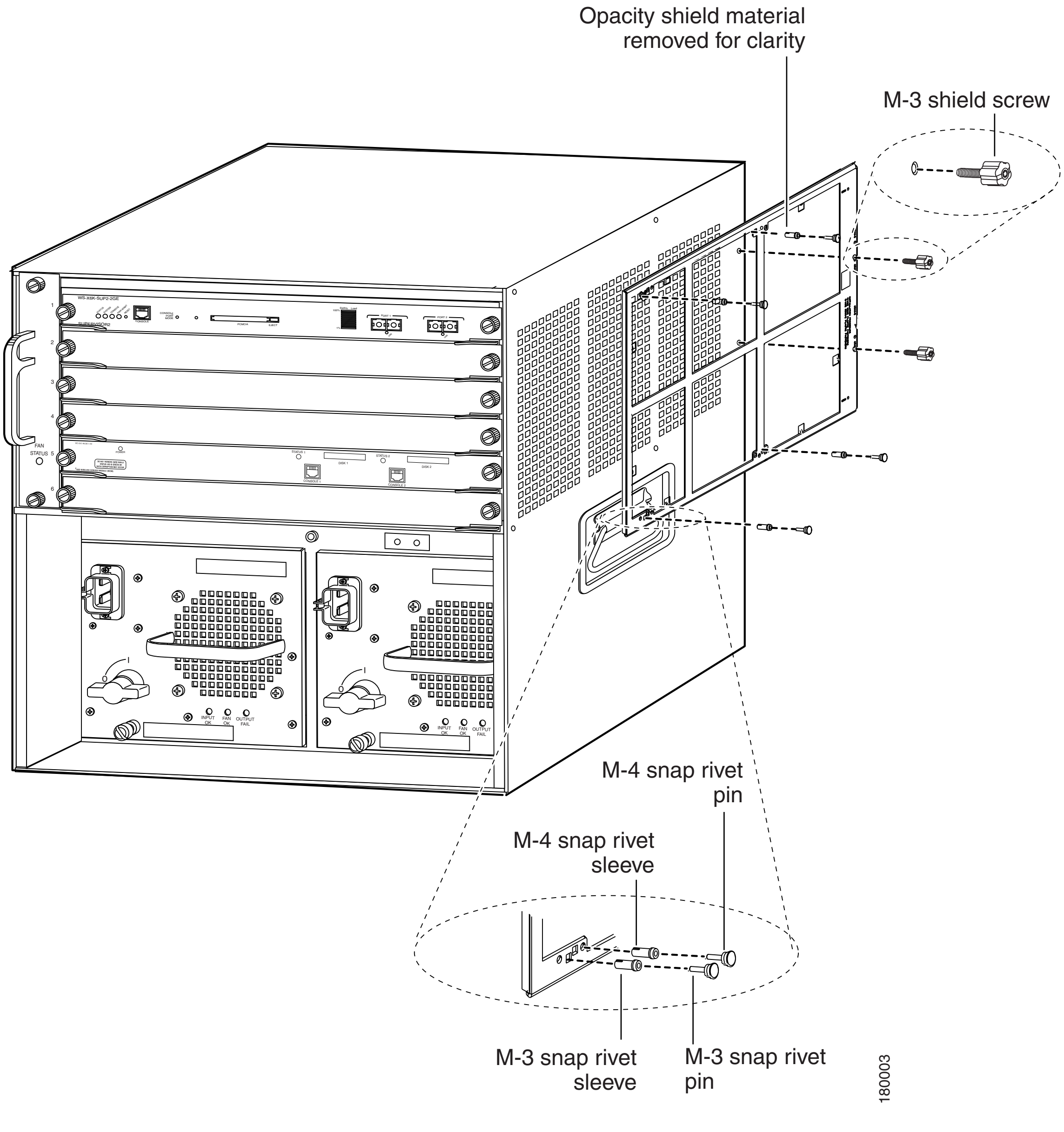
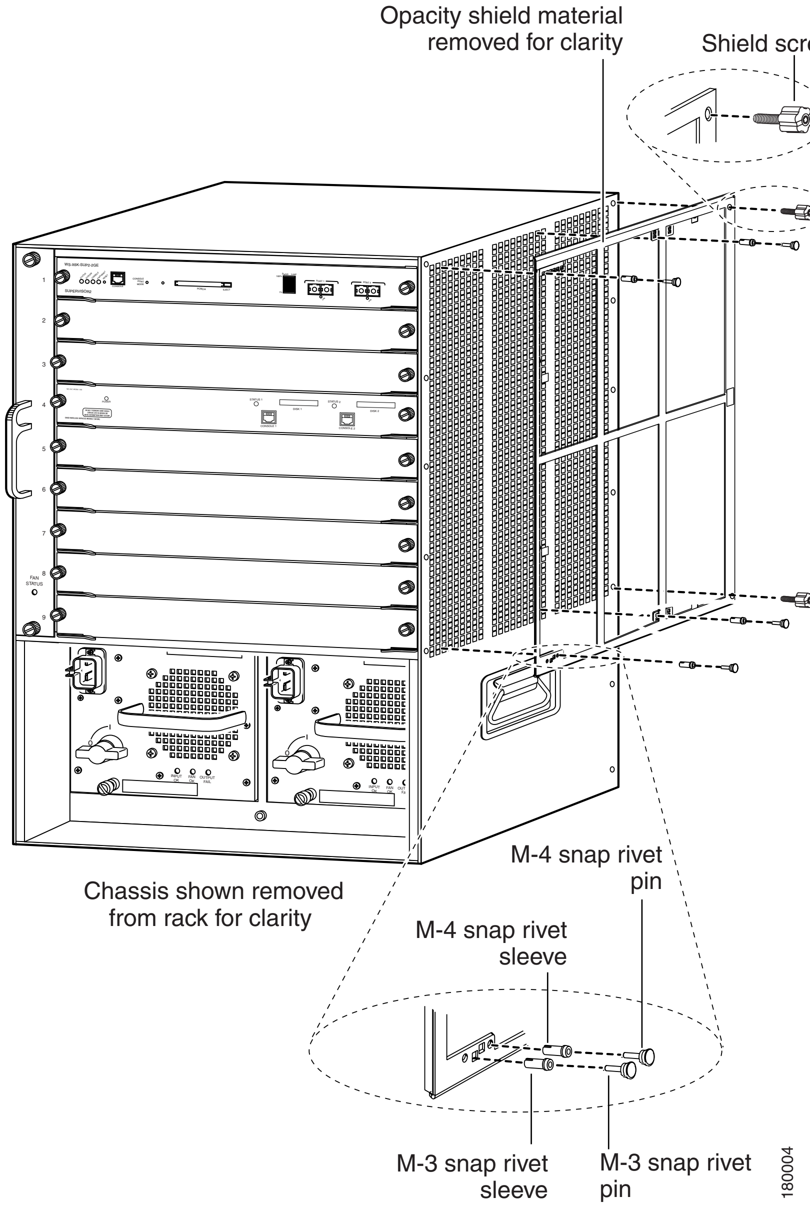


Figure 4 Installing the Opacity Shield on the Catalyst 6509 or Catalyst 6509E Switch



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 engines, and console connectors are provided on the WiSM. The power cable connection and a power switch are provided on the power supply of all the 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.

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 Engine 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 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 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 Engine 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 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.

Step 4 Place labels on each WiSM installed in the chassis as shown in the figures below.

a. 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

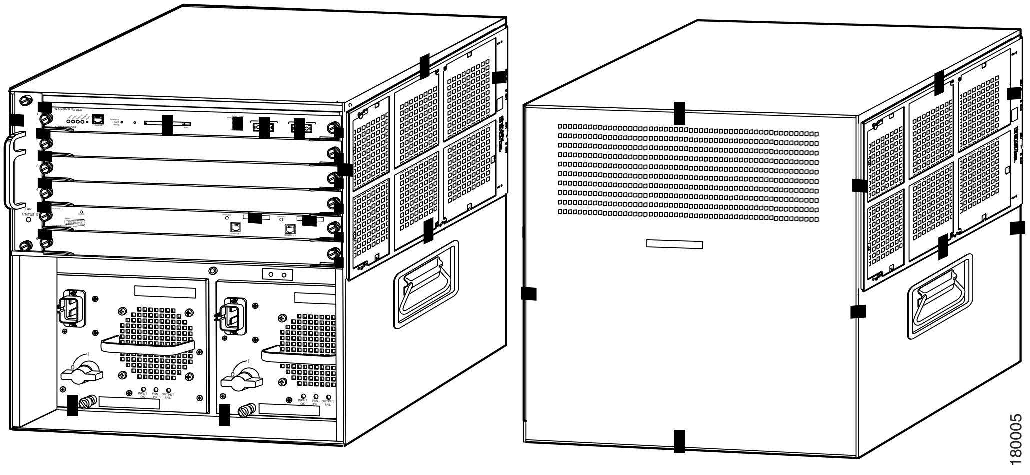
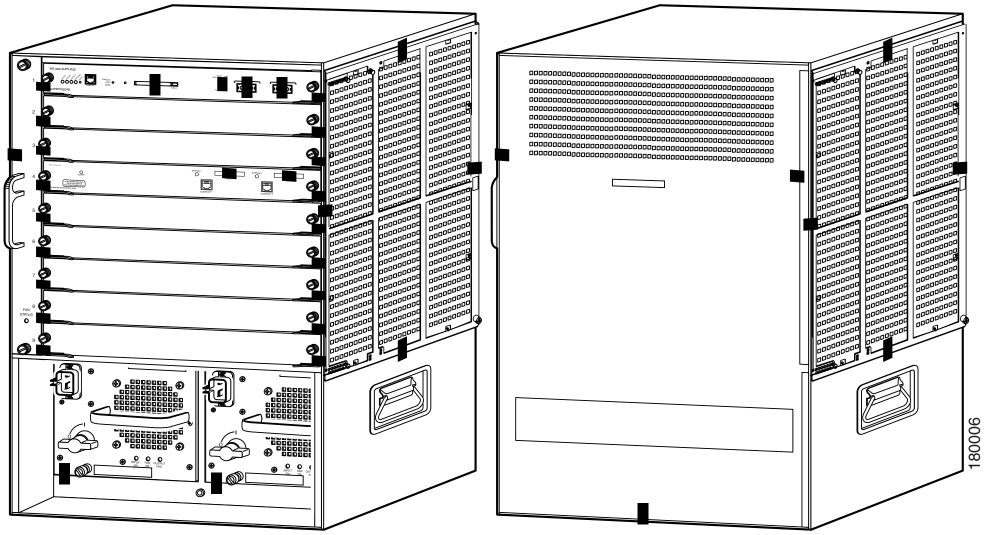


Figure 6 Catalyst 6509 and Catalyst 6509E Switch Chassis Tamper-Evidence Label Placement



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.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

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

http://www.cisco.com/techsupport

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

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

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

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

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

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

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

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

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 will find information about how to do the following:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

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

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

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

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

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco 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 at this URL:

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

Access to all tools on the Cisco 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 Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This 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.

Tip **Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

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 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 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)—An existing 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 operations 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 the network is impaired while 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.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, 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

- *Internet Protocol Journal* is a quarterly journal published by Cisco 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

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- 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

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.