Cisco 3825 and Cisco 3845 Integrated Services Routers FIPS 140-2 Non Proprietary Security Policy

Level 2 Validation
Version 1.1
November 1, 2005

Introduction

This document is the non-proprietary Cryptographic Module Security Policy for the Cisco 3825 and Cisco 3845 Integrated Services Routers without an AIM card installed. This security policy describes how the Cisco 3825 and Cisco 3845 Integrated Services Routers (Hardware Version: Cisco 3825 or Cisco 3845; Firmware Version: IOS 12.3(11)T03) meet the security requirements of FIPS 140-2, and how to operate the router with on-board crypto enabled in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the Cisco 3825 and Cisco 3845 Integrated Services Routers.

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/.

This document contains the following sections:

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

References

This document deals only with operations and capabilities of the Cisco 3825 and Cisco 3845 routers in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the routers from the following sources:

- The Cisco Systems website contains information on the full line of Cisco Systems routers. Please refer to the following website:

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

- For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.
- The NIST Validated Modules website (http://csrc.nist.gov/cryptval) contains contact information for answers to technical or sales-related questions for the module.

Terminology

In this document, the Cisco 3825 or Cisco 3845 routers are referred to as the router, the module, or the system.

Document Organization

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

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

This document provides an overview of the routers and explains their secure configuration and operation. This introduction section is followed by the "Cisco 3825 and Cisco 3845 Routers" section on page 2, which details the general features and functionality of the router. The "Secure Operation of the Cisco 3825 or Cisco 3845 router" section on page 23 specifically addresses the required configuration for the FIPS-mode of operation.

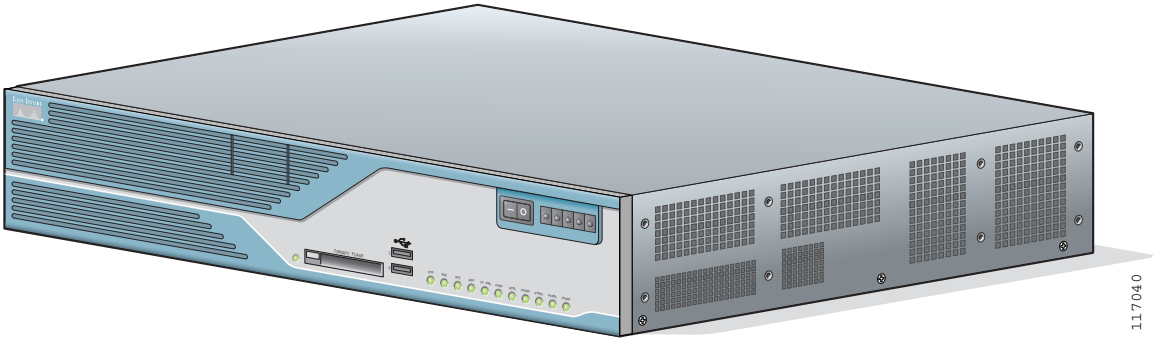
With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

Cisco 3825 and Cisco 3845 Routers

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 Cisco 3825 and Cisco 3845 routers provide a scalable, secure, manageable remote access server that meets FIPS 140-2 Level 2 requirements. This section describes the general features and functionality provided by the routers. The following subsections describe the physical characteristics of the routers.

The Cisco 3825 Cryptographic Module Physical Characteristics

Figure 1 The Cisco 3825 Router Case



The Cisco 3825 Router is a multiple-chip standalone cryptographic module. The router has a processing speed of 500MHz. Depending on configuration, either the internal Safenet chip or the IOS software is used for cryptographic operations.

The cryptographic boundary of the module is the device's case. All of the functionality discussed in this document is provided by components within this cryptographic boundary.

The interface for the router is located on the rear and front panels as shown in Figure 2 and Figure 3, respectively.

Figure 2 Cisco 3825 Rear Panel Physical Interfaces

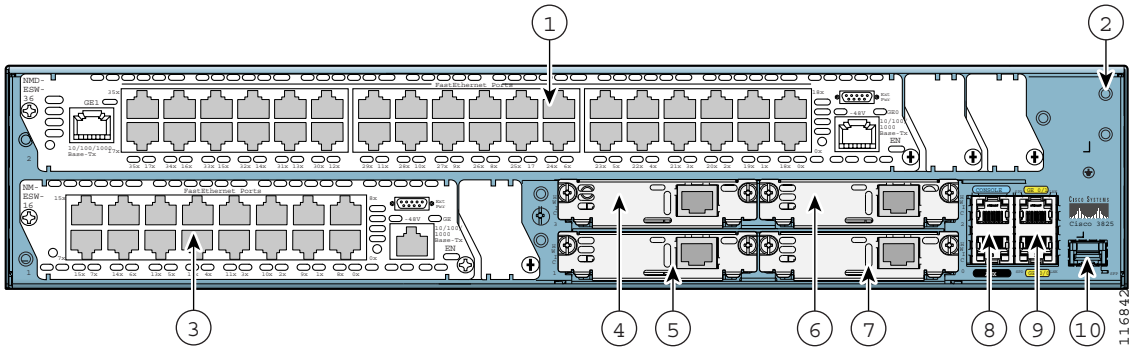
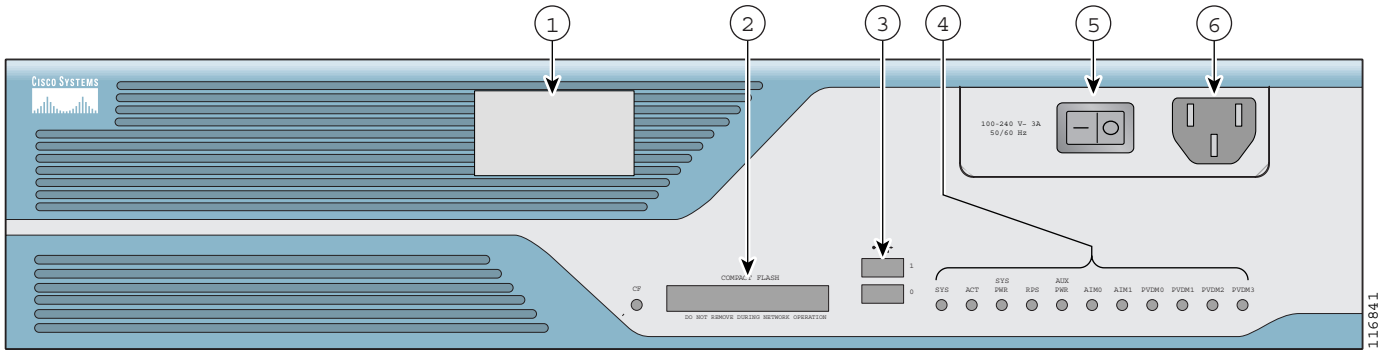


Figure 3 Cisco 3825 Front Panel Physical Interfaces



The Cisco 3825 router features a console port, auxiliary port, dual Universal Serial Bus (USB) ports, four high-speed WAN interface card (HWIC) slots, two 10/100/1000 Gigabit Ethernet RJ45 ports, two Enhanced Network Module (ENM) slots, small form factor pluggable (SFP), redundant power supply (RPS) inlet, power inlet, and Compact Flash (CF) drive. The Cisco 3825 router supports two internal advanced integration modules (AIMs)[1], and two Ethernet connections. Figure 2 shows the rear panel and Figure 3 shows the front panel. The front panel consists of 12 LEDs: CF LED, SYS LED, ACT LED, SYS PWR LED, RPS LED, AUX PWR LED, AIM0 LED, AIM1 LED, PVDM0 LED, PVDM1 LED, PVDM2 LED, and PVDM3 LED. The back panel contains LEDs to indicate the status of the GE ports.

The front panel contains the following:

- LEDs
- Power switch
- Power input
- CF drive
- USB ports

The rear panel contains the following:

- HWIC/WIC/VIC slots 0 and 1
- Console port
- Auxiliary port
- GE ports
- ENM Ports
- SFP Port

Table 1 and Table 2 provide more detailed information conveyed by the LEDs on the front and rear panel of the router:

1. However, an AIM module may not be installed in accordance with this security policy. There is a separate security policy covering the Cisco 3825 and Cisco 3845 routers with AIM module installed.

Table 1 Cisco 3825 Front Panel Indicators

Name	State	Description
System	Solid Green	Normal System Operation.
	Blinking Green	Booting or in ROM monitor (ROMMON) mode.
	Amber	Powered, but malfunctioning.
	Off	Router is not receiving power.
System Power	Green	Power supply present and enabled.
	Amber	Power supply present and off or with failure.
	Off	Power supply not present.
Auxiliary Power	Green	Indicates IP phone power supply present.
	Amber	Indicates IP phone power supply present.
	Off	IP phone power supply not present.
Redundant Power Supply	Green	System running on RPS PSU.
	Off	System running on primary PSU.
Activity	Green	Solid or blinking indicates packet activity.
	Off	No interrupts or packet transfer occurring.
Compact Flash	Solid Green	Compact Flash present and enabled.
	Blinking Green	Compact Flash accessed.
	Off	Compact Flash not present.
PVDM3	Green	PVDM3 installed and initialized.
	Amber	PVDM3 installed and initialized error.
	Off	PVDM3 not installed.
PVDM2	Green	PVDM2 installed and initialized.
	Amber	PVDM2 installed and initialized error.
	Off	PVDM2 not installed.
PVDM1	Green	PVDM1 installed and initialized.
	Amber	PVDM1 installed and initialized error.
	Off	PVDM1 not installed.
PVDM0	Green	PVDM0 installed and initialized.
	Amber	PVDM0 installed and initialized error.
	Off	PVDM0 not installed.
AIM1	Green	AIM1 present and enabled.
	Amber	AIM1 present with failure.
	Off	AIM1 not installed.
AIM0	Green	AIM0 present and enabled.
	Amber	AIM0 present with failure.
	Off	AIM0 not installed.

Table 2 Cisco 3825 Rear Panel Indicators

Name	State	Description
Speed	Green (Blinking)	Blinking frequency indicates port speed.
Link	Solid Green	Ethernet link is established
	Off	No link established

Table 3 describes the meaning of Ethernet LEDs on the rear panel:

Table 3 Cisco 3825 Ethernet Indicators

Name	State	Description
Duplex	Solid Green	Full-Duplex
	Off	Half-Duplex
Speed	Solid Green	100 Mbps
	Off	10 Mbps
Link	Solid Green	Ethernet link is established
	Off	No link established

The physical interfaces are separated into the logical interfaces from FIPS 140-2 as described in Table 4:

Table 4 Cisco 3825 FIPS 140-2 Logical Interfaces

Router Physical Interface	FIPS 140-2 Logical Interface
10/100/1000 Ethernet LAN Ports HWIC Ports Console Port Auxiliary Port ENM Slots SFP	Data Input Interface
10/100/1000 Ethernet LAN Ports HWIC Ports Console Port Auxiliary Port ENM Slots SFP	Data Output Interface

Table 4 Cisco 3825 FIPS 140-2 Logical Interfaces (Continued)

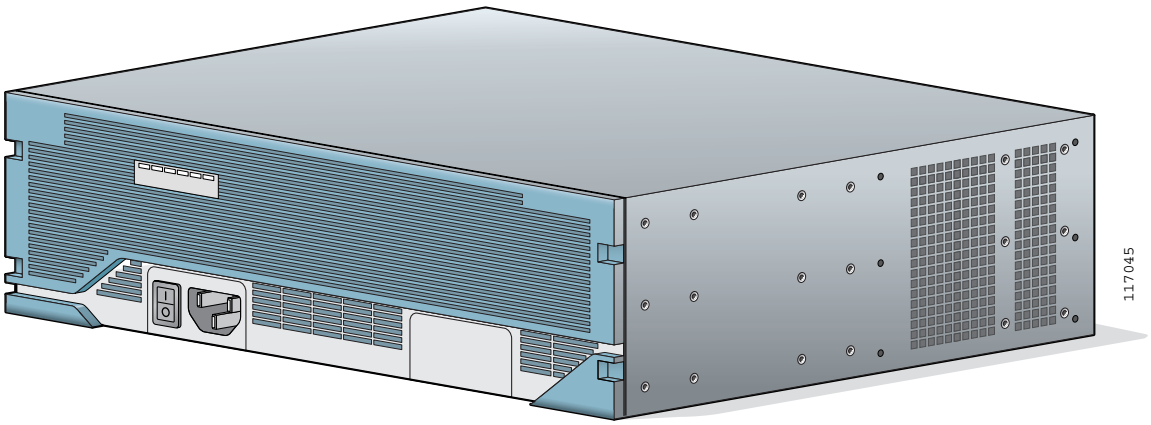
10/100/1000 Ethernet LAN Ports HWIC Ports Console Port Auxiliary Port ENM Slots SFP	Control Input Interface
10/100/1000 Ethernet LAN LEDs SFP LED AIM LEDs PVDM LEDs Power LED System Activity LED System LED Compact Flash LED Auxiliary Power LED RPS LED Console Port Auxiliary Port	Status Output Interface
Power Plug Redundant Power Supply Plug	Power Interface

There are two USB ports but they are not supported currently. The ports will be supported in the future for smartcard or token reader.

The CF card that stored the IOS image is considered an internal memory module, because the IOS image stored in the card may not be modified or upgraded. The card itself must never be removed from the drive. Tamper evident seal will be placed over the card in the drive.

The Cisco 3845 Cryptographic Module Physical Characteristics

Figure 4 The Cisco 3845 Router Case



The Cisco 3845 router with on-board crypto enabled is a multiple-chip standalone cryptographic module. The router has a processing speed of 650MHz. Depending on configuration, either the internal Safenet chip or the IOS software is used for cryptographic operations.

The cryptographic boundary of the module is the device's case. All of the functionality discussed in this document is provided by components within this cryptographic boundary.

The interfaces for the router are located on the front and rear panel as shown in Figure 5 and Figure 6, respectively.

Figure 5 Cisco 3845 Front Panel Physical Interfaces

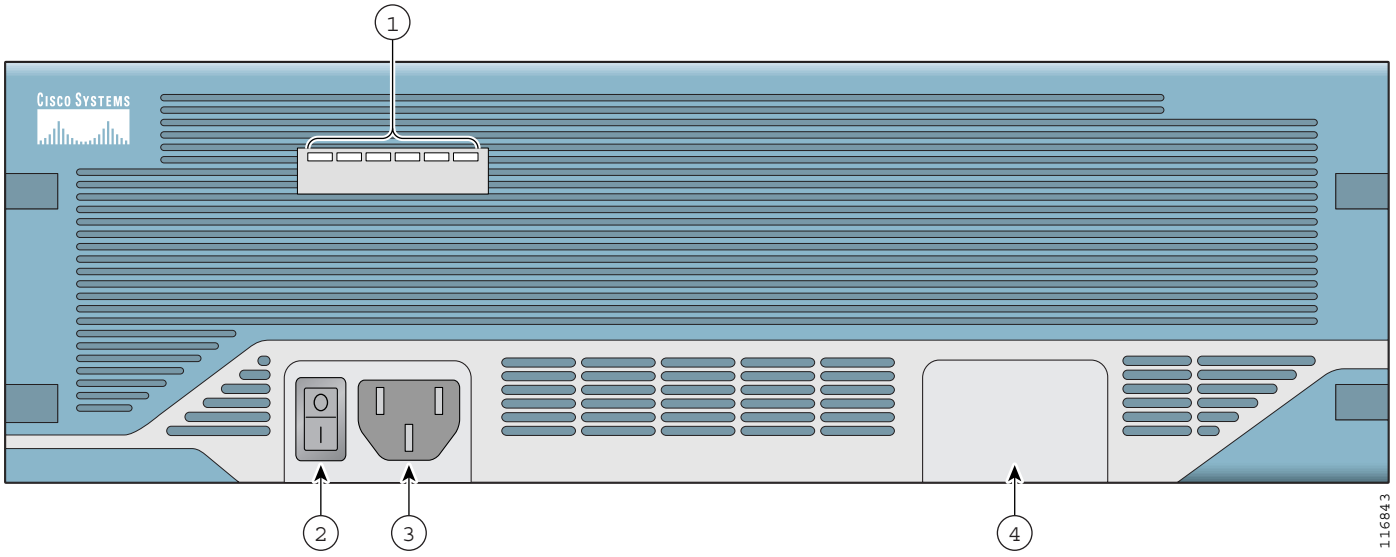
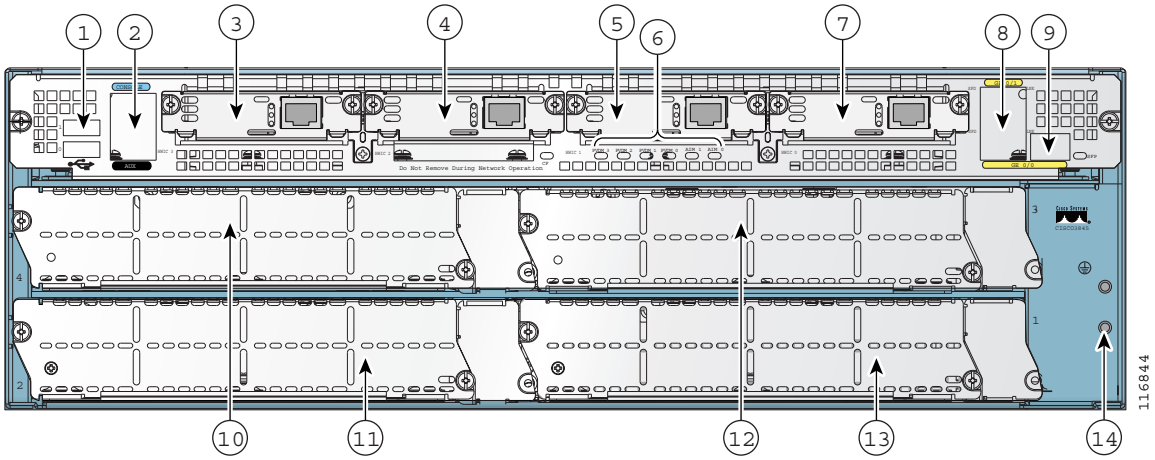


Figure 6 Cisco 3845 Rear Panel Physical Interfaces



The Cisco 3845 router features a console port, auxiliary port, dual Universal Serial Bus (USB) ports, four high-speed WAN interface card (HWIC) slots, two 10/100/1000 Gigabit Ethernet RJ45 ports, four Enhanced Network Module (ENM) slots, small form factor pluggable (SFP), power inlets, and Compact Flash (CF) drive. The Cisco 3845 router supports two internal advanced integration modules (AIMs)[1], and two Ethernet connections. Figure 5 shows the front panel and Figure 6 shows the rear panel. The front panel consists of 7 LEDs: CF LED, PVDM0 LED, PVDM1 LED, PVDM2 LED, PVDM3 LED, AIM0 LED, and AIM1 LED. The back panel consists of 6 LEDs: SYS LED, ACT LED, SYS PWR1 LED, AUX PWR1 LED, SYS PWR2 LED, and AUX PWR2 LED.

The front panel contains the following:

- LEDs
- Power switch
- Power input

The rear panel contains the following:

- CF drive
- USB ports
- Console and Auxiliary ports
- HWIC ports
- LEDs
- HWIC ports
- GE ports
- SFP port
- ENM slots

Table 5 provides more detailed information conveyed by the LEDs on the front of the router:

1. However, an AIM module may not be installed in accordance with this security policy. There is a separate security policy covering the Cisco 3825 and Cisco 3845 routers with AIM module installed.

Table 5 Cisco 3845 Front Panel Indicators

Name	State	Description
System	Solid Green	Normal System Operation.
	Blinking Green	Booting or in ROM monitor (ROMMON) mode.
	Amber	Powered, but malfunctioning.
	Off	Router is not receiving power.
System Power1	Green	Power1 supply present and enabled.
	Amber	Power1 supply present and off or with failure.
	Off	Power1 supply not present.
Auxiliary Power1	Green	Indicates IP phone power1 supply present.
	Amber	Indicates IP phone power1 supply present.
	Off	IP phone power1 supply not present.
System Power2	Green	Power2 supply present and enabled.
	Amber	Power2 supply present and off or with failure.
	Off	Power2 supply not present.
Auxiliary Power2	Green	Indicates IP phone power2 supply present.
	Amber	Indicates IP phone power2 supply present.
	Off	IP phone power2 supply not present.
Activity	Green	Solid or blinking indicates packet activity.
	Off	No interrupts or packet transfer occurring.
Compact Flash	Solid Green	Compact Flash present and enabled.
	Blinking Green	Compact Flash accessed.
	Off	Compact Flash not present.
PVDM3	Green	PVDM3 installed and initialized.
	Amber	PVDM3 installed and initialized error.
	Off	PVDM3 not installed.
PVDM2	Green	PVDM2 installed and initialized.
	Amber	PVDM2 installed and initialized error.
	Off	PVDM2 not installed.
PVDM1	Green	PVDM1 installed and initialized.
	Amber	PVDM1 installed and initialized error.
	Off	PVDM1 not installed.
PVDM0	Green	PVDM0 installed and initialized.
	Amber	PVDM0 installed and initialized error.
	Off	PVDM0 not installed.

Table 5 Cisco 3845 Front Panel Indicators (Continued)

AIM1	Green Amber Off	AIM1 present and enabled. AIM1 present with failure. AIM1 not installed.
AIM0	Green Amber Off	AIM0 present and enabled. AIM0 present with failure. AIM0 not installed.

Table 6 describes the meaning of Ethernet LEDs on the front panel:

Table 6 Cisco 3845 Ethernet Indicators

Name	State	Description
Speed	One Blinking Green Two Blinking Green Three Blinking Green	10 Mbps 100 Mbps 1000Mbps
Link	Solid Green Off	Ethernet link is established No link established
SFP	Solid Green Off	SFP fiber link is established No link established

The physical interfaces are separated into the logical interfaces from FIPS 140-2 as described in Table 7:

Table 7 Cisco 3845 FIPS 140-2 Logical Interfaces

Router Physical Interface	FIPS 140-2 Logical Interface
10/100/1000 Ethernet LAN Ports HWIC Ports Console Port Auxiliary Port ENM Slots SFP	Data Input Interface
10/100/1000 Ethernet LAN Ports HWIC Ports Console Port Auxiliary Port ENM Slots SFP	Data Output Interface

Table 7 Cisco 3845 FIPS 140-2 Logical Interfaces (Continued)

10/100/1000 Ethernet LAN Ports HWIC Ports Console Port Auxiliary Port ENM Slots SFP	Control Input Interface
10/100/1000 Ethernet LAN LEDs SFP LED AIM LEDs PVDM LEDs System Power LEDs System Activity LED System LED Compact Flash LED Auxiliary Power LEDs Console Port Auxiliary Port	Status Output Interface
Power Plug	Power Interface

There are two USB ports but they are not supported currently. The ports will be supported in the future for smartcard or token reader.

The CF card that stored the IOS image is considered an internal memory module. The reason is the IOS image stored in the card cannot be modified or upgraded. The card itself must never be removed from the drive. Tamper evident seal will be placed over the card in the drive.

Roles and Services

Authentication in Cisco 3825 and Cisco 3845 is role-based. There are two main roles in the router that operators can assume: the Crypto Officer role and the User role. The administrator of the router assumes the Crypto Officer role in order to configure and maintain the router using Crypto Officer services, while the Users exercise only the basic User services. The module supports RADIUS and TACACS+ for authentication. A complete description of all the management and configuration capabilities of the router can be found in the *Performing Basic System Management* manual and in the online help for the router.

User Services

Users enter the system by accessing the console port with a terminal program or via IPSec protected telnet or SSH session to a LAN port. The IOS prompts the User for username and password. If the password is correct, the User is allowed entry to the IOS executive program.

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

- **Status Functions**—View state of interfaces and protocols, version of IOS currently running.
- **Network Functions**—Connect to other network devices through outgoing telnet, PPP, etc. and initiate diagnostic network services (i.e., ping, mtrace).
- **Terminal Functions**—Adjust the terminal session (e.g., lock the terminal, adjust flow control).
- **Directory Services**—Display directory of files kept in flash memory.

Crypto Officer Services

During initial configuration of the router, the Crypto Officer password (the "enable" password) is defined. A Crypto Officer can assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration and maintenance of the router. The Crypto Officer services consist of the following:

- **Configure the router**—Define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, and load authentication information.
- **Define Rules and Filters**—Create 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.
- **View Status Functions**—View the router configuration, routing tables, active sessions, use gets to view SNMP MIB statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.
- **Manage the router**—Log off users, shutdown or reload the outer, manually back up router configurations, view complete configurations, manager user rights, and restore router configurations.
- **Set Encryption/Bypass**—Set up the configuration tables for IP tunneling. Set keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.

Physical Security

The router is entirely encased by a metal, opaque case. The rear of the unit contains auxiliary port, console port, Gigabit Ethernet ports, HWIC ports, and ENM slots. The front of the unit contains USB connectors, CF drive, power inlets, power switch, and LEDs. The top, side, and front portion of the chassis can be removed to allow access to the motherboard, memory, AIM slots, and expansion slots.

Once the router has been configured in to meet FIPS 140-2 Level 2 requirements, the router cannot be accessed without signs of tampering. To seal the system, apply serialized tamper-evidence labels as follows:

To apply serialized tamper-evidence labels to the Cisco 3825:

Step 1 Clean the cover of any grease, dirt, or oil before applying the tamper evidence labels. Alcohol-based cleaning pads are recommended for this purpose. The temperature of the router should be above 10 C.

Step 2 Tamper evidence label A shall be placed so that one half of the label covers the top of the front panel and the other half covers the enclosure.

Step 3 Tamper evidence label B shall be placed so that one half of the label covers the bottom of the front panel and the CF card and the other half covers the enclosure.

Step 4 Tamper evidence labels C and D should be placed so that the one half of the label covers the enclosure and the other half covers the left and right upper ENM slots.

Step 5 Tamper evidence label E should be placed so that the one half of the label covers the lower right ENM slot and the other half covers the enclosure.

Step 6 Tamper evidence label F should be placed so that the one half of the label covers the left upper and lower HWIC slots and the other half covers the enclosure.

Step 7 Tamper evidence label G should be placed so that the one half of the label covers the right upper and lower HWIC slots and the other half covers the enclosure.

Step 8 Allow the labels five minutes to completely cure.

Figure 7 and Figure 8 show the tamper evidence label placements for the Cisco 3825.

Figure 7 Cisco 3825 Tamper Evident Label Placement (Front View)

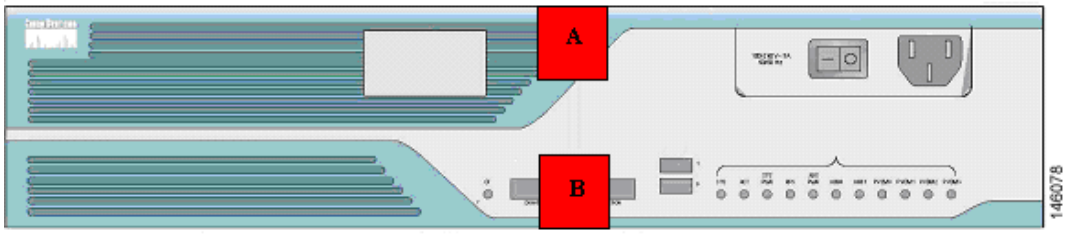
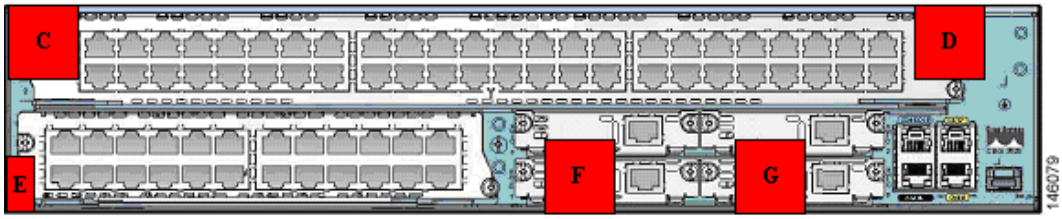


Figure 8 Cisco 3825 Tamper Evident Label Placement (Back View)



To apply serialized tamper-evidence labels to the Cisco 3845:

Step 1 Clean the cover of any grease, dirt, or oil before applying the tamper evidence labels. Alcohol-based cleaning pads are recommended for this purpose. The temperature of the router should be above 10 C.

Step 2 Tamper evidence labels A and B should be placed so that one half of the label covers the front panel and the other half covers the enclosure.

Step 3 Tamper evidence label C should be placed so that one half of the label covers the left upper and lower ENM modules and the other half covers the enclosure.

Step 4 Tamper evidence labels D and E should be placed so that one half of each label covers the side of right ENM modules and the other half covers the enclosure.

Step 5 Tamper evidence labels F, G, H and I should be placed so that one half of each label covers the top side of HWIC modules and the other half covers the enclosure.

Step 6 Tamper evidence label J should be placed over the CF slot.

Step 7 Allow the labels five minutes to completely cure.

Figure 9 and Figure 10 show the tamper evidence label placements for the Cisco 3845.

Figure 9 Cisco 3845 Tamper Evident Label Placement (Front View)

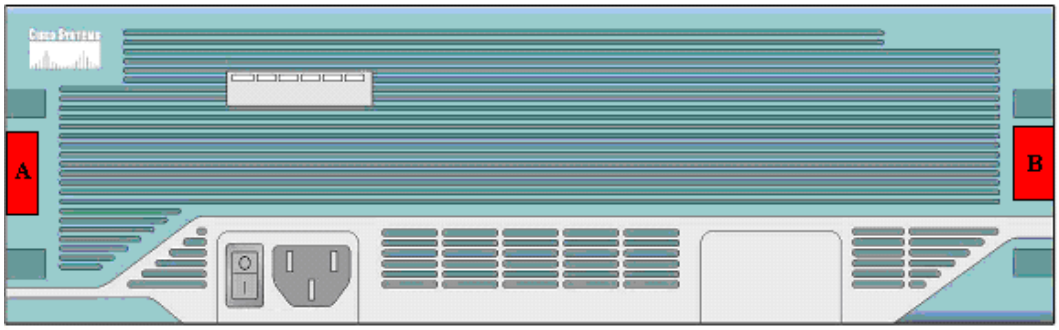
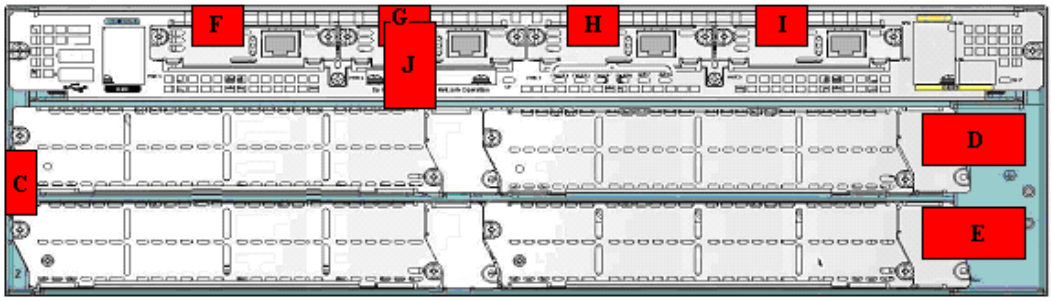


Figure 10 Cisco 3845 Tamper Evident Label Placement (Back View)



The tamper evidence seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the router will damage the tamper evidence seals or the material of the module cover. Since the tamper evidence seals have non-repeated serial numbers, they can be inspected for damage and compared against the applied serial numbers to verify that the module has not been tampered. 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 router securely administers both cryptographic keys and other critical security parameters such as passwords. The tamper evidence seals provide physical protection for all keys. All keys are also protected by the password-protection on the Crypto Officer role login, and can be zeroized by the Crypto Officer. All zeroization consists of overwriting the memory that stored the key. Keys are exchanged and entered electronically or via Internet Key Exchange (IKE).

The routers support the following FIPS 140-2 approved algorithm implementations:

- Software (IOS) implementations
  - AES
  - DES (for legacy use only)
  - 3DES
  - SHA-1
  - HMAC-SHA-1
  - X9.31 PRNG
- Onboard hardware implementations (Safenet chip)
  - AES
  - DES (for legacy use only)
  - 3DES
  - SHA-1
  - HMAC-SHA-1

The router is in the approved mode of operation only when FIPS 140-2 approved algorithms are used (except DH which is allowed for use in FIPS approved mode for key establishment). The following are not FIPS 140-2 approved algorithms: RC4, MD5, HMAC-MD5, RSA and DH. DH is allowed for use in key establishment. The key establishment methodology provides between 80-bits and 96-bits of encryption strength.

The module supports two types of key management schemes:

- Pre-shared key exchange via electronic key entry. DES/3DES/AES key and HMAC-SHA-1 key are exchanged and entered electronically.
- Internet Key Exchange method with support for pre-shared keys exchanged and entered electronically.
  - The pre-shared keys are used with Diffie-Hellman key agreement technique to derive DES, 3DES or AES keys.
  - The pre-shared key is also used to derive HMAC-SHA-1 key.

The module supports commercially available methods of key establishment, including Diffie-Hellman and IKE. See Document 7A, Cisco IOS Reference Guide.

All pre-shared 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 via the IKE protocol.

Key Zeroization:

Each key can be zeroized by sending the “no” command prior to the key function commands. This will zeroize each key from the DRAM, the running configuration.

“Clear Crypto IPSec SA” will zeroize the IPSec DES/3DES/AES session key (which is derived using the Diffie-Hellman key agreement technique) from the DRAM. This session key is only available in the DRAM; therefore this command will completely zeroize this key. The following command will zeroize the pre-shared keys from the DRAM:

- no set session-key inbound ah spi hex-key-data

- no set session-key outbound ah spi hex-key-data
- no set session-key inbound esp spi cipher hex-key-data [authenticator hex-key-data]
- no set session-key outbound esp spi cipher hex-key-data [authenticator hex-key-data]

The DRAM running configuration must be copied to the start-up configuration in NVRAM in order to completely zeroize the keys.

The following commands will zeroize the pre-shared keys from the DRAM:

- no crypto isakmp key key-string address peer-address
- no crypto isakmp key key-string hostname peer-hostname

The DRAM running configuration must be copied to the start-up configuration in NVRAM in order to completely zeroize the keys.

The module supports the following keys and critical security parameters (CSPs). Note that keys stored in NVRAM are in plaintext unless the configuration file encryption key is configured via the "key config-key" command is used.

Table 8 Cryptographic Keys and CSPs

Name	Algorithm	Description	Storage	Zeroization Method
PRNG Seed	X9.31	This is the seed for X9.31 PRNG. This CSP is stored in DRAM and updated periodically after the generation of 400 bytes – after this it is reseeded with router-derived entropy; hence, it is zeroized periodically. Also, the operator can turn off the router to zeroize this CSP.	DRAM (plaintext)	Automatically every 400 bytes, or turn off the router.
Diffie Hellman private exponent	DH	The private exponent used in Diffie-Hellman (DH) exchange. Zeroized after DH shared secret has been generated.	DRAM (plaintext)	Automatically after shared secret generated.
Diffie Hellman public key	DH	The public key used in Diffie-Hellman (DH) exchange as part of IKE. Zeroized after the DH shared secret has been generated.	DRAM (plaintext)	Automatically after shared secret generated.
skeyid	Keyed SHA-1	Value derived from the shared secret within IKE exchange. Zeroized when IKE session is terminated.	DRAM (plaintext)	Automatically after IKE session terminated.
skeyid_d	Keyed SHA-1	The IKE key derivation key for non ISAKMP security associations.	DRAM (plaintext)	Automatically after IKE session terminated.
skeyid_a	SHA-1 HMAC or DES MAC	The ISAKMP security association authentication key.	DRAM (plaintext)	Automatically after IKE session terminated.
skeyid_e	DES/TDES /AES	The ISAKMP security association encryption key.	DRAM (plaintext)	Automatically after IKE session terminated.
IKE session encrypt key	DES/TDES /AES	The IKE session encrypt key.	DRAM (plaintext)	Automatically after IKE session terminated.
IKE session authentication key	SHA-1 HMAC or DES MAC	The IKE session authentication key.	DRAM (plaintext)	Automatically after IKE session terminated.

Table 8 Cryptographic Keys and CSPs (Continued)

ISAKMP preshared	Secret	The key used to generate IKE skeyid during preshared-key authentication. “no crypto isakmp key” command zeroizes it. This key can have two forms based on whether the key is related to the hostname or the IP address.	NVRAM (plaintext or encrypted)	“# no crypto isakmp key”
IKE hash key	SHA-1 HMAC	This key generates the IKE shared secret keys. This key is zeroized after generating those keys.	DRAM (plaintext)	
secret_1_0_0		The fixed key used in Cisco vendor ID generation. This key is embedded in the module binary image and can be deleted by erasing the Flash.	NVRAM (plaintext or encrypted)	
IPSec encryption key	DES/TDES /AES	The IPSec encryption key. Zeroized when IPSec session is terminated.	DRAM (plaintext)	Automatically when IPSec session terminated.
IPSec authentication key	SHA-1 HMAC or DES MAC	The IPSec authentication key. The zeroization is the same as above.	DRAM (plaintext)	Automatically when IPSec session terminated.
Configuration encryption key	AES	The key used to encrypt values of the configuration file. This key is zeroized when the “no key config-key” is issued. Note that this command does **not** decrypt the configuration file, so zeroize with care.	NVRAM (plaintext or encrypted)	“# no key config-key”
Router authentication key 1	Shared secret	This key is used by the router to authenticate itself to the peer. The router itself 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 upon completion of authentication attempt.
PPP authentication key	RFC 1334	The authentication key used in PPP. This key is in the DRAM and not zeroized at runtime. One can turn off the router to zeroize this key because it is stored in DRAM.	DRAM (plaintext)	Turn off the router.
Router authentication key 2	Shared Secret	This key is used by the router 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 router itself). Issuing the “no username password” zeroizes the password (that is used as this key) from the local database.	NVRAM (plaintext or encrypted)	“# no username password”
SSH session key	Various symmetric	This is the SSH session key. It is zeroized when the SSH session is terminated.	DRAM (plaintext)	Automatically when SSH session terminated
User password	Shared Secret	The password of the User role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext or encrypted)	Overwrite with new password
Enable password	Shared Secret	The plaintext password of the CO role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext or encrypted)	Overwrite with new password

Table 8 Cryptographic Keys and CSPs (Continued)

Enable secret	Shared Secret	The ciphertext password of the CO role. However, the algorithm used to encrypt this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext or encrypted)	Overwrite with new password
RADIUS secret	Shared Secret	The RADIUS shared secret. This shared secret is zeroized by executing the "no radius-server key" command.	NVRAM (plaintext or encrypted), DRAM (plaintext)	"# no radius-server key"
TACACS+ secret	Shared Secret	The TACACS+ shared secret. This shared secret is zeroized by executing the "no tacacs-server key" command.	NVRAM (plaintext or encrypted), DRAM (plaintext)	"# no tacacs-server key"

Note All RSA operations are prohibited by policy, and commands that can be executed by Officer are shown "# command".

Table 9 Role and Service Access to CSP

SRDI/Role/Service Access Policy	Role/Service	User Role	Status Functions	Network Functions	Terminal Functions	Directory Services	Crypto-Officer Role	Configure the Router	Define Rules and Filters	Status Functions	Manage the Router	Set Encryptions/Bypass	Change WAN Interface Cards
Security Relevant Data Item													
PRNG Seed				r							d	r w d	
DH private exponent				r								r w d	
DH public key				r								r w d	

Table 9 Role and Service Access to CSP (Continued)

SRDI/Role/Service Access Policy	Role/Service	User Role	Status Functions	Network Functions	Terminal Functions	Directory Services	Crypto-Officer Role	Configure the Router	Define Rules and Filters	Status Functions	Manage the Router	Set Encryptions/Bypass	Change WAN Interface Cards
DH public key				r								r w d	
skeyid				r								r w d	
skeyid_d				r								r w d	
skeyid_a				r								r w d	
skeyid_e				r								r w d	
IKE session encrypt key				r								r w d	
IKE session authentication key				r								r w	
ISAKMP preshared				r								r w d	
IKE hash key				r								r w d	
secret_1_0_0				r				r w d					
IPSec encryption key				r								r w d	
IPSec encryption key				r								r w d	

Table 9 Role and Service Access to CSP (Continued)

SRDI/Role/Service Access Policy	Role/Service	User Role	Status Functions	Network Functions	Terminal Functions	Directory Services	Crypto-Officer Role	Configure the Router	Define Rules and Filters	Status Functions	Manage the Router	Set Encryptions/Bypass	Change WAN Interface Cards
Configuration encryption key								r w d			r w d		
Router authentication key				r							r w d		
PPP Authentication key				r							d	r w	
Router authentication key 2				r				r w d					
SSH session key				r								r w d	
User password				r							r w d		
Enable password											r w d		
Enable secret											r w d		
RADIUS secret											r w d		
TACACS+ secret											r w d		

Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The router includes an array of self-tests that are run during startup and periodically during operations. All self-tests are

implemented by the software. An example of self-tests run at power-up is a cryptographic known answer test (KAT) on each of the FIPS-approved cryptographic algorithms and on the Diffie-Hellman algorithm. Examples of tests performed at startup are a software integrity test using an EDC, and a set of Statistical Random Number Generator (RNG) tests. Examples of tests run periodically or conditionally include: a bypass mode test performed conditionally prior to executing IPSec, and a continuous random number generator test. If any of the self-tests fail, the router transitions into an error state. In the error state, all secure data transmission is halted and the router outputs status information indicating the failure.

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

- IOS image integrity checksum failed
- Microprocessor overheats and burns out
- Known answer test failed
- NVRAM module malfunction.
- Temperature high warning

Self-tests performed by the IOS image

IOS Self Tests

- POST tests
  - AES Known Answer Test
  - Software/firmware test
  - Power up bypass test
  - RNG Known Answer Test
  - Diffie Hellman test
  - HMAC-SHA-1 Known Answer Test
  - SHA-1 Known Answer Test
  - DES Known Answer Test
  - 3DES Known Answer Test
- Conditional tests
  - Conditional bypass test
  - Continuous random number generation test

Self-tests performed by Safenet

Safenet Self Tests

- POST tests
  - AES Known Answer Test
  - DES Known Answer Test
  - 3DES Known Answer Test
  - HMAC-SHA-1 Known Answer Test
  - SHA-1 Known Answer Test

Secure Operation of the Cisco 3825 or Cisco 3845 router

The Cisco 3825 and Cisco 3845 routers meet all the Level 2 requirements for FIPS 140-2. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating this router without maintaining the following settings will remove the module from the FIPS approved mode of operation.

Initial Setup

- The Crypto Officer must apply tamper evidence labels as described in the "Physical Security" section on page 13 of this document.
- The Crypto Officer must disable IOS Password Recovery by executing the following commands:

```
configure terminal
no service password-recovery
end
show version
```

Note Once Password Recovery is disabled, administrative access to the module without the password will not be possible.

System Initialization and Configuration

- The Crypto Officer must perform the initial configuration. IOS version 12.3(11)T03, Advanced Security build (advsecurity) is the only allowable image; no other image should be loaded.
- The value of the boot field must be 0x0102. This setting disables break from the console to the ROM monitor and automatically boots the 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 8 characters to include at least one number and one letter 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 8 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
```

- RADIUS and TACACS+ shared secret key sizes must be at least 8 characters long, and must include at least one number and one letter.

IPSec Requirements and Cryptographic Algorithms

- The only type of key management that is allowed in FIPS mode is Internet Key Exchange (IKE).
- Although the IOS implementation of IKE allows a number of algorithms, only the following algorithms are allowed in a FIPS 140-2 configuration:
  - ah-sha-hmac
  - esp-des
  - esp-sha-hmac
  - esp-3des
  - esp-aes
- The following algorithms are not FIPS approved and should not be used during FIPS-approved mode:
  - RSA
  - MD-5 for signing
  - MD-5 HMAC

Protocols

- SNMP v3 over a secure IPSec tunnel may be employed for authenticated, secure SNMP gets and sets. Since SNMP v2C uses community strings for authentication, only gets are allowed under SNMP v2C.
- SSL is not an Approved protocol, and shall not be used in FIPS mode.

Remote Access

- Telnet access to the module is only allowed via a secure IPSec tunnel between the remote system and the module. The Crypto officer must configure the module so that any remote connections via telnet are secured through IPSec, using FIPS-approved algorithms. Note that all users must still authenticate after remote access is granted.
- SSH access to the module is only allowed if SSH is configured to use a FIPS-approved algorithm. The Crypto officer must configure the module so that SSH uses only FIPS-approved algorithms. Note that all users must still authenticate after remote access is granted.

Related Documentation

For more information about the Cisco 3825 and Cisco 3845 Integrated Services Router, refer to the following documents:

- *Cisco 3800 Series Integrated Services Routers Quick Start Guides*
- *Cisco 3800 Series Hardware Installation* documents
- *Cisco 3800 Series Software Configuration* documents
- *Cisco 3800 Series Cards and Modules*

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/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

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

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco 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

  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.

- 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 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 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.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation 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 Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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/techsupport

Access to all tools on the Cisco Technical Support & Documentation 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 & Documentation 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 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)—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, 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

- *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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *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

- Networking products offered by Cisco Systems, 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 for networking professionals to 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

- 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 Cisco Systems.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.