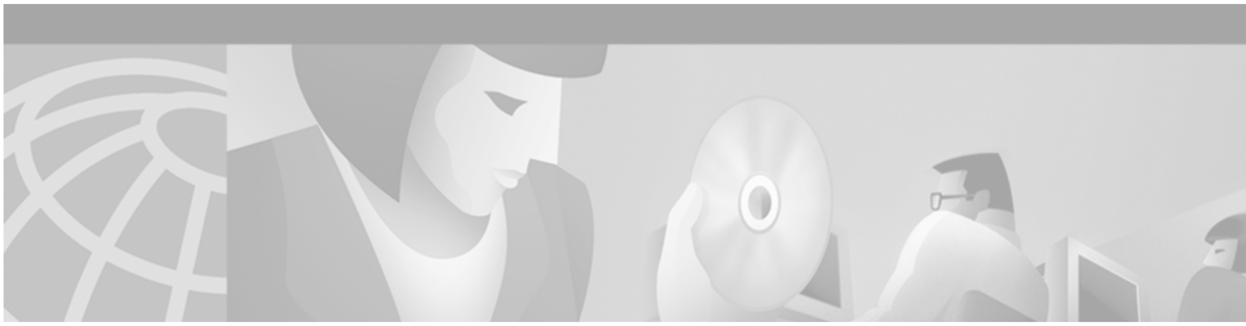


Cisco 2621 Modular Access Router Security Policy

Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Cisco 2621 router. This security policy describes how the 2621 router meets the security requirements of FIPS 140-1, and how to operate the 2621 router in a secure FIPS 140-1 mode. This policy was prepared as part of the Level 2 FIPS 140-1 certification of the 2621 router.

Note This document may be copied in its entirety and without modification. All copies must include the copyright notice and statements on the last page.

FIPS 140-1 (Federal Information Processing Standards Publication 140-1 - Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-1 standard and validation program is available on the NIST website at the following NIST website:

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

This document contains the following sections:

CISCO SYSTEMS

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 2621 router in the technical terms of a FIPS 140-1 cryptographic module security policy. More information is available on the 2621 router and the entire 2600 Series from the following sources:

- The Cisco Systems website contains information on the full line of Cisco Systems products. Refer to the following website:

  www.cisco.com.

- The 2600 Series product descriptions can be found at the following website:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/2600hig/2600ovr.htm

- For answers to technical or sales related questions, please refer to the contacts listed on the following website:

  www.cisco.com.

Terminology

In this document, the Cisco 2621 router is referred to as the router, the module, or the system.

Document Organization

The Security Policy document is part of the complete FIPS 140-1 Submission Package. In addition to this document, the complete Submission Package contains:

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

This document provides an overview of the 2621 router and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the 2621 router. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

This Security Policy and other Certification Submission Documentation was produced by Corsec Security, Inc. under contract to Cisco Systems. With the exception of this Non-Proprietary Security Policy, the FIPS 140-1 Certification Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

Cisco 2621 Modular Access Routers

Branch office networking requirements are dramatically evolving, driven by web and e-commerce applications to enhance productivity and converging the voice and data infrastructure to reduce costs. The Cisco 2621 modular multi-service router offers versatility, integration, and security to branch offices. With over 70 network modules and interfaces, the modular architecture of the Cisco router easily allows interfaces to be upgraded to accommodate network expansion. The Cisco 2621 provides a scalable, secure, manageable remote access server that meets FIPS 140-1 Level 2 requirements. This section describes the general features and functionality provided by the Cisco 2621 router. Section 3 provides further details on how the router addresses FIPS 140-1 requirements.

The 2621 Cryptographic Module

The metal casing that fully encloses the module establishes the cryptographic boundary for the router, all the functionality discussed in this document is provided by components within the casing. Cisco IOS features such as tunneling, data encryption, and termination of Remote Access WANs via IPSec, Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocols (L2TP) make the Cisco 2600 an ideal platform for building virtual private networks or outsourced dial solutions. Cisco 2600`s RISC-based processor provides the power needed for the dynamic requirements of the remote branch office, achieving wire speed Ethernet to Ethernet routing with up to 25 thousand packets per second (Kpps) throughput capacity.

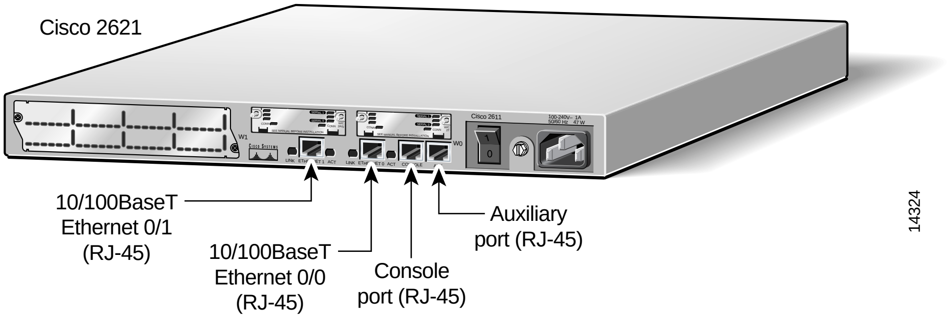
Figure 1 shows a Cisco 2621 modular access router.

Figure 1 Cisco 2621 Router

Module Interfaces

The interfaces for the router are located on the rear panel as shown in Figure 2.

Figure 2 Physical Interfaces



The Cisco 2600 series features single or dual fixed LAN interfaces, a network module slot, two Cisco WAN interface card (WIC) slots, and a new Advanced Integration Module (AIM) slot. LAN support includes single and dual Ethernet options; 10/100 Mbps auto-sensing Ethernet; mixed Token-Ring and Ethernet; and single Token Ring chassis versions. WAN interface cards support a variety of serial, ISDN

BRI, and integrated CSU/DSU options for primary and backup WAN connectivity, while available network modules support multi-service voice/data/fax integration, departmental dial concentration, and high-density serial options. The AIM slot supports integration of advanced services such as hardware-assisted data compression and encryption. All Cisco 2600 series routers include an auxiliary port supporting 115Kbps Dial On Demand Routing, ideal for back-up WAN connectivity.

The physical interfaces include power plug for the power supply and a power switch. The router has two Fast Ethernet (10/100 RJ-45) connectors for data transfers in and out. The module also has two other RJ-45 connectors on the back panel for a console terminal for local system access and an auxiliary port for remote system access or dial backup using a modem. The 10/100Base-T LAN ports have Link/Activity, 10/100Mbps, and half/full duplex LEDs.

Figure 3 shows the LEDs located on the rear panel with descriptions detailed in Table 1:

Figure 3 Rear Panel LEDs

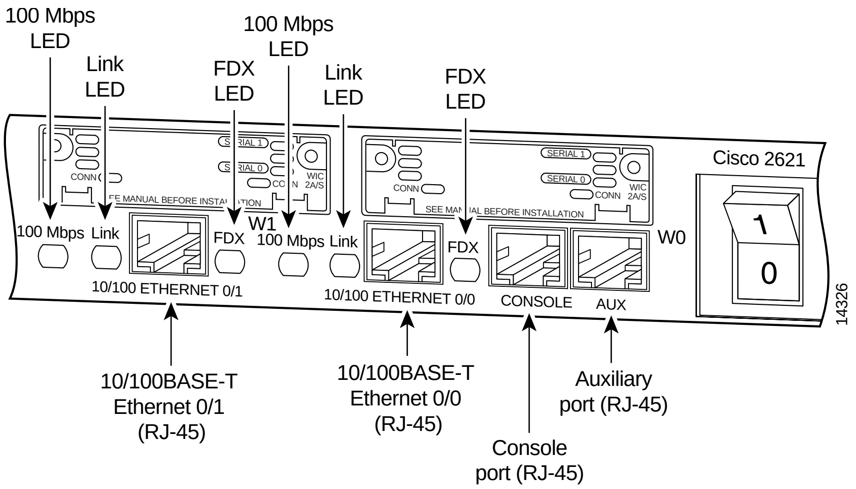
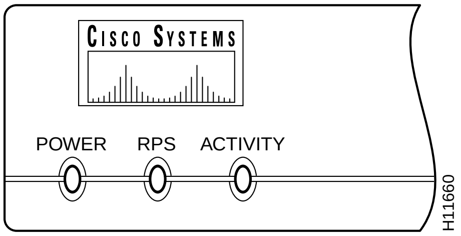


Table 1 Rear Panel LEDs and Descriptions

LED	Indication	Description
LINK	Green	An Ethernet link has been established
	Off	No Ethernet link established
FDX	Green	The interface is transmitting data in full-duplex mode
	Off	When off, the interface is transmitting data in half-duplex mode
100 Mbps	Green	The speed of the interface is 100 Mbps
	Off	The speed of the interface is 10 Mbps or no link is established

Figure 4 shows the front panel LEDs, which provide overall status of the router's operation. The front panel displays whether or not the router is booted, if the redundant power is (successfully) attached and operational, and overall activity/link status.

Figure 4 Front Panel LEDs



The following table provides more detailed information conveyed by the LEDs on the front panel of the router:

Table 2 Front Panel LEDs and Descriptions

LED	Indication	Description
Power	Green	Power is supplied to the router and the router is operational
	Off	The router is not powered on
Redundant Power System (RPS)	Green	RPS is attached and operational
	Off	No RPS is attached
	Blink	RPS is attached, but has a failure
Activity	Off	In the Cisco IOS software, but no network activity
	Blink (500 ms ON, 500 ms OFF)	In ROMMON, no errors
	Blink (500 ms ON, 500 ms OFF, 2 sec between codes)	In ROMMON, error detected
	Blink (less than 500 ms)	In the Cisco IOS software, the blink rate reflects the level of activity

All of these physical interfaces are separated into the logical interfaces from FIPS as described in the following table:

Table 3 FIPS 140-1 Logical Interfaces

Router Physical Interface	FIPS 140-1 Logical Interface
10/100BASE-TX LAN Port WAN Interface Network Module Interface Console Port Auxiliary Port*	Data Input Interface
10/100BASE-TX LAN Port WAN Interface Network Module Interface Console Port Auxiliary Port*	Data Output Interface
Power Switch Console Port Auxiliary Port*	Control Input Interface
LAN Port LEDs 10/100BASE-TX LAN Port LEDs Power LED Redundant Power LED Activity LED Console Port Auxiliary Port*	Status Output Interface
Power Plug	Power Interface

*The auxiliary port must be disabled in FIPS mode. See Section 3.

In addition to the built-in interfaces, the router also has approximately 70 network modules that can optionally be placed in an available slot. These networks modules have many embodiments, including multiple Ethernet, token ring, and modem cards to handle frame relay, ATM, and ISDN connections.

Roles and Services

There are two main roles in the router (as required by FIPS 140-1) that operators may assume: Crypto Officer role and 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.

Crypto Officer Services

During initial configuration of the router a Crypto Officer or Administrator password is defined and all management services are available from this role. The Administrator connects to the router through the console port via terminal program. An administrator of the router may assign permission to access the Administrator role to additional accounts, thereby creating additional administrators.

At the highest level, Crypto Officer services include 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, load authentication information, etc.
- 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.
- Status Functions: view the router configuration, routing tables, active sessions, use Gets to view SNMP MIB II 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 router, manually back up router configurations, view complete configurations, manager user rights, restore router configurations, etc.
- 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.
- Change Network Modules: insert and remove modules in the network module slot as described in Section 3.1, Number 2 of this document.
- Change WAN Interface Cards: insert and remove modules in the network module slot as described in Section 3.1, Number 3 of this document.

A complete description of all the management and configuration capabilities of the Cisco 2621 router can be found in the Performing Basic System Management manual and in the online help for the router.

User Services

A User enters the system by accessing the console port with a terminal program. The IOS prompts the User for their password. If it matches the plaintext password stored in IOS memory, the User is allowed entry to the IOS executive program. The services available to the User role include:

At the highest level, User services include the following:

- Status Functions: view state of interfaces, state of layer 2 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

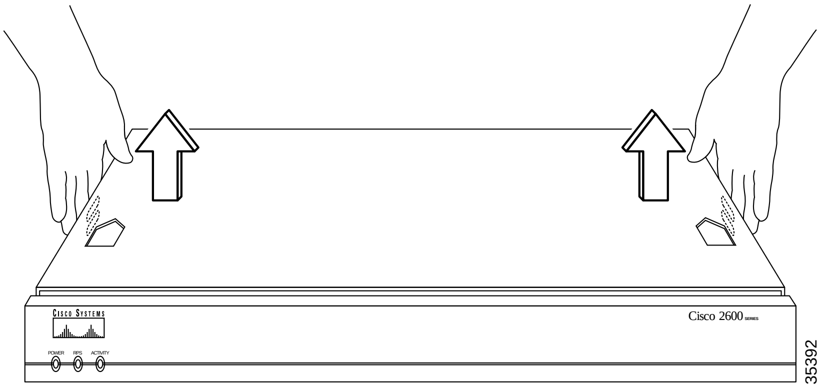
Physical Security

The router is entirely encased by a thick steel chassis. The rear of the unit provides 1 Network Module slot, 2 WIC slots, on-board LAN connectors, Console/Auxiliary connectors, the power cable connection and a power switch. The top portion of the chassis may be removed (see Figure 5) to allow access to the motherboard, memory, expansion slots and Advanced Interface Module.

Warning **Two people are required to lift the chassis. Grasp the chassis underneath the lower edge and lift with both hands. To prevent injury, keep your back straight and lift with your legs, not your back. To prevent damage to the chassis and components, never attempt to lift the chassis with the**

handles on the power supplies or on the interface processors, or by the plastic panels on the front of the chassis. These handles were not designed to support the weight of the chassis. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.

Figure 5 Chassis Removal



Once the router has been configured in to meet FIPS 140-1 Level 2 requirements, the router cannot be accessed without signs of tampering. To seal the system, apply serialized tamper-evidence labels as follows:

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 ambient air must be above 10ºC, otherwise the labels may not properly cure..

Step 2 Place the first label on the router as shown in Figure 6. The tamper evidence label should be placed so that the one half of the tamper evidence label covers the enclosure and the other half covers the side of the router. Any attempt to remove the enclosure will leave tamper evidence.

Step 3 Place the second label on the router as shown in Figure 6. The tamper evidence label should be placed so that the one half of the tamper evidence label covers the enclosure and the other half covers the side of the router. Any attempt to remove the enclosure will leave tamper evidence.

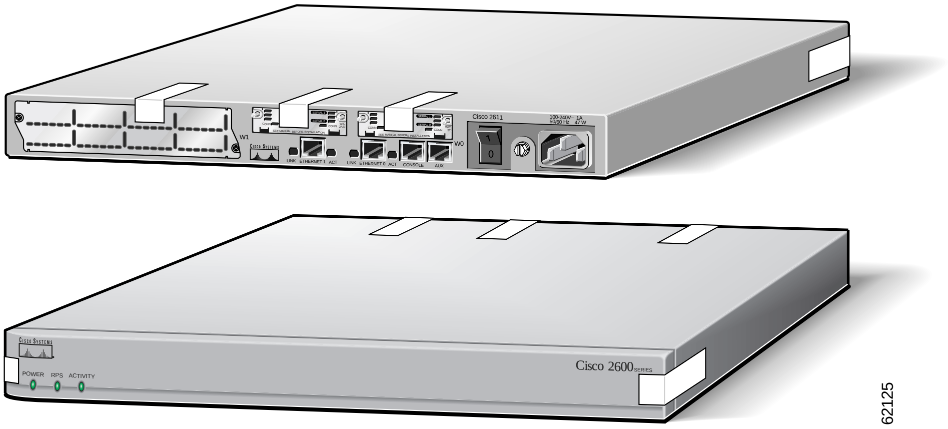
Step 4 Place the third label on the router as shown in Figure 6. The tamper evidence label should be placed so that the one half of the label covers the enclosure and the other half covers the Network Module slot. Any attempt to remove a network module will leave tamper evidence.

Step 5 Place the fourth label on the router as shown in Figure 6. The tamper evidence label should be placed so that the half of the label covers the enclosure and the other half covers the WAN interface card slot. Any attempt to remove a WAN interface card will leave tamper evidence.

Step 6 Place the fifth label on the router as shown in Figure 6. The tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the WAN interface card slot. Any attempt to remove a WAN interface card will leave tamper evidence.

Step 7 The labels completely cure within five minutes.

Figure 6 Tamper-Evident Labels



The tamper evidence seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the router, remove network modules or WIC cards, or the front faceplate will damage the tamper evidence seals or the painted surface and metal of the module cover. Since the tamper evidence labels have non-repeated serial numbers, the labels may be inspected for damage and compared against the applied serial numbers to verify that the module has not been tampered. Tamper evidence labels can also be inspected for signs of tampering, which include the following: curled corners, bubbling, crinkling, rips, tears, and slices. The word "Opened" 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. Keys are also password protected and can be zeroized by the Crypto Officer. Keys are exchanged manually and entered electronically via manual key exchange or Internet Key Exchange (IKE). The 2621 router supports the following FIPS-approved algorithms: DES. 3DES, and SHA-1. These algorithms received certification numbers 74, 17, and 26 respectively.

Self-Tests

In order to prevent any secure data 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. The self-test run at power-up includes a cryptographic known answer tests (KAT) on the FIPS-approved cryptographic algorithms (DES, 3DES), on the message digest (SHA-1) and on Diffie-Hellman algorithm. Also performed at startup are software integrity test using an EDC, and a set of Statistical Random Number Generator (RNG) tests. The following tests are also run periodically or conditionally: a Bypass Mode test performed conditionally prior to executing IPSec, a software load test for upgrades and the continuous random number generator test. If any of these self-tests fail, the router will transition into an error state. Within the error state, all secure data transmission is halted and the router outputs status information indicating the failure.

Secure Operation of the Cisco 2621 Router

The Cisco 2621 router meets all the Level 2 requirements for FIPS 140-1. Follow the setting instructions provided below to place the module in FIPS mode. Operating this router without maintaining the following settings will remove the module from the FIPS approved mode of operation.

Initial Setup

Step 1 The Crypto Officer must apply tamper evidence labels as described inthe "Physical Security" section on page 7 of this document. The Crypto Officer must securely store tamper evidence labels before use, and any tamper evidence labels not used should also be stored securely.

Step 2 Only a Crypto Officer may add and remove network modules. When removing the tamper evidence label, the Crypto Officer should remove the entire label from the router and clean the cover of any grease, dirt, or oil with an alcohol-based cleaning pad. The Crypto Officer must re-apply tamper evidence labels on the router as described in the "Physical Security" section on page 7

Step 3 Only a Crypto Officer may add and remove WAN Interface Cards. When removing the tamper evidence label, the Crypto Officer should remove the entire label from the router and clean the cover of any grease, dirt, or oil with an alcohol-based cleaning pad. The Crypto Officer must re-apply tamper evidence labels on the router as described in the "Physical Security" section on page 7.

System Initialization and Configuration

Step 1 The Crypto Officer must perform the initial configuration. The IOS version shipped with the router, version 12.1(5)T, is the only allowable image. No other image may be loaded.

Step 2 The value of the boot field must be 0x0101 (the factory default). This setting disables break from the console to the ROM monitor and automatically and boots the IOS image. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

```
config-register 0x0101
```

Step 3 The Crypto Officer must create the "enable" password for the Crypto Officer role. The password must be at least 8 characters 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]
```

Step 4 The Crypto Officer must always assign passwords (of at least 8 characters) to users. Identification and authentication of 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
```

Step 5 The Crypto Officer shall only assign users to a privilege level 1 (the default).

Step 6 The Crypto Officer shall not assign a command to any privilege level other than its default.

Non-FIPS Approved Algorithms

The following algorithms are not FIPS approved and should be disabled:

- RSA for encryption
- MD-4 and MD-5 for signing
- ah-sha-hmac
- esp-sha-hmac
- HMAC SHA-1

Protocols

The following network services affect the security data items and must not be configured: NTP, TACACS+, RADIUS, Kerberos.

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.

Remote Access

Auxiliary terminal services must be disabled, except for the console. The following configuration disables login services on the auxiliary console line.

```
line aux 0
no exec
```

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.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

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

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

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

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.