Using the Cisco Media Convergence Server Network Teaming Driver

Supports Operating System Versions 2000.4.3 and 2000.4.3a

Note Unless otherwise indicated in this document, all references to 2000.4.3 mean 2000.4.3 and 2000.4.3a.

The Cisco Media Convergence Server (MCS) Network Teaming Driver enables the functionality for the failover fault-tolerant network adapters. This driver works with Cisco Media Convergence Servers that have dual network interface cards (NICs) installed. With this functionality, the standby NIC can handle all IP traffic if the primary NIC fails.

Operating system version 2000.4.3 automatically installs the Network Teaming Driver as part of the installation process. You must perform configuration tasks, as described in this document, to set up and use the Network Teaming Driver.

Use this document with operating system version 2000.4.3 (or later). For information about installing and configuring the Network Teaming Driver with earlier versions of the operating system, refer to previous versions of this document, which are available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/install/index.htm

Contents

This document contains the following topics:

CISCO SYSTEMS

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

Related Cisco Unified CallManager and Operating System Documentation

Table 1 provides a list of Cisco Unified CallManager and operating system documentation. You can navigate to the appropriate documentation by clicking the URLs that are shown in the table.

Table 1   Quick Reference for Documentation and Software URLs

Related Documentation and Software	URL and Additional Information
Operating system documentation and Virtual Network Computing (VNC) documentation (not readme documentation)	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm
Cisco MCS data sheets	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html
Software-only servers (IBM, HP, Compaq, Aquarius)	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html
Cisco Unified CallManager Compatibility Matrix	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
Cisco Unified CallManager documentation, including installation and upgrade documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
Backup and Restore documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm
Support patches and readme documentation	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml **Note** The operating system and SQL Server 2000 support patches post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco Unified CallManager software page.

Server Requirements

The following servers support the HP Network Teaming Driver:

- Cisco MCS-7825H-2266
- Cisco MCS-7825H-3000
- Cisco MCS-7825H1
- Cisco MCS-7825-H2
- Cisco MCS-7835H-1266

- Cisco MCS-7835H-2400
- Cisco MCS-7835H-3000
- Cisco MCS-7835H1
- Cisco MCS-7845H-1400
- Cisco MCS-7845H-2400
- Cisco MCS-7845H-3000
- Cisco MCS-7845-H1
- Cisco-approved, customer-provided HP DL380 G2 server
- Cisco-approved, customer-provided HP DL380 G3 server, including single and dual processors
- Cisco-approved, customer-provided HP DL320 G2 server
- Cisco-approved, customer-provided HP DL320 G3 server
- Cisco-approved, customer-provided HP DL320 G4 server
- Cisco-approved, customer-provided HP DL380 G4 server, including single and dual processors

Before You Begin

Before you configure the Network Teaming Driver, review the following information:

- Cisco requires that your system runs Cisco-provided operating system version 2000.4.3 (or later).
- You must reboot the server after you perform the driver configuration tasks.
- If you want to uninstall the network teaming driver, you must reboot the server for the changes to take effect.
- Perform all configuration tasks on every server in the cluster where the driver is supported.
- You must enable network teaming from the console. You cannot perform this procedure remotely through Terminal Services or Virtual Network Computing (VNC).

Note Before you install or upgrade Cisco Unified CallManager, Cisco strongly recommends that you configure the Network Teaming Driver.

If you do not perform the tasks in the recommended order and decide to configure the driver after the application upgrade, you might encounter a Service Control Manager message, as described in the "Troubleshooting the Network Teaming Driver" section on page 11.

Before you configure the driver, perform the following procedure:

Procedure

Step 1 After you install Cisco-provided operating system 2000.4.3 on every server in the cluster, right-click **My Network Places**.

Step 2 Right-click **Local Area Connection**; choose **Properties**.

Step 3 Choose the **Internet Protocol (TCP/IP)** component and click the **Properties** button.

Step 4 In Table 2 on page 4, enter the IP information, including the IP address, subnet mask, the default gateway, and the DNS/WINS settings.

⌕

Tip To obtain the WINS setting, click the **Advanced** button for WINS settings.

Table 2   Internet Protocol Information for the Primary Network Card

Information	Your Entry
IP address	
Subnet mask	
Default gateway	
DNS settings	
• Primary	
• Secondary	
WINS settings	
• Primary	
• Secondary	
Link speed setting	
Duplex setting	

Step 5 After you record the information, click **Cancel**.

Step 6 In the Local Area Connection window, click the **Configure** button.

Step 7 Click the **Advanced** tab.

Step 8 In the Property pane, locate the speed and duplex settings.

One or two different settings may exist, depending on the server type.

Step 9 In Table 2, enter the speed and duplex setting values for the primary network card.

Step 10 Right-click the second network card connection, **Local Area Connection 2**.

Step 11 Choose **Enable**.

✎

Note The installation of Cisco-provided operating system version 2000.4.3 (or later) automatically disables the second network card. You must enable it now.

In addition, make sure that the second network card is connected to the network. When only one network card is connected, the network team does not get created correctly. If the network team is not created correctly, verify the connection of the second network card and rerun the Network Teaming Driver configuration procedures.

Configuration Tasks

This section includes information on the following topics:

Configuring the HP Network Teaming Driver

To configure the Network Teaming Driver, perform the following procedure:

Procedure

Step 1 Locate the HP Network Configuration Utility icon in the Windows 2000 system tray or by choosing **Start > Settings > Control Panel > HP Network**.

Figure 1 shows this icon.

Figure 1   *HP Network Configuration Utility Icon*

Step 2 Double-click the icon to launch the HP Network Configuration Utility.

The HP Network Configuration Utility Properties window displays, as shown in Figure 2.

Figure 2　　　*HP Network Configuration Utility Properties Window*
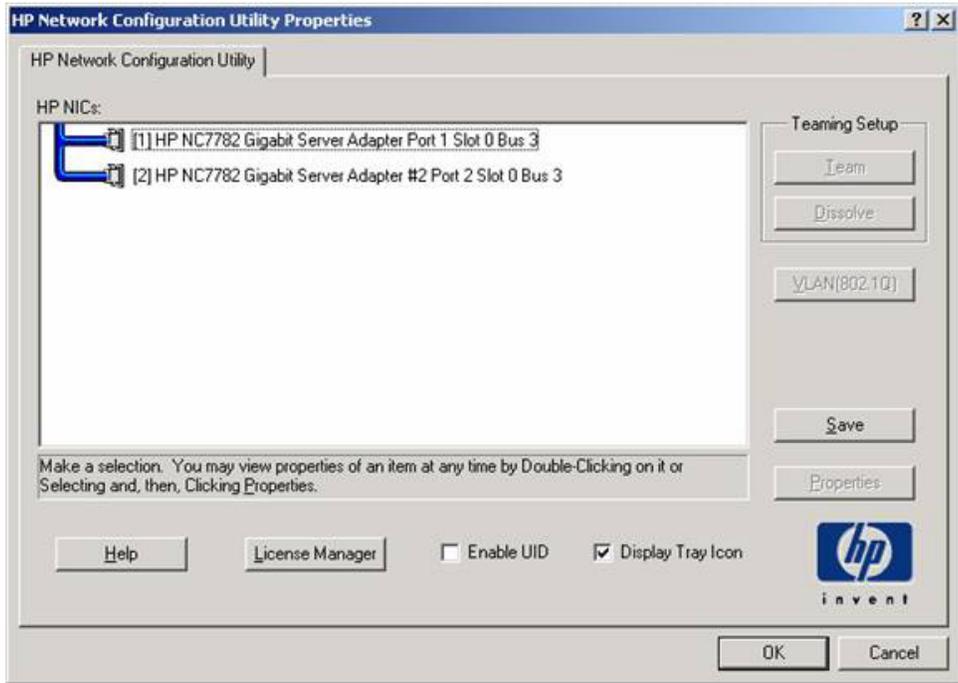
Step 3　Click each HP NIC that is listed to select both entries, as shown in Figure 3.

Figure 3　　　*Selected HP NICs*
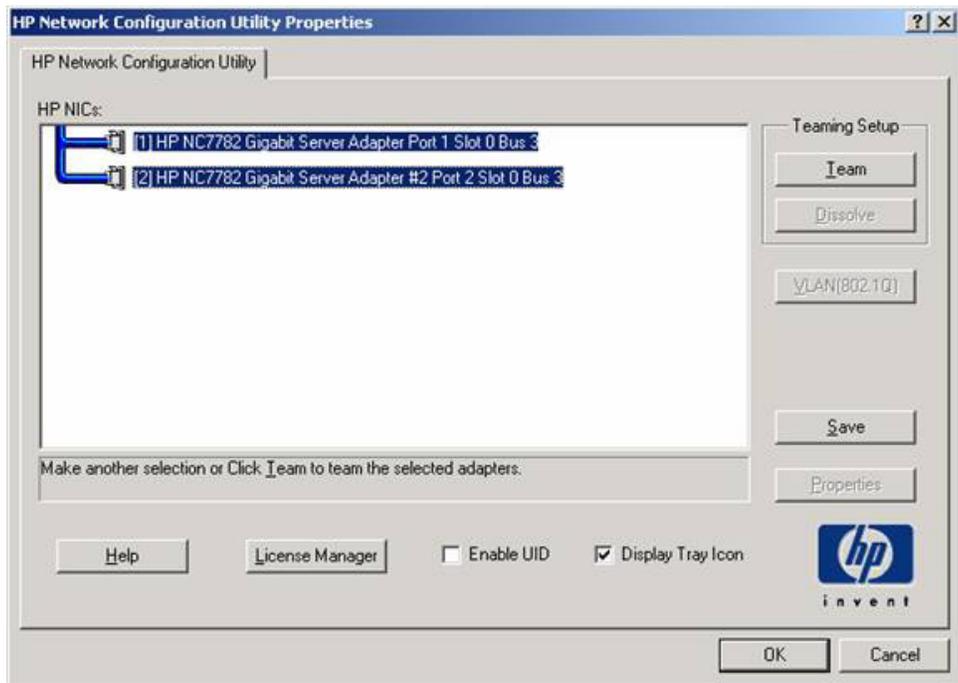
Step 4　In the Teaming Setup area, click **Team** to team the selected HP NICs.

The system creates the NIC team, as shown in Figure 4:

Figure 4   *Team Created*
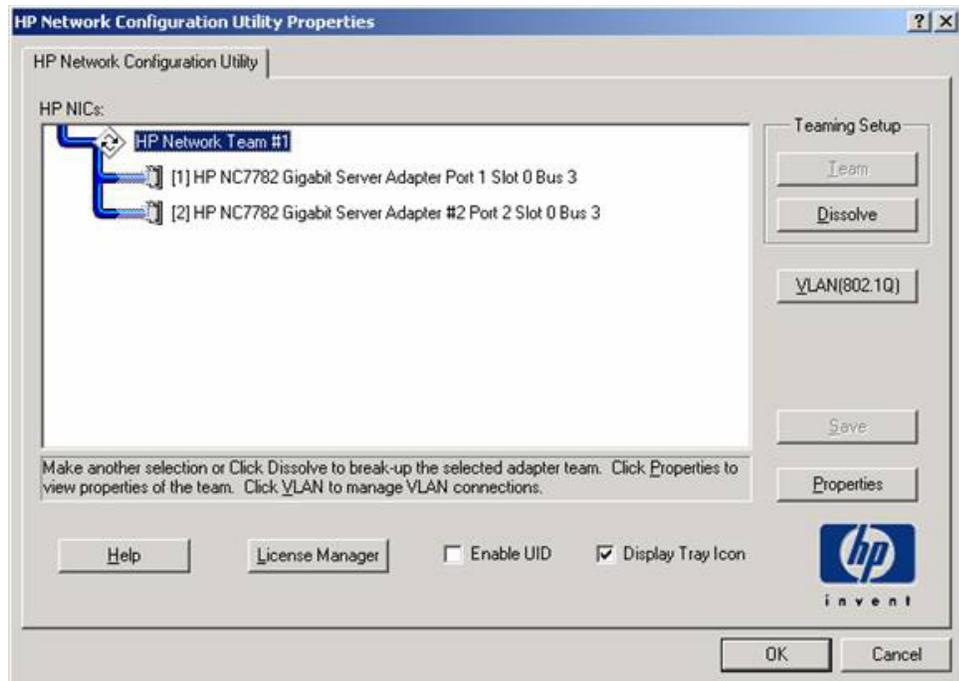
Step 5   Click **Properties**.

The Team Properties window displays, as shown in Figure 5. In this figure, HP Network Team #1 represents the default name for the team.

Figure 5   Team Properties Window
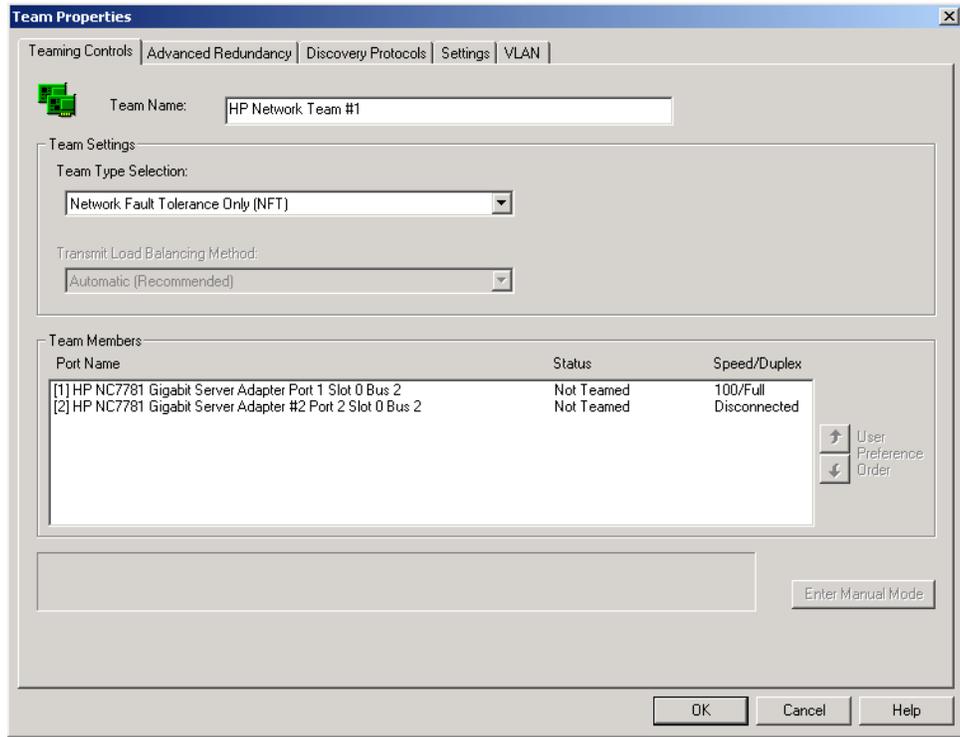
> **Note**   In the Team Properties window, Cisco strongly recommends that you choose the specified setting in Step 6.

Step 6   Under the Team Controls tab in the Team Properties window, choose **Network Fault Tolerance Only (NFT)** from the Team Type Selection drop-down list box.

After you choose this setting, the options in the Transmit Load Balancing Method drop-down list box appear disabled.

Step 7   In the Team Properties window, click **OK**.

You have created the HP Network Team.

Step 8   In the HP Network Configuration Utility Properties window, click **OK**.

A confirmation window displays, as shown in Figure 6.

Figure 6   Confirmation
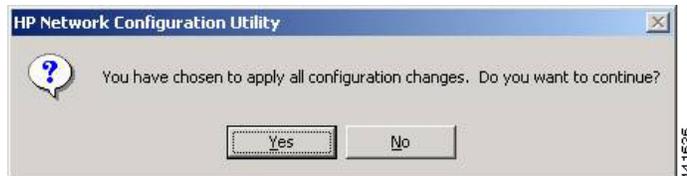
Tip   You can change the team properties, if you want to do so, by clicking **Properties** in the HP Network Configuration Utility Team Properties window. For example, you can use Properties to change the name of the HP Network Team. After you change the properties, click **OK**.

Step 9   To confirm your changes and continue, click **Yes**.

Step 10   Wait while the adapters are being configured; then, click **Yes** when prompted to reboot the server, as shown in Figure 7.

Figure 7   Successful Configuration Changes
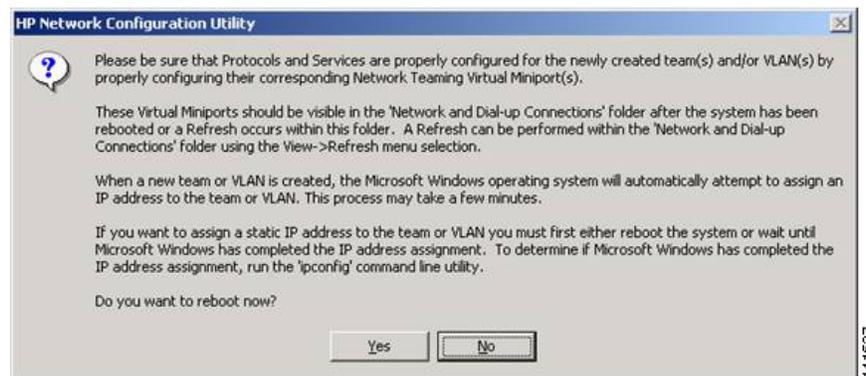
Step 11   Launch the HP Network Configuration Utility, as described in Step 2.

Step 12   To choose the NIC, click **NIC Port #1** (or a variation of that name); then, click **Properties**.

Step 13   Click the **Settings** tab.

Step 14   Choose **Speed/Duplex Setting** and enter the setting that you recorded in Table 2 on page 4.

Step 15   Click **OK**.

Step 16   To deselect the NIC, click **NIC Port #1** (or a variation of that name).

Step 17   Repeat Step 12 through Step 15 for **NIC Port #2** (or a variation of that name).

Step 18   Click **OK**.

Step 19   Right-click **My Network Places**; choose **Properties** for the Local Area Connection.

An additional network card, Local Area Connection 3, displays in the window.

Step 20   Right-click the teamed connection; choose **Properties**.

Step 21   Choose the **Internet Protocol (TCP/IP)** option and click the **Properties** button.

Step 22   From Table 2 on page 4, enter the information, including the IP address, the subnet mask, the default gateway, and the DNS/WINS settings.

Tip   To enter the WINS setting, click the **Advanced** button for WINS settings. After you enter the information, make sure that you click **OK**.

Step 23   After you enter the information, click **OK**.

Step 24   Click **OK**.

Step 25 Close the Network and Dial-up Connections window.

You do not need to reboot the server.

Step 26 Perform all teaming procedures on every server in the cluster where the teaming driver is supported.

Step 27 Perform Cisco Unified CallManager installation tasks. See Table 1 on page 2 for reference to Cisco Unified CallManager documentation.

Dissolving the HP Network Teaming Driver

When you dissolve the driver, you disassociate the two NICs and the virtual NIC that is used for the driver. The teaming drivers remain installed, but they no longer are configured or used.

In this case, the server uses NIC #1 only for IP telephony.

To dissolve the HP Network Teaming Driver, perform the following procedure:

Procedure

Step 1 Double-click the HP Network Configuration Utility icon that displays in the Windows 2000 system tray.

Step 2 Click **HP Network Team #1**.

Step 3 Click **Dissolve**.

Step 4 Click **OK**.

Step 5 To apply changes, click **Yes**.

Step 6 After all configuration changes are successful, click **OK**.

⚠

Caution Failing to disable the second NIC may result in two IP addresses being assigned to the server. Assigning two IP addresses to the Cisco Unified CallManager server may cause a loss of service.

Uninstalling the HP Network Teaming Driver

When you uninstall the HP Network Teaming Driver, you delete the drivers from the server. The server uses only NIC #1 for IP telephony.

To uninstall the HP Network Teaming Driver, perform the following procedure:

Procedure

Step 1 Right-click **My Network Places** and choose **Properties**.

Step 2 Right-click any active network card connection and click **Properties**.

Step 3 Choose **HP Network Configuration Utility** and click **Uninstall**.

Step 4 To uninstall the driver, click **Yes**.

Step 5 For the changes to take effect, click **Yes** to reboot the server.

Step 6 After the server reboots, disable the second NIC.

> **Note** If you need to reinstall the Network Teaming Driver, you must run HPConfigUtil.exe. To do so, navigate to **C:\Utils\DualNIC\HPConfigUtil.exe** and follow the procedure for configuring the driver (see Step 11 in the "Configuring the HP Network Teaming Driver" section on page 5).

> **Caution** Failing to disable the second NIC may result in two IP addresses being assigned to the server. Assigning two IP addresses to the Cisco Unified CallManager server may cause a loss of service.

Step 7 To verify that you uninstalled the driver, perform the following procedure:

   a. Right-click **My Network Properties** and choose **Properties**.

     A list, which should not include the network team, displays.

   b. Right-click the primary network card connection, which is, by default, Local Area Connection, and choose **Properties**.

   c. Choose **Internet Protocol (TCP/IP)** option and click **Properties**.

   d. Verify that the settings from Step 4 in the "Before you configure the Network Teaming Driver, review the following information:" section on page 3 display.

Troubleshooting the Network Teaming Driver

After you configure the Network Teaming Driver and install Cisco Unified CallManager, you might encounter a Service Control Manager message, such as "At least one service or driver failed during system startup. Use Event Viewer to examine the event log for details." To resolve this problem, perform the following procedure:

Procedure

Step 1 Open the Event Viewer by choosing **Start > Programs > Administrative Tools > Event Viewer**.

Step 2 Select **System Log**.

Step 3 To find an occurrence of the following entry around the time of the error, browse the System Log:

   • Source entry—Service Control Manager

   • Event ID—7000

Step 4 To open the Event Properties window, double-click **Service Control Manager**.

The following description displays:

```
The HP Network Configuration Utility service failed to start due to the following error:
The service cannot be started, either because it is disabled or because it has enabled
devices associated with it.
```

Step 5 Navigate to the **C:\Utils\DualNIC** folder and double-click **Teaming-CDP.cmd**.

The utility runs for a few seconds. The fix takes effect without rebooting the server.

After the next reboot of the server, this message no longer displays.

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

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML 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= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

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

Cisco Systems, Inc.
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 will find information about how to:

- 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 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 at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

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)—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 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 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

- *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