Release Notes for the Cisco 806 Router and Cisco 820 Series Routers for Cisco IOS Release 12.2(8)YM

July 30, 2003

These release notes for the Cisco 806 routers and Cisco 820 Series routers describe the enhancements provided in Cisco IOS Release 12.2(8)YM1. These release notes are updated as needed. Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.2 T* located on Cisco.com and the Documentation CD.

For a list of the software caveats that apply to Cisco IOS Release 12.2(8)YM1, see the "Caveats" section on page 9 and *Caveats for Cisco IOS Release 12.2 T.* The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD.

Contents

These release notes discuss the following topics:

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

System Requirements

This section describes the system requirements for Release 12.2(8)YM1 and includes the following sections:

Memory Requirements

Table 1 provides the memory requirements for the Cisco IOS feature sets supported by Cisco IOS Release 12.2(8)YM1 on the Cisco 800 Series Routers. All images are run from RAM.

Table 1 Recommended Memory for the Cisco 800 Series Routers

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM Memory
Cisco 806 Routers	Cisco 806 Series IOS IP Plus FW IPSec 3DES	IP Plus FW IPSec 3DES	c806-k9o3sy6-mz	8 MB	32 MB
	Cisco 806 Series IOS IP Plus FW	IP Plus FW	c806-o3sy6-mz	8 MB	32 MB
	Cisco 806 Series IOS IP Plus	IP Plus	c806-sy6-mz	8 MB	20 MB
Cisco 826, Cisco 827, and Cisco 827H routers	Cisco 820 Series IOS IP Plus FW IPSec 3DES	IP Plus FW IPSec 3DES	c820-k9osy6-mz	8 MB	24 MB
	Cisco 820 Series IOS IP/FW	IP/FW	c820-oy6-mz	8 MB	20 MB
	Cisco 820 Series IOS IP Plus	IP Plus	c820-sy6-mz	8 MB	24 MB
	Cisco 820 Series IOS IP	IP	c820-y6-mz	8 MB	20 MB
Cisco 827-4V Routers	Cisco 820 Series IOS IP Plus FW/Voice IPSec 3DES	IP Plus FW/Voice IPSec 3DES	c820-k9osv6y6-mz	8 MB	32 MB
	Cisco 820 Series IOS IP/FW/Voice	IP/FW/Voice	c820-ov6y6-mz	8 MB	32 MB
	Cisco 820 Series IOS IP Plus Voice	IP Plus Voice	c820-sv6y6-mz	8 MB	32 MB
	Cisco 820 Series IOS IP/Voice	IP/Voice	c820-v6y6-mz	8 MB	32 MB
Cisco 828	IP	IP	c828-y6-mz	8 MB	20 MB
	IP/FW	IP/FW	c828-oy6-mz	8 MB	20 MB
	IP Plus	IP Plus	c828-sy6-mz	8 MB	20 MB
	IP/FW Plus 3DES	IP/FW Plus	c828-k9osy6-mz	8 MB	24 MB

Hardware Supported

Cisco IOS Release 12.2(8)YM1 supports the following Cisco routers:

- Cisco 806 Routers
- Cisco 820 series routers:
  - Cisco 826 Routers
  - Cisco 827 Routers
  - Cisco 827H Routers
  - Cisco 827-4V Routers
- Cisco 828 Routers

For detailed descriptions of new hardware features and which features are supported on each router, see the "New and Changed Information" section on page 6. For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to SOHO 70 Series Routers and Cisco 800 Series Routers, which are available on Cisco.com and the Documentation CD at the following location:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/index.htm

This URL is subject to change without notice. If it changes, point your web browser to CCO, and click the following path:
Cisco Product Documentation: **Access Servers and Access Routers**: **Fixed Configuration Access Routers**: **<platform_name>**

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco router, log in to the router and enter the **show version** EXEC command. The following sample displays command output from a Cisco 806 router running Release 12.2(8)YM1:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) C806 Software (C806-SY6-MZ), Version 12.2(8)YM1, EARLY DEPLOYMENT RELEASE SOFTWARE
(fc1)
Synched to technology version 12.2(11.2u)T
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see Software Installation and Upgrade Procedures located at: http://www.cisco.com/warp/public/130/upgrade_index.shtml.

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features. Release 12.2(8)YM1 supports the same feature sets as Releases 12.2(8)T, but Release 12.2(8)YM1 can include new features supported by the Cisco 800 Series Routers.

Table 2 through Table 5 list the features and feature sets supported in Cisco IOS Release 12.2(8)YM1:

- Table 2—Cisco 806 routers
- Table 3—Cisco 826, Cisco 827, and Cisco 827-4V Routers
- Table 4—Cisco 827-4V Routers
- Table 5—Cisco 828 Routers

The tables use the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the "In" column indicates the Cisco IOS release in which the feature was introduced. For example, "12.2(8)YM" means the feature was introduced in 12.2(8)YM. If a cell in this column is empty, the feature was included in a previous release or the initial base release.

Note These feature set tables only contain a selected list of features. These tables are not cumulative—nor do they list all the features in each image.

Table 2 Feature List by Feature Set for the Cisco 806 routers

		Feature Sets		
Features	**In**	**IP Plus FW IPSec 3DES**	**IP Plus FW**	**IP Plus**
IP Routing				
HSRP	12.2(8)YM	Yes	Yes	Yes
IP Addressing and Services				
DNS Proxy	12.2(8)YM	Yes	Yes	Yes
Skinny Passthrough NAT	12.2(8)YM	Yes	Yes	Yes
NAT Support for SIP	12.2(8)YM	Yes	Yes	Yes
Security				
Easy VPN Client Phase II		Yes	No	No
Quality of Service				
LLQ		Yes	Yes	Yes

Table 3 Feature List by Feature Set for the Cisco 826, Cisco 827 and Cisco 827H Routers

		Feature Sets			
Features	**In**	**IP Plus FW IPSec 3DES**	**IP/FW**	**IP Plus**	**IP**
Routing					
HSRP	12.2(8)YM	Yes	No	Yes	No
IP Addressing and Services					
DNS Proxy	12.2(8)YM	Yes	Yes	Yes	Yes
Skinny Passthrough NAT	12.2(8)YM	Yes	Yes	Yes	Yes
NAT Support for SIP	12.2(8)YM	Yes	Yes	Yes	Yes

Table 3 Feature List by Feature Set for the Cisco 826, Cisco 827 and Cisco 827H Routers

		Feature Sets			
Features	**In**	**IP Plus FW IPSec 3DES**	**IP/FW**	**IP Plus**	**IP**
Security					
Easy VPN Client Phase II		Yes	No	No	No
Quality of Service					
LLQ		Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 827-4V Router

		Feature Sets			
Features	**In**	**IP FW/Voice Plus 3DES**	**IP/FW/ Voice**	**IP Plus Voice**	**IP Voice**
IP Routing					
HSRP	12.2(8)YM	Yes	No	Yes	No
IP Addressing and Services					
DNS Proxy	12.2(8)YM	Yes	Yes	Yes	Yes
Skinny Passthrough NAT	12.2(8)YM	Yes	Yes	Yes	Yes
NAT Support for SIP	12.2(8)YM	Yes	Yes	Yes	Yes
Security					
Easy VPN Client Phase II		Yes	No	No	No
Quality of Service					
LLQ		Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 828 Router

		Feature Sets			
Features	**In**	**IP Plus FW IPSec 3DES**	**IP/FW**	**IP Plus**	**IP**
IP Routing					
HSRP	12.2(8)YM	Yes	No	Yes	No
IP Addressing and Services					
DNS Proxy	12.2(8)YM	Yes	Yes	Yes	Yes
Skinny Passthrough NAT	12.2(8)YM	Yes	Yes	Yes	Yes
NAT Support for SIP	12.2(8)YM	Yes	Yes	Yes	Yes
QoS					
LLQ	12.2(8)YM	Yes	Yes	Yes	Yes
Security					
Easy VPN Remote Phase II	12.2(8)YM	Yes	No	No	No

Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

New and Changed Information

The following sections list the new hardware and software features supported by Release 12.2(8)YM for the SOHO 70 Series Routers and the Cisco 800 Series Routers.

New Software Features in Release 12.2(8)YM

The following sections list the new software features supported by Cisco IOS Release 12.2(8)YM1 on the and the Cisco 800 Series Routers.

Hot Standby Router Protocol

Hot Standby Router protocol (HSRP) enables a set of routers to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN. HSRP is particularly useful in environments where critical applications are running and fault-tolerant networks have been designed. By sharing an IP address and a MAC address two or more routers acting as one virtual router are able to seamlessly assume the routing responsibility in the case of a defined event or the unexpected failure. This enables hosts on a LAN to continue to forward IP packets to a consistent IP and MAC address enabling the changeover of devices doing the routing to be transparent to them and their sessions.

Refer to Software Enhancements for the Cisco 800 Routers and SOHO Routers for more information on this feature.

Domain Name System Proxy

Domain Name System (DNS) proxy enables the router to act as a Proxy DNS server. This means that it will receive DNS queries on behalf of the real DNS servers and proxy for hosts connected to the LAN. This enables the DHCP server to immediately send hosts on the LAN the router's own LAN address as the DNS server IP address. The router then forwards the DNS queries from local users to real DNS servers after the WAN connection is initiated, and it caches the DNS records in the answers.

Refer to Software Enhancements for the Cisco 800 Routers and SOHO Routers for more information on this feature.

Skinny NAT–Support of IP Phone to Cisco Call Manager

Cisco IP phones use the Selsius Skinny Station Protocol to connect with and register to the Cisco CallManager (CCM). Messages flow back and forth that include IP address and port information used to identify other IP phone users with which a call can be placed. To be able to deploy Cisco IOS Network Address Translation between the IP phone and CCM in a scalable environment, NAT needs to be able to detect the Selsius Skinny Station Protocol and understand the information passed within the messages.

When an IP phone attempts to connect to the CCM and it matches the configured NAT translation rules, NAT will translate the original source IP address and replace it with one from the configured pool. This new address will be reflected in the CCM and be visible to other IP phone users.

Skinny +NAT allows NAT to "dynamically" perform IP address translation, eliminating the need to manually configure an IP address within NAT for each IP phone. It enables service providers and enterprise customers to deploy IP phones to remote offices and to maintain centralized CCMs back at the head office or a major regional center, while making use of NAT for address translation between the IP phone and CCM.

Refer to Software Enhancements for the Cisco 800 Routers and SOHO Routers for more information on this feature.

NATSupport for SIP

Release 12.2(8)YM1 supports the ability to deploy Network Address Translation (NAT) between VoIP solutions that are based on the Session Initiation protocol (SIP). The SIP is an application-layer signaling protocol for creating and controlling multimedia sessions with two or more participants and a client-server protocol transported over TCP or UDP. An Application Layer Gateway (ALG) with NAT enables the SIP. The messages in the protocol might have IP addresses embedded in the packet payload. If a message passes through a router configured with NAT, the embedded information must be translated and encoded back to the packet.

Refer to Software Enhancements for the Cisco 800 Routers and SOHO Routers for more information on this feature.

Low Latency Queuing

Low Latency Queueing (LLQ) provides a low-latency, strict-priority transmit queue for voice over IP (VoIP) traffic. Strict priority queueing allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic. Refer to Software Enhancements for the Cisco 800 Routers and SOHO Routers for more information on this feature.

Easy VPN Remote Phase II

Applications for routers (and other forms of broadband access devices) that provide high-performance connections to the Internet often require the security of virtual private network (VPN) connections with a high level of access authentication and the capability to encrypt data between two endpoints. However, establishing a VPN connection between two routers can be complex, and typically requires detailed coordination between network administrators to configure the router VPN parameters.

The Cisco Easy VPN client feature eliminates much of this work by implementing the Cisco Unity Client protocol, which allows most VPN parameters to be defined at a VPN 3000 concentrator, acting as an IPSec server. After network administrators configure the IPSec server, they can create a VPN connection with minimal configuration on an IPSec client (such as a Cisco 800 series router). Note that Cisco 800 series routers are supported as Easy VPN clients of VPN 3000 IPSec servers. When the IPSec client initiates the VPN tunnel connection, the IPSec server transmits the IPSec policies to the IPSec client and creates the corresponding VPN tunnel connection.

Note The Cisco Easy VPN client can establish communication with a single peer (IPSec server).

The Phase II implementation of the Cisco Easy VPN Client provides enhancements and additional capabilities to Phase I features. In Phase II, the Cisco Easy VPN Client can provide the following enhancements and feature capabilities:

- Manual Control of IPSec VPN tunnels—to establish and terminate the IPSec VPN tunnel on demand.
- Restore NAT Configuration when IPSec VPN Tunnel Is Down—automatically restores the NAT configuration when the IPSec VPN tunnel is disconnected.
- Peer Hostname Enhancement

For instructions on configuring Cisco Easy VPN client, refer to the publication Cisco Easy VPN Client Feature Phase II. This document is available on Cisco Connection Online.

New Software Features in Release 12.2 T

For information regarding the features supported in Cisco IOS Release 12.2 T, refer to the Cross-Platform Release Notes and New Feature Documentation links at the following location on Cisco.com and the Documentation CD-ROM:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/index.htm

This URL is subject to change without notice. If it changes, point your web browser to Cisco.com, and click on the following path:

Service & Support: **Technical Documents**: **Release 12.2** (from the **Cisco IOS Software** drop-down list)

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2(8)YM1 that can apply to Cisco 800 series routers. (Also, see the "Caveats" section on page 9.)

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.

Caveats in Cisco IOS Releases 12.2 and 12.2 T are also in Cisco IOS Release 12.2(8)YM1. For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*. For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 T*. These two documents list severity 1 and 2 caveats and are located on CCO and the Documentation CD-ROM.

Note If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Service & Support**: **Technical Assistance Center**: **Tool Index**: **Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Resolved Caveats - Release 12.2(8)YM1

Cisco IOS Release 12.2(8)YM1 is a rebuild release for Cisco IOS Release 12.2(8)YM. This section describes unexpected behavior that is fixed in Release 12.2(8)YM1.

CSCdz71127

Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

Cisco has made software available, free of charge, to correct the problem.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

CSCea02355

Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

Cisco has made software available, free of charge, to correct the problem.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

Open Caveats- Release 12.2(8)YM

This section describes unexpected behavior in Release 12.2(8)YM.

CSCdy28747

Microsoft MSN Messenger clients using the SIP protocol will not be able to communicate correctly with each other when NAT is enabled on the router. There is no workaround at present.

CSCin14702

The HSRP **interface track** command sets the decrement value for an interface. It can also be used to modify the decrement value associated with an interface. At any given time, it is possible to have only one such command active for an interface.

However, the router seems to allow multiple track commands to be applied to an interface. Thus, more than one command can be active at any time. The commands get accumulated instead of getting overwritten. When that interface goes down, the decrement values specified in all these commands are added up, and the resulting value is used as the decrement value.

Workaround

Use the **no** version of the **track** command to disable the previous setting for that interface, before issuing a new **track** command to change the decrement value. This will prevent accumulation of **track** commands.

CSCin11465

Easy VPN split tunneling extended ACL issue. This occurs when split tunneling is used in client mode. If the access list at the remote end is configured with two entries that have the same source IP address, the Cisco 806 client will try to install the same address twice and will clean up all the NAT configurations. In this case, one expects NAT to fail. However, NAT on the Cisco 806 continues to work correctly.

CSCin11192

Dial-on-Demand Routing (DDR) is normally triggered by traffic going in the direction opposite the one for which it is enabled. When DDR is enabled on the Cisco 806 for inbound traffic, one does not expect DDR to activate upon detecting incoming traffic. However, DDR activates and the router gets assigned an IP address.

CSCin08502

tftp fails with NAT overload when the router listens for tftp traffic on a non-standard port.

CSCin11017

In lab test scenarios, the Cisco 806 router client crashes after the idle timeout expires for DDR.

Resolved Caveats- Release 12.2(8)YM

This section describes problems that have been fixed in this release.

CSCdw37744

The firewall audit trail test for tftp fails. This problem has been fixed in this release.

CSCin12882

The udpLocalAddress and udpLocalPort objects of the UDP MIB are not populated. This problem has been fixed in this release.

CSCin08637

The rttMonEchoAdminPktDataRequestSize shows an incorrect value during echo. This problem has been fixed in this release.

CSCin08536

The Cisco 806 is unable to resolve the domain name and the router probe timeout occurs for a DNS operation. This problem has been fixed in this release.

CSCin08549

The rttMonCtrlAdminTimeout value does not show the default value. This problem has been fixed in this release.

CSCin12023

The Cisco 827 router crashes while configuring an IP add-on virtual template. This problem has been fixed in this release.

CSCin11373

Ping is not successful when aal5mux ppp encapsulation is used. This problem has been fixed in this release.

CSCin11727

When the permanent virtual circuit (PVC) is removed and configured again, and Point-to-Point Protocol over ATM encapsulation is used, the virtual access interface doesn't come up, causing the ping between the UUT and the remote to fail. This problem has been fixed in this release.

CSCin09643

The NAT translation functionality does not work for IPSec traffic on a Cisco 806. This problem has been fixed in this release.

CSCin10161

The router returns a value of 0 instead of the default value of 1 for the TCP MIB object rttMonEchoAdminPktDataRequestSize. This problem has been fixed in this release.

CSCin08623

The router timeout is lost after a reload if the timeout value is set to a value greater than 60,000 ms and the frequency parameter is set to 300 seconds. Although the timeout setting works in the running configuration, when the configuration is saved and the router is reloaded, the timeout is set to 30,000 ms and the following error message appears.

```
%Illegal Value:  Cannot set Timeout to be greater than Frequency
```

This problem has been fixed in this release.

Related Documentation

The following sections describe the documentation available for the SOHO 70 and Cisco 800 series routers. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules and the Cisco IOS release notes, which are available online on Cisco.com and the Documentation CD-ROM.

Use these release notes with the documents listed in the following sections:

- Release-Specific Documents
- Platform-Specific Documents

Release-Specific Documents

The following documents are specific to Release 12.2 and apply to Release 12.2(8)YM1. They are located on Cisco.com and the Documentation CD-ROM (under the heading **Service & Support**):

- To reach the *Release Notes for the Cisco 806 Routers and the Cisco 820 Series Routers for Cisco IOS Release 12.2(8)YM1*, click this path:

  Technical Documents: **Cisco IOS Software**: **Release 12.2**: **Release Notes**: **Cisco 800 Series Routers**: **Cisco 800 Series - Release Notes for Release 12.2(8)YM**

- To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.2 T*, click this path:

  Technical Documents: **Cisco IOS Software**: **Release 12.2**: **Release Notes**: **Cisco IOS Release 12.2 T**

- To reach product bulletins, field notices, and other release-specific documents, click this path:

  Technical Documents: **Product Bulletins**

- The *Caveats for Cisco IOS Release 12.2* and *Caveats for Cisco IOS Release 12.2 T* documents contain caveats applicable to all platforms for all maintenance releases of Release 12.2. To reach the caveats documents, click this path:

  Technical Documents: **Cisco IOS Software**: **Release 12.2**: **Caveats**

Note If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in toCisco.com and click **Service & Support**: **Technical Assistance Center**: **Tool Index**: **Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents are available for the SOHO 70 and Cisco 800 series routers on Cisco.com and the Documentation CD-ROM.

SOHO 70 and Cisco 800 Series Routers

Documentation specific to the SOHO 70 Series Routers and Cisco 800 Series Routers is available on Cisco.com and the Documentation CD at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/index.htm

This URL is subject to change without notice. If it changes, point your web browser to CCO, and click the following path:

Cisco Product Documentation: **Access Servers and Access Routers**: **Fixed Configuration Access Routers**:**<platform_name>**

Software Configuration

The document *Cisco Router Web Setup User Guide* is available for the Cisco 800 series routers at the following location:

http://www.cisco.com/univercd/cc/td/doc/clckstrt/crws/ugcrws30.htm

This URL is subject to change without notice. If it changes, point your web browser to Cisco.com or the Documentation CD, and click the following path:

Technical Documents: **Router Configuration Tools**: **Cisco Router Web Setup**

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped 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 through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/web/ordering/root/index.html

- 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 Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

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

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

Cisco Systems
Attn: Document Resource Connection
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 online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.

- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

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