



Release Notes for Cisco ONS 15310-MA Release 7.22



Note

The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

August 2007

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15310-MA. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to Release 7.0 of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*, *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*, and the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*, and Release 7.2 of the *Cisco ONS SONET TL1 Command Guide*. For the most current version of the Release Notes for Cisco ONS 15310-MA Release 7.22, visit the following URL:

http://www.cisco.com/en/US/products/hw/optical/ps2001/prod_release_notes_list.html

Cisco also provides Bug Toolkit, a web resource for tracking defects. To access Bug Toolkit, visit the following URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Contents

- [Changes to the Release Notes, page 3](#)
- [Caveats, page 3](#)
- [Resolved Caveats for Release 7.2.x, page 6](#)
- [New Features and Functionality, page 9](#)
- [Related Documentation, page 12](#)



Corporate Headquarters:

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

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

- [Obtaining Documentation, page 13](#)
- [Documentation Feedback, page 14](#)
- [Cisco Product Security Overview, page 14](#)
- [Obtaining Technical Assistance, page 15](#)
- [Obtaining Additional Publications and Information, page 17](#)

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15310-MA Release 7.2* since the production of the Cisco ONS 15310-MA System Software CD for Release 7.22.

The following changes have been added to the release notes for Release 7.2.2.

Changes to New Features and Functionality

The following new feature's summary has been revised to better explain secure mode locking behavior:

[IP Addressing with Secure Mode Enabled, page 9](#)

Caveats

Review the notes listed below before deploying the ONS 15310-MA. Caveats with tracking numbers are known system limitations that are scheduled to be addressed in a subsequent release. Caveats without tracking numbers are provided to point out procedural or situational considerations when deploying the product.

Maintenance and Administration



Caution

VxWorks is intended for qualified Cisco personnel only. Customer use of VxWorks is not recommended, nor is it supported by Cisco's Technical Assistance Center. Inappropriate use of VxWorks commands can have a negative and service affecting impact on your network. Please consult the troubleshooting guide for your release and platform for appropriate troubleshooting procedures. To exit without logging in, enter a Control-D (hold down the Control and D keys at the same time) at the Username prompt. To exit after logging in, type "logout" at the VxWorks shell prompt.

CSCse36337

When a Server Trail is created on a 1+1 Protection Group, the Node's database gets deleted, and the Node goes for continuous reboot. No workaround available. This issue will be resolved in Release 7.22, 8.0.

CSCse89357

CTC Network view shows up without any Nodes. The initialization of the network view sometimes would get interrupted with exceptions. Workaround is to relaunch CTC. This issue will be resolved in a future release.

CSCse96077

On an IO port with this issue false TCAs that indicate line or traffic problems are raised every 15 min after the 15 min pm report. There are no alarms with the associated ports. Traffic is not affected. In Release 7.2, during a very short period when the defect is present (less than 1 sec), false TCAs might be raised. This can be reproduced by either removing or then reinserting the card, or by a small burst of defects.

The cards affected are:

- ONS 15454 DS1, DS1_E1_56, DS3 (including DS3, DS3N, DS3E, DS3NE), DS3_EC1, DS3XM.
- DWDM, E1, E1_42, OC3-8, OC12-4, MRC-12, OC192XFP; and ONS 15310-CL and ONS 15310-MA IO ports.

There are two workarounds:

- Place the affected ports in OOS-DSBLD and then back to IS. This clears the problem for the specific port on the card, but the traffic will be down during the period of OOS-DSBLD.
- Soft reset the card with problem ports. This clears the problem on all ports on the card. Soft reset might cause a protection switch if any circuit path on the card or any port on the card or the card itself is in a protection group. Note that the protection switch itself might cause a defect burst, which might introduce false TCAs. Before resetting the card, check if any circuit, port, or card is in a protection group. If there is path protection, BLSR, 1+1 or 1:1/1:N protection on the card, lock the protection using a switch command (for example, LOCKOUT/LOCKON) available to users before you reset the card ensuring that no protection switch occurs during soft reset, and that traffic will not be affected. For a card with no protection type, simply soft reset the card and traffic will not be affected.

This issue will be resolved in a future release.

CSCsh37934

Unable to create 1+1 Optimized APS (also called J-APS) on a line timed port. Can do so using TL1 . This issue will be resolved in a future release.

CSCsh37934

Unable to create 1+1 Optimized APS (also called J-APS) on a line timed port using CTC. Use TL1 to create the 1+1 Optimized APS. This will be resolved in a future release

CSCsd84638

Sometimes IP connectivity to an ONS 15310-MA is lost and pinging the node fails. Also, as a result, CTC fails to come up. This can occur if both the Ethernet port on the CTXMA card and the Ethernet port on the backplane are accidentally connected to the same network, resulting in loops in the switching network. In normal operation the backport should be used to connect to the network and the frontport should only be used for onsite maintenance. If this issue occurs detach the Ethernet cables from both the frontport and the backport and connect via the backport (or frontport) only, rather than via both at the same time. This issue will not be resolved.

CSCsc56694

IPPM enabled by CTC for an OCn trunk card is disabled automatically after two hours. This issue will be resolved in Release 8.0.

Alarms

CSCsh48090

When there is a mismatch in the Trace Identifier String configured and what is received, TIM-S is raised as expected on 310MA WBE-84 card. Now if we pull the cable, Loss Of Signal (LOS) alarm is raised, however TIM-S is not suppressed. LOS alarm should suppress TIM-S as LOS alarm has higher priority. This will be resolved in a future release.

CSCsh48107

After an upgrade from 7.0 to 7.22 in a Revertive Protection Group set up with two connected nodes and with circuits between them, when issued protection switch from working to protect and back, WKSWPR alarm was not raised. This issue will be resolved in a future release.

CSCse85355 CSCsd52665 CSCsd56328

The NE should report alarms or conditions on ingress port not on any internal ports. Alarm detected at the internal ports (TERM) side will be ingress map to the MON side. So the NE raises the STS-MON/VT-MON and STS-TERM/VT-TERM alarms or conditions on the STS-MON/VT-MON ports, irrespective of the actual detection port (MON or TERM). If the user wants the customized severity to be reflected for a specific STS/VT alarms, the alarm profile entities of both STS-MON and STS-TERM, if available, should be changed to the same severity.

Common Control Cards

CSCsc52028

The CTX 2500 card does not accept more than 52 ENE sessions. Figuring 16 ENE sessions per GNE session, the expected ENE logins for 7 GNE sessions is 112, whereas the CTX 2500 accepts only 52. This issue will not be resolved.

CSCsb62127

A DCC Link discovered by CTC, can show incorrect bandwidth. When a DCC tunnel is created using two different OC cards, like OC12 and OC48 at its ends, CTC Network view shows incorrect bandwidth. Such a provisioning is a provisioning mistake. No workaround available. This issue will be resolved in a future release.

Electrical IO Cards

CSCsh20228

1-Day TCA is not generated for DS1-84. Provision TOD 23:59:59 from TL1 with DST as 0. We have DS3 line errors (LOS). After date is changed after one second of time change, the 1-Day bucket must be restarted. The TCAs must be generated for 1-Day, which is not happening. This issue will be fixed in a future release.

Alarms

CSCsh37976

APSCM(Protection Switching Channel Match Failure) is NOT raised for 1+1 Optimized Protection. The configuration is as below

- Connected 15310MA and 15454 in a OC12 1+1 Protection.
- Slot 3 of 310MA is connected to 15454 Slot 3
- Slot 4 of 310MA is connected to 15454 Slot 4
- Now at 310 MA, created 1+1 Optimized protection, made slot 3 working and slot 4 protection.
- Now at 15454, created 1+1 Optimized protection, made slot 4 working and slot 3 protection.
- As per the above setup, APSCM should have been raised but was not.

This issue is expected to be resolved in a future release.

TL1

**Note**

To be compatible with TL1 and DNS, all nodes must have valid names. Node names should contain alphanumeric characters or hyphens, but no special characters or spaces.

Resolved Caveats for Release 7.2.x

The following items are resolved in Release 7.2.x

Maintenance and Administration

CSCsg52340

Automatic Routing of circuits using CTC 7.2 or higher, on nodes older than 7.2 is not possible. A new NE Default introduced in 7.2, causes this problem. Workaround is to toggle the CIRCUIITS_AUTO_ROUTE_DEFAULT_OVERRIDABLE NE Default. This issue is resolved in Release 7.22, 8.0.

CSCse92125

Attempt to log-in using CTC. CTC login fails. Workaround is to ensure that the PC is not running a Turkish locale. This issue is fixed in Release 8.0.

CSCse99104

CTC can incur either repeated failures when you attempt to log in to an NE, and/or a very long time to discover all ENEs behind a GNE (could be over 30 minutes on a medium sized network). This issue affects all ONS 15xxx releases from R4.1 to 7.2. This condition is more likely to happen on Windows XP after an upgrade to Service Pack 2, and when the network is made of a medium to large number of GNEs/ENEs with SOCKS enabled. This condition can also happen in the case of networks with poor connectivity between CTC and the GNEs.

The solution involves an enhancement to the SOCKS discovery protocol by introducing the concept of designated SOCKS servers. A designated SOCKS server is a NE that runs SOCKS, is LAN connected and has been explicitly marked as a potential SOCKS server by the user. CTC allows the user to enter an unlimited number of designated SOCKS servers. When designated SOCKS servers are defined, the automatic SOCKS server discovery protocol is disabled, resulting in substantial performance improvement during CTC login and ENE discovery.

CSCse53017

Circuit creation when attempted on ML cards between a 7.2 NE and an older NE, the wizard would die. The source should be on 7.2 NE and destination on the older NE. Workaround is to interchange the source and destination. This issue is resolved in Release 7.22, 8.0.

CSCse53017

Circuit creation when attempted on ML cards between a 7.2 NE and an older NE, the wizard would die. The source should be on 7.2 NE and destination on the older NE. Workaround is to interchange the source and destination. This issue is resolved in Release 7.22, 8.0.

Common Control Cards

CSCse01108

When the NE time is changed from CTC (or TL1), the pm bins of the interfaces (OCn/Ds1 on ctx-cl and OCn on 310-MA), which are on the active tcc, does n't get marked as partial. No workaround available. This issue is resolved in Release 7.22 and 8.0.

CSCse98996

The issue can be reproduced as follow:

-
- Step 1** On the node Infy12 went to Network view, Edit--->Preferences---->Checked Display events with Node Time Zone
 - Step 2** Changed the time to 11-Mar-2007 01:59:00 PST and let it pass the 02:00:00 am.
 - Step 3** CTC Node view-->Provisioning-->General Tab correctly showed the changed time as 03:00:00 PDT.
 - Step 4** Generated a LOS on a OC3 card. CTC Alarm pane showed the new PDT time.
 - Step 5** Retrieved audit trail. Audit trail showed the correct PDT time.
-

Electrical Cards

CSCsg23128

All DS3 Ports Automatically Transition to IS State After Card Upgrade. Have a WBE28 card in one of the IO slots (1/2/5/6) of 310MA. Provision admin state of DS3 ports to IS-AINS. Upgrade this card to WBE84 using change card option of CTC window. We see MEA alarm raised. At this time, when we plug-out WBE28 and plug-in WBE84 card, we see WBE84 card comes up and all DS3 ports transition from IS-AINS to IS autonomously. After this, the user can't set the admin state of these ports to IS-AINS as these ports autonomously transition from AINS to IS within few seconds after provisioning. No workaround available. This issue is resolved in Releases 7.22, 7.04 and 8.0.

Alarms

CSCse98987

AIS-P and RFI-P are seen on the same STS if the path terminating equipment is a DS3 card. This happens when you configure a bi-directional circuit using a DS3 card as the path terminating equipment. Inject AIS-P into the circuit. AIS-P and RFI-P are seen on the same STS. This is fixed in 7.22

CSCsh24561

When you change the alarm profile of BITS:SSM-STU from default value which is NA/NSA to CR/MN. The alarm severity changes to CR. BITS-SSM-STU reports a critical alarm event though it is NSA. Single node provisioned in external timing mode with BITS 1 as the primary reference. Connect a testset to BITS-In 1 and feed a DS1 signal with SSM-STU as the Dsn loopcode. BITS reports SSM-STU traceable and the node synchronizes to STU with default NA/NSA severity. Now From the CTC change the alarm profile such that BITS:SSM-STU is set to CR/MN. The alarm severity changes to CR. BITS-SSM-STU reports a critical alarm. This issue will be fixed in Release 8.01.

CSCsf09471

SFP's with a serial number starting with ECL cause the 15310-MA to raise an MEA alarm when using R7.0 or R7.2 sw. This has been seen on Release 7.0 and 7.2. Workaround is to use SFP's with SN#'s that do not start with ECL or upgrade to 7.2.2.

TL1**CSCsg22884**

When the RTRV-T1::<aid>:<ctag>:1::<montype>,,fend; command is issued on a T1 facility on 15310MA DS1-28/84-DS3-EC1-3, the Far End performance monitoring counts are not available on DS1-28/84-DS3-EC1-3 cards through TL1 . However the far end performance monitoring counts can be viewed on the CTC. This issue is fixed in 7.04 and 7.22 and 8.0.

New Features and Functionality

This section highlights new features and functionality for Release 7.2. For complete documentation of each of the features of the ONS 15310-MA, consult the user documentation.

New Software Features

The following sections describe new software features for Release 7.2.

IP Addressing with Secure Mode Enabled

This section addresses Release 7.2 secure mode. It also describes how this mode's locked or unlocked options operate in various scenarios with R7.2, or R7.2 in combination with R7.0.

Secure Mode

In Release 7.2, you can separate LAN interface access from backplane Ethernet port access by use of the secure mode. Additionally, you can lock this mode so that a node's configuration cannot be altered.

The CTX2500 card defaults to nonsecure, unlocked mode. (Your network's defaults may differ; refer to the NE Defaults documentation to confirm them.) In nonsecure mode, the LAN and backplane Ethernet ports share a single MAC address and IP address. The CTX2500 card allows you to place a node in secure mode to prevent a LAN port user from accessing the network through the backplane port. Secure mode can also be locked, which prevents the mode from being altered.

Dual IP Addresses

Changing an ONS 15310-MA node from nonsecure mode to secure mode allows you to provision two Ethernet addresses for the node and causes the active CTX2500 to assign the ports different MAC addresses. In secure mode, one IP address is provisioned for the ONS 15310-MA backplane Ethernet port and the other is provisioned for the CTX2500 LAN port. Both addresses reside on different subnets and packets are not exchanged between these two ports. The dual addresses provide an additional layer of separation between the LAN access port and the ONS 15310-MA network. If secure mode is enabled, the IP addresses provisioned for both ports must follow general IP addressing guidelines and must reside on different subnets from each other and the default router IP address.

In secure mode, the LAN port IP address becomes a private address while the backplane port connects the node to an Operations Support System (OSS) through a central office or private enterprise network. A superuser can configure the node to hide or reveal the backplane's Ethernet IP address in CTC, the routing table, or autonomous message reports.

Secure Mode Locking

A superuser can convert a secure node from unlocked to locked mode. Doing so permanently changes the chassis hardware. The procedure for placing a node in secure mode or secure locked mode is similar to the process for an ONS 15454 node. Refer to the "Manage the Node" chapter in the *Cisco ONS 15454 Procedure Guide* for instructions.

When a node is secure and locked, its configuration, Ethernet port status, its secure mode, and the locked status cannot be changed by any network user—including a superuser. To have a secure node's lock removed, contact Cisco Technical Support to arrange a Return Material Authorization (RMA) for the chassis and the CTX2500 card(s). Refer to the Obtaining Technical Assistance section of the *Cisco ONS 15310- CL and ONS 15310-MA Procedure Guide* as needed.

When a node is secure and locked, its configuration, Ethernet port status, its secure mode, and the locked status cannot be changed by any network user—including a superuser. To have a secure node's lock removed, contact Cisco Technical Support to arrange a Return Material Authorization (RMA) for the chassis and the CTX2500 card(s). Refer to the Obtaining Technical Assistance section of the *Cisco ONS 15310- CL and ONS 15310-MA Procedure Guide* as needed.



Note

If a CTX2500 card or chassis needs to be unlocked, the locked cards and chassis need to be unlocked together by Cisco Technical Support. RMA the cards and chassis together.

Mixed Release Shelf Scenarios

When an active CTX2500 card is converted to locked mode, the standby CTX2500 card and chassis are also changed. The components retain their locked status even if separated.



Caution

Enabling secure mode on a CTX2500 card causes it to reboot.

**Note**

A chassis can only be locked by using Release 7.2 software on the active CTX2500 controller card.

**Note**

Software Release 7.0 does not support secure mode locking. This software's behavior in a R7.2 node depends upon where it is used.

Following are some example scenarios using locked or unlocked Release 7.2 and Release 7.0 components:

- If you insert two unlocked R 7.2 CTX2500 cards into a locked chassis, the chassis hardware lock prevails and converts the cards to locked.
- If you remove both CTX2500 cards from a locked chassis and insert both cards into an unlocked R7.2 chassis, the lock follows the active controller card and converts the unlocked chassis to locked.
- If you remove a locked standby CTX2500 from a shelf and insert it as active in an unlocked R7.2 chassis, the locks follows the active controller card and converts the chassis and standby card to locked.
- If you insert a locked CTX2500 as standby into an R7.2 chassis with an unlocked active CTX2500, the active card overwrites the standby card's lock. The chassis remains unlocked.
- If you insert an R7.0 CTX2500 as standby card in a locked chassis (with an active R7.2 card), the active card updates the standby card software version to R7.2. After R7.2 is fully loaded on the standby card, the chassis activates the standby's lock status.

Node Role Flexibility

In nonsecure mode, a node can be a GNE or ENE. Placing the node into secure mode automatically turns on SOCKS proxy and defaults the node to GNE status. However, the node can be changed back to an ENE. In nonsecure mode, an ENE's SOCKS proxy can be disabled—effectively isolating the node beyond the LAN firewall—but it cannot be disabled in secure mode. To change a node's GNE or ENE status and disable the SOCKS proxy, refer to the “Turn Up a Node” chapter in the *Cisco ONS 15310-CL and ONS 15310-MA Procedure Guide*.

**Note**

If the LAN and backplane access ports are disabled in an ENE and the node is isolated from DCC communication (due to user provisioning or network faults), the LAN and backplane ports are automatically reenabled.

Network Circuit Automatic Routing Overridable NE Default

The Network Circuit Automatic Routing Overridable NE default makes it possible to set by default whether or not a user creating circuits can change (override) the automatic circuit routing setting (also provisionable as a default).

The new NE default supporting this feature is:

```
CTC.circuits.RouteAutomaticallyDefaultOverridable
```

This default works in combination with the existing circuit routing default:

```
CTC.circuits.RouteAutomatically
```

The overridable option enables network administrators to manage how circuits are created on a network-wide basis. For example, if the Automatic Circuit Routing default is set to FALSE (the check box is unchecked by default), then setting the Network Circuit Automatic Routing Overridable default to FALSE ensures that manual circuit routing is enforced for all users creating circuits (the default is not overridable by the user). When the Network Circuit Automatic Routing Overridable default is set to TRUE (the factory configured setting) users can click in the Automatic Routing check box to change the automatic routing setting if they wish.

When the Route Automatically check box is not selectable during circuit creation, the following automatic routing sub-options will also be unavailable:

- Using Required Nodes/Spans
- Review Route Before Creation

Like the Automatic Circuit Routing default, the Network Circuit Automatic Routing Overridable default applies to all nodes in the network. The Route Automatically check box is either overridable or not depending on how the default is set for the node you are logged into through CTC. To ensure correct behavior after setting the default, propagate the chosen default setting to all nodes through which users might log into the network to perform provisioning. For more information on NE defaults and their provisioning consult the user documentation.

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15310-MA Release 7.0*
- *Release Notes for the Cisco ONS 15310-CL Release 7.2*
- *Release Notes for the Cisco ONS 15454 SDH Release 7.2*
- *Release Notes for the Cisco ONS 15327 Release 7.2*
- *Release Notes for the Cisco ONS 15600 Release 7.2*
- *Release Notes for the Cisco ONS 15454 Release 7.2*

Platform-Specific Documents

- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*
Provides installation, turn up, test, and maintenance procedures
- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*
Provides technical reference information for cards, nodes, and networks
- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*
Provides a list of SONET alarms and troubleshooting procedures, general troubleshooting information, transient conditions, and error messages
- *Cisco ONS SONET TL1 Command Guide*
Provides a comprehensive list of TL1 commands
- *Cisco ONS SONET TL1 Reference Guide*
Provides general information, procedures, and errors for TL1

- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*
Provides software feature and operation information for Ethernet cards

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/>

Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco ONS 15xxx product documentation, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated periodically and may be more current than printed documentation.

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
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://cisoiq.texterity.com/cisoiq/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>

Use this document in conjunction with the documents listed in the “Related Documentation” section on page 12.

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

© 2006 Cisco Systems, Inc. All rights reserved.

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.