Release Notes for *Cisco ONS 15540 ESP* for Cisco IOS Release 12.2(29)SV3

This document describes caveats for Cisco IOS Release 12.2(29)SV3 for the Cisco ONS 15540 ESP (Extended Services Platform).

Date: May 22, 2007

Text Part Number OL-12760-01

Contents

This document includes the following information:

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

Introduction

The Cisco ONS 15540 ESP is an optical transport platform that employs DWDM (dense wavelength division multiplexing) technology. With the Cisco ONS 15540 ESP, users can take advantage of the availability of dark fiber to build a common infrastructure that supports data, SAN (storage area networking), and TDM (time-division multiplexing) traffic. For more information about DWDM technology and applications, refer to the *Introduction to DWDM Technology* publication and the *Cisco ONS 15540 ESP Planning Guide*.

System Requirements

This section describes the system requirements for the Cisco ONS 15540 ESP and includes the following sections:

Memory Requirements

The DRAM memory configuration is 128 MB, which is the default for the Cisco ONS 15540 ESP.

Hardware Supported

Table 1 lists the hardware components supported on the Cisco ONS 15540 ESP and the minimum software version required. See the "Determining the Software Version" section on page 6.

Table 1 Cisco ONS 15540 ESP Supported Hardware Modules and Minimum Software Requirements

Component	Part Number	Description	Minimum Software Version Required
Chassis	15540-CHSA		12.1(7a)EY2
Power supplies	15540-PWR-AC	120 to 240 VAC power supply	12.1(7a)EY2
	15540-CAB-AC	Custom AC-input power entry cable	12.1(7a)EY2
	15540-CAB-AC	North America	12.1(7a)EY2
	15540-CAB-ACA	Australia	12.1(7a)EY2
	15540-CAB-ACE	Europe	12.1(7a)EY2
	15540-CAB-CU	UK	12.1(7a)EY2
	15540-CAB-ACI	Italy	12.1(7a)EY2
	15540-CAB-ACR	Argentina	12.1(7a)EY2

Table 1 Cisco ONS 15540 ESP Supported Hardware Modules and Minimum Software Requirements (continued)

Component	Part Number	Description	Minimum Software Version Required
Filler motherboards and filler modules	15540-COV-01	Mux/demux motherboard blank panel	12.1(7a)EY2
	15540-COV-02	Mux/demux module	12.1(7a)EY2
	15540-COV-03	Line card motherboard blank panel	12.1(7a)EY2
	15540-COV-04	Transponder module blank panel	12.1(7a)EY2
	15540-COV-06	Processor card cover panel	12.1(7a)EY2
Fans	15540-FTMP	Fan tray module populated with eight fans	12.1(7a)EY2
Processor cards	15540-CPU	Processor card without switch fabric	12.1(7a)EY2
Mux/demux motherboards	15540-MMMB-0100	Supports mux/demux modules with OSC	12.1(7a)EY2
	15540-MMMB-0200	Supports mux/demux modules without OSC	12.1(7a)EY2
Mux/demux modules without OSC	15540-MDXA-04A0	4-channel Band A	12.1(7a)EY2
	15540-MDXA-04B0	4-channel Band B	12.1(7a)EY2
	15540-MDXA-04C0	4-channel Band C	12.1(7a)EY2
	15540-MDXA-04D0	4-channel Band D	12.1(7a)EY2
	15540-MDXA-04E0	4-channel Band E	12.1(7a)EY2
	15540-MDXA-04F0	4-channel Band F	12.1(7a)EY2
	15540-MDXA-04G0	4-channel Band G	12.1(7a)EY2
	15540-MDXA-04H0	4-channel Band H	12.1(7a)EY2
	15540-MDXA-08A0	8-channel Band AB	12.1(7a)EY2
	15540-MDXA-08B0	8-channel Band CD	12.1(7a)EY2
	15540-MDXA-08C0	8-channel Band EF	12.1(7a)EY2
	15540-MDXA-08D0	8-channel Band GH	12.1(7a)EY2
	15540-MDXA-16EH	16-channel Band EH	12.1(7a)EY2
Mux/demux modules with OSC	15540-MDXA-04A0	4-channel Band A	12.1(7a)EY2
	15540-MDXB-04B0	4-channel Band B	12.1(7a)EY2
	15540-MDXB-04C0	4-channel Band C	12.1(7a)EY2
	15540-MDXB-04D0	4-channel Band D	12.1(7a)EY2
	15540-MDXB-04E0	4-channel Band E	12.1(7a)EY2
	15540-MDXB-04F0	4-channel Band F	12.1(7a)EY2
	15540-MDXB-04G0	4-channel Band G	12.1(7a)EY2
	15540-MDXB-04H0	4-channel Band H	12.1(7a)EY2
	15540-MDXB-08A0	8-channel Band AB	12.1(7a)EY2
	15540-MDXB-08B0	8-channel Band CD	12.1(7a)EY2
	15540-MDXB-08C0	8-channel Band EF	12.1(7a)EY2
	15540-MDXB-08D0	8-channel Band GH	12.1(7a)EY2
	15540-MDXB-16AD	16-channel Band AD	12.1(7a)EY2

Table 1 Cisco ONS 15540 ESP Supported Hardware Modules and Minimum Software Requirements (continued)

Component	Part Number	Description	Minimum Software Version Required
Line card motherboards	15540-LCMB-0100	Supports four transponders with protection	12.1(7a)EY2
	15540-LCMB-0200	Supports four transponders -East	12.1(7a)EY2
	15540-LCMB-0201	Supports four transponders -West	12.1(7a)EY2
MM transponder modules	15540-TSP1-01A3	Ch 1-2 —1310-nm MM 16 to 622 Mbps with SC	12.1(7a)EY2
	15540-TSP1-03A3	Ch 3-4 — 1310-nm MM 16 to 622 Mbps with SC	12.1(7a)EY2
	15540-TSP1-05A3	Ch 5-6 —1310-nm MM 16 to 622 Mbps with SC	12.1(7a)EY2
	15540-TSP1-07A3	Ch 7-8 — 1310-nm MM 16 to 622 Mbps with SC	12.1(7a)EY2
	15540-TSP1-09A3	Ch 9-10 — 1310-nm MM 16 to 622 Mbps with SC	12.1(7a)EY2
	15540-TSP1-11A3	Ch 11-12 — 1310-nm MM 16 to 622 Mbps with SC	12.1(7a)EY2
	15540-TSP1-13A3	Ch 13-14 — 1310-nm MM 16 to 622 Mbps with SC	12.1(7a)EY2
	15540-TSP1-15A3	Ch 15-16 — 1310-nm MM 16 to 622 Mbps with SC	12.1(7a)EY2
	15540-TSP1-17A3	Ch 17-18 — 1310-nm MM 16 to 622 Mbps with SC	12.1(7a)EY2
	15540-TSP1-19A3	Ch 19-20 — 1310nm MM 16 to 622 Mbps with SC	12.1(7a)EY2
	15540-TSP1-21A3	Ch 21-22 — 1310-nm MM 16 to 622 Mbps with SC	12.1(7a)EY2
	15540-TSP1-23A3	Ch 23- 24—1310-nm MM 16 to 622 Mbps with SC	12.1(7a)EY2
	15540-TSP1-25A3	Ch 25-26—1310-nm MM 16 to 622 Mbps with SC	12.1(7a)EY2
	15540-TSP1-27A3	Ch 27-28—1310-nm MM 16 to 622 Mbps with SC	12.1(7a)EY2
	15540-TSP1-29A3	Ch 29-30—1310-nm MM 16 to 622 Mbps with SC	12.1(7a)EY2
	15540-TSP1-31A3	Ch 31-32—1310-nm MM 16 to 622 Mbps with SC	12.1(7a)EY2

Table 1 Cisco ONS 15540 ESP Supported Hardware Modules and Minimum Software Requirements (continued)

Component	Part Number	Description	Minimum Software Version Required
SM transponder modules	15540-TSP1-01B3	Ch 1-2—1310-nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
	15540-TSP1-03B3	Ch 3-4—1310-nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
	15540-TSP1-05B3	Ch 5-6—1310-nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
	15540-TSP1-07B3	Ch 7-8—1310-nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
	15540-TSP1-09B3	Ch 9-10—1310-nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
	15540-TSP1-11B3	Ch 11-12—1310-nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
	15540-TSP1-13B3	Ch 13-14— 1310-nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
	15540-TSP1-15B3	Ch 15-16—1310-nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
	15540-TSP1-17B3	Ch 17-18—1310-nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
	15540-TSP1-19B3	Ch 19-20—1310nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
	15540-TSP1-21B3	Ch 21-22—1310-nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
	15540-TSP1-23B3	Ch 23- 24—1310-nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
	15540-TSP1-23B3	Ch 23- 24—1310-nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
	15540-TSP1-25B3	Ch 25-26—1310-nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
	15540-TSP1-27B3	Ch 27-28—1310-nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
	15540-TSP1-29B3	Ch 29-30 —1310-nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
	15540-TSP1-31B3	Ch 31-32—1310-nm SM 16 Mbps to 2.5 Gbps with SC	12.1(7a)EY2
Type 2 extended range transponder modules	15540-TSP2-0100	Ch 1-2	12.1(11b)E
	15540-TSP2-0300	Ch 3-4	12.1(11b)E
	15540-TSP2-0500	Ch 5-6	12.1(11b)E
	15540-TSP2-0700	Ch 7-8	12.1(11b)E
	15540-TSP2-0900	Ch 9-10	12.1(11b)E
	15540-TSP2-1100	Ch 11-12	12.1(11b)E
	15540-TSP2-1300	Ch 13-14	12.1(11b)E
	15540-TSP2-1500	Ch 15-16	12.1(11b)E
	15540-TSP2-1700	Ch 17-18	12.1(11b)E
	15540-TSP2-1900	Ch 19-20	12.1(11b)E
	15540-TSP2-2100	Ch 21-22	12.1(11b)E
	15540-TSP2-2300	Ch 23-24	12.1(11b)E
	15540-TSP2-2500	Ch 25-26	12.1(11b)E
	15540-TSP2-2700	Ch 27-28	12.1(11b)E
	15540-TSP2-2900	Ch 29-30	12.1(11b)E
	15540-TSP2-3100	Ch 31-32	12.1(11b)E

Table 1 Cisco ONS 15540 ESP Supported Hardware Modules and Minimum Software Requirements (continued)

Component	Part Number	Description	Minimum Software Version Required
Fixed rate SFP optics for Type 2 extended range transponder modules	15500-XVRA-01A2	ESCON and OC-3 1310-nm MM MT-RJ	12.1(11b)E
	15500-XVRA-03B1	Gigabit Ethernet and Fibre Channel (1 Gbps) 1310-nm SM MTLC	12.1(11b)E
	15500-XVRA-03B2	1-Gbps Fibre Channel and 2 Gbps Fibre Channel 1310-nm SM MTLC	12.1(11b)E
	15500-XVRA-02C1	Gigabit Ethernet and Fibre Channel (1 Gbps) 850-nm MM MTLC	12.1(11b)E
	15500-XVRA-02C2	Fibre Channel (1 Gbps and 2 Gbps) 850-nm SM MTLC	12.1(11b)E
	15500-XVRA-06B1	SONET OC-12 1310-nm SM MTLC	12.1(11b)E
	15500-XVRA-07B1	SONET OC-48 1310-nm SM MTLC	12.1(11b)E
Variable rate SFP optics	15500-XVRA-10A1	Low band (16 to 200 Mbps) variable rate, MM (1310 nm) with LC	12.1(12c)EV3
	15500-XVRA-10B1	Low band (16 to 200 Mbps) variable rate, SM (1310 nm) with LC	12.1(12c)EV3
	15500-XVRA-11A1	Mid band (200 to 622 Mbps) variable rate, MM (1310 nm) with LC	12.1(12c)EV3
	15500-XVRA-11B1	Mid band (200 to 1250 Mbps) variable rate, SM (1310 nm) with LC	12.1(12c)EV3
	15500-XVRA-12B1	High band (1.062 Gbps to 2.5 Gbps) variable rate, SM (1310 nm) with LC	12.1(12c)EV3

Determining the Software Version

Note We strongly recommend that you use the latest available software release for all Cisco ONS 15540 ESP hardware.

To determine the version of Cisco IOS software currently running on a Cisco ONS 15540 ESP system, log in to the system and enter the **show version** EXEC command. The following sample output is from the **show version** command. The software version number is shown on the second line of the sample output.

```
Switch# show version
Cisco Internetwork Operating System Software
IOS (tm) ONS-15540 Software (ONS15540-I-M), Version 12.2(29)SV3
<Information deleted>
```

Upgrading the System Image

To ensure proper system functioning, follow the system image upgrading procedure described in the *Cisco ONS 15540 ESP Software Upgrade Guide*.

Note Always set the configuration register to 0x2102 when upgrading the system image using the **config-reg 0x2102** command in configuration mode.

Caution Improper system image upgrades can affect system functioning and redundancy. Always follow the recommended upgrade procedures.

Feature Set Table

The Cisco IOS Release software is packaged in feature sets (also called software images) depending on the platform. Each feature set contains a specific set of Cisco IOS features. Table 2 lists the Cisco IOS software feature sets available for the Cisco ONS 15540 ESP.

Table 2 Feature Sets Supported by the Cisco ONS 15540 ESP

Feature Set	Introduced in This Release
Gigabit Ethernet	12.1(7a)EY2
Fast Ethernet	12.1(7a)EY2
Ethernet	12.1(7a)EY2
ATM OC-3/STM-1, OC-12/STM-4, and OC-48/STM-16	12.1(7a)EY2
SONET[1]/SDH[2]	12.1(7a)EY2
POS[3]	12.1(7a)EY2
Coupling link	12.1(7a)EY2
Fibre Channel (1 Gbps)	12.1(7a)EY2
Fibre Channel (2 Gbps)	12.1(7a)EY2
FDDI[4]	12.1(7a)EY2
ESCON[5] SM (200 Mbps)	12.1(7a)EY2
FICON[6] (800 Mbps)	12.1(7a)EY2
FICON (1 Gbps)	12.1(12c)EV3
Token Ring	12.1(7a)EY2
SNMP	12.1(7a)EY2
CiscoView	12.1(7a)EY2
Cisco Transport Manager	12.1(7a)EY2
IP packets	12.1(7a)EY2
OSCP[7]	12.1(7a)EY2
APS[8] protocol packets	12.1(7a)EY2
Point-to-point	12.1(7a)EY2
Hubbed ring	12.1(7a)EY2
Meshed ring	12.1(7a)EY2

Table 2 Feature Sets Supported by the Cisco ONS 15540 ESP (continued)

Feature Set	Introduced in This Release
IBM GDPS[9] ETR/CLO[10]	12.1(7a)EY2
IBM GDPS[9] coupling link	12.1(7a)EY2
2-Gbps Fibre Channel protocol monitoring on transponder modules	12.2(18)SV
2-Gbps FICON protocol monitoring on transponder modules	12.2(18)SV
Functional image version diagnostics	12.2(18)SV
2-Gbps ISC links peer mode protocol monitoring on 2.5-Gbps transponder modules	12.2(22)SV
1-Gbps ISC links peer mode protocol monitoring on transponder modules	12.2(23)SV
SSHv1 client and server support	12.2(24)SV
SNMPv3 support	12.2(24)SV
Counter preservation on processor card switchovers	12.2(24)SV
Performance history counter support on Cisco ONS 15540 line cards	12.2(29)SV
SSHv2 support on Cisco ONS 15540	12.2(29)SV
Critical temperature shutdown support on Cisco ONS 15540. Temperature alarm thresholds can be configured.	12.2(29)SV

1. SONET = Synchronous Optical Networking
2. SDH = Synchronous Digital Hierarchy
3. POS = Packet over SONET
4. FDDI = Fiber Distributed Data Interface
5. ESCON = Enterprise Systems Connection
6. FICON = Fiber Connection
7. OSCP = Optical Supervisory Channel Protocol
8. APS = Automatic Protection Switching
9. GDPS = Geographically Dispersed Parallel Sysplex
10. ETR/CLO = external timer reference/control link oscillator

New and Changed Information

This section lists new features that appear in this and previous releases of Cisco IOS Release 12.2. The new features are sorted by release number.

New Features in Release 12.2(29)SV3

There are no new features for this release.

New Features in Release 12.2(29)SV1

There are no new features for this release.

New Features in Release 12.2(29)SV

The following new software features are available for the Cisco ONS 15540 ESP in Cisco IOS Release 12.2(29)SV:

- Performance history counter support on Cisco ONS 15540 ESP line cards.
- SSHv2 support.
- Critical temperature shutdown and configurable temperature alarm thresholds are supported.

New Features in Release 12.2(26)SV1

There are no new features for this release.

New Features in Release 12.2(26)SV

There are no new features for this release.

New Features in Release 12.2(25)SV

There are no new features for this release.

New Features in Release 12.2(24)SV

The following new software features are available for the Cisco ONS 15540 ESP in Cisco IOS Release 12.2(24)SV:

- SSHv1 client and server support
- SNMPv3 support
- Counter preservation on processor card switchovers

New Features in Release 12.2(23)SV

The following new software feature is available for the Cisco ONS 15540 ESP in Cisco IOS Release 12.2(23)SV:

- 1-Gbps ISC links peer mode protocol monitoring on the transponder module

New Features in Release 12.2(22)SV

The following new software feature is available for the Cisco ONS 15540 ESP in Cisco IOS Release 12.2(22)SV:

- 2-Gbps ISC links peer mode protocol monitoring on 2.5-Gbps transponder modules.

Note 2-Gbps Fibre Channel/FICON protocol monitoring requires transponder functional image release 1.A3 or later.

New Features in Release 12.2(18)SV2

No new features are available for this release.

New Features in Release 12.2(18)SV1

No new features are available for this release.

New Features in Release 12.2(18)SV

The following new software features are available for the Cisco ONS 15540 ESP in Cisco IOS Release 12.2(18)SV:

- 2-Gbps Fibre Channel protocol monitoring on 2.5-Gbps transponder modules

  Note 2-Gbps Fibre Channel/FICON protocol monitoring requires transponder functional image release 1.A3 or later.

- 2-Gbps FICON protocol monitoring on 2.5-Gbps transponder modules

  Note 2-Gbps Fibre Channel/FICON protocol monitoring requires transponder functional image release 1.A3 or later.

- Data file with upgrade information for the ROMMON and functional images
- **show upgrade-info functional-image** command

Caveats

This section describes open and resolved severity 1 and 2 caveats and certain severity 3 caveats. The "Open Caveats" section lists open caveats that apply to the current release and may apply to previous releases. The "Resolved Caveats" sections list caveats resolved in a particular release, but open in previous releases.

Open Caveats in Release 12.2(29)SV3

- CSCsb12598

  Symptom: Cisco IOS device crashes while processing malformed Secure Sockets Layer (SSL) packets. This is caused when a malicious client sends malformed packets during the SSL protocol exchange with the vulnerable device.

This causes the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS). However, they are not known to compromise either the confidentiality or integrity of the data or the device and will not allow an attacker to decrypt anypreviously encrypted information.

Workaround: Cisco has made free software available to address these vulnerabilities for affected customers.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsb40304

Symptom: Cisco IOS device crashes while processing malformed Secure Sockets Layer (SSL) packets. This is caused when a malicious client sends malformed packets during the SSL protocol exchange with the vulnerable device.

This causes the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS). However, they are not known to compromise either the confidentiality or integrity of the data or the device and will not allow an attacker to decrypt anypreviously encrypted information.

Workaround: Cisco has made free software available to address these vulnerabilities for affected customers.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsd92405

  Symptom: Cisco IOS device crashes while processing malformed Secure Sockets Layer (SSL) packets. This is caused when a malicious client sends malformed packets during the SSL protocol exchange with the vulnerable device.

  This causes the following vulnerabilities:

  – Processing ClientHello messages, documented as Cisco bug ID CSCsb12598

  – Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304

  – Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS). However, they are not known to compromise either the confidentiality or integrity of the data or the device and will not allow an attacker to decrypt anypreviously encrypted information.

  Workaround: Cisco has made free software available to address these vulnerabilities for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsh84591

  Symptom: When using the line subcommand login, the vty may get in to a state where the user will not be able to log in to the IOS router. The user will be presented with password followed immediately by "Bad passwords", without anything being entered. The line in this state can be seen with the exec command show line <line number>. In the "Status" line, if 'Ctrl-c Enabled' appears, then you may see this problem on that line.

  Workaround: The condition on the line can be cleared by reloading the router. Without reloading, it is possible to clear this condition by following these sequence of steps. First remove the login from the line. Telnet into the router on the line which is in this state. From enable mode, run the command setup. When prompted with "Continue with configuration dialog" type no. Add the login back to the vty line. Access to the gateway would need to be either through the console or another vty not in this state to first remove the line login command. If console access is not possible and the vty in this state is the first vty on the router, try opening up multiple (two or more) simultaneous telnet sessions to the router. The first one will fail but the second session should access a vty not in this faulty state.

- CSCee75578

Symptom: Ons15540 system may reload on performing an FPGA upgrade for a 2.5Gig transparent transponder.

Workaround: None

- CSCed74239

  Symptom: Though the working trunk has a failure, the protection path may not become active for a Y-cable APS link when the client device is administratively shutdown and restarted.

  Conditions: The symptom may be observed on some FC devices connected to 2.5-Gbps transparent transponder cards.

  Workaround: Configure a loopback interface on the client side to restore the traffic.

- CSCee70825

  Symptom: During normal operation, an outage may result when trying to connect through the console port. The console port issues error messages. These can be routine messages relating to Loss of Light on wave ports that were enabled. Interface alarm flapping may cause a hardware watchdog timeout that failed to switchover to the standby processor card.

  Workaround: None

- CSCee75578

  Symptom: The GE optical link fails to come up between two Catalyst 65xx 8-port GBIC modules through the Cisco ONS 15540 transparent transponders when Forward Laser Control (FLC) is enabled on the system. The link fails to come up irrespective of the type of protection scheme.

  Workaround: Use a 16-port GBIC module on the Catalyst 65xx or deactivate FLC on the Cisco ONS 15540.

- CSCef12108

  Symptom: The Cisco ONS15540 might not allow you to connect to the standby processor card due to an authentication failure. This occurs when AAA or a local database is used for user authentication as this information (AAA or local database) is not replicated from the active to the standby processor card.

  Workaround: None.

- CSCin86897

  Symptom: A temporary traffic interruption in 2.5G transparent transponders during ONS 15540 and 15530 CPU switchover. This depends on the software versions of the Active CPU before and after the switchover. When the switchover is complete, traffic resumes. This symptom is intermittent and may not affect all transponders in a chassis.

  The traffic interruption may occur for the following types of encapsulation:

  - ETR/CLO

  - 100-Mbps Fast Ethernet / FDDI

  - 1-Gbps FC/FICON

  - 1-Gbps ISC (ISC-1, ISC-3 peer mode, 1-Gbps)

  - 2-Gbps FC/FICON

  - 2-Gbps ISC (ISC-3 peer mode, 2 Gbps)

  Conditions: This can occur when switching from a CPU that is running on IOS software without the fix for CSCec64326, to a CPU running on IOS software with the fix for CSCec64326. The fix for CSCec64326 involves changes to hardware settings, causing the temporary datahit.

  Workaround: None. The problem will be fixed in a future release of IOS software.

- CSCsa51395

  Symptom: The client Laser on the ten gig interface goes down for around 4 to 5 seconds, when the FLC is configured on the waveethernetphy interface and PSM APS switchover happens on an ONS 15540 setup with a combination of 10GE transponder and PSM APS.

  Workaround: Disable FLC on Waveethernetphy interface.

- CSCse28718

  Symptom: Ons15540 system may reload on performing an FPGA upgrade. FPGA upgrade is done for Type-1 TSP. This is a rare occurence.

  Workaround: None.

Resolved Caveats in Release 12.2(29)SV3

- CSCse51920

  Symptom: It is possible to add "SNMP-server host", but cannot remove it from the config.
  Workaround: Reload the router with a new startup config.

- CSCse50139

  Symptom: Client and Trunk Laser shut down after a cpu switchover, if any OIR was performed on the card earlier. This problem is seen on a 2.5Gig transparent transponder. The OIR related operations include i) FPGA upgrade, ii) physical OIR of LCMB or TSP; iii) And any OIR simulation debug commands. This problem is observed on IOS versions 12.2(25)SV or later; and on all FPGA versions.

  Workaround: After switchover shut/no shut the interfaces bring back the laser in up state.

  If you happen to perform a OIR operation on a 2.5Gig transparent transponder, do the following in a maintenance window.

  i) Perform a cpu switchover

  ii) shut/no shut the interfaces with laser shut issue

  Now, the future cpu switchovers, wouldn't cause the above problem.

- CSCed90109

  Symptom: Spurious low warning alarms may be indicated on a ONS15540 system having PSM module. These spurious alarms are indicated for the wdmsplit interfaces of the PSM module and they are asserted even though the actual power level received on the interface is above the low warning threshold limit. These spurious alarms may appear once in a couple of hours. These alarms can be ignored; they do not affect any functionality.

  Workaround: None. These spurious alarms do not affect any functionality and hence can be ignored

Resolved Caveats in Release 12.2(29)SV1

- CSCsb38669

  Symptom: When there are no connections on the OSC wave interface, the state of the interface and the line protocol must be `down`, and signal quality must be `Loss of Light`. But, the **show interface** command incorrectly displays the wave interface state as `up`, and the signal quality as `good`.

Conditions: The symptom is observed only when the PSM is inserted in subslot 0 of the motherboard.

Workaround: Insert the PSM in any other subslot.

- CSCsd40488

  Symptom: The performance history counters for the wave interface of the 2.5-Gbps transparent transponder linecards are not displayed.

  Condition: None.

  Workaround: None.

- CSCsd43471

  Symptom: The CVRD thresholds are incorrectly displayed in the **show interface** output for FC 1 Gbps and FC 2 Gbps encapsulations. These thresholds are used in the 2.5-Gbps transparent transponder linecards.

  Condition: None.

  Workaround: None.

- CSCsd12813

  Symptom: The help string for the sdh encapsulation STM-16 rate configuration is incorrect for the 2.5-Gbps transparent transponder.

  Condition: None.

  Workaround: None.

- CSCin86829

  Symptom: The PSM hardware supports optical power monitoring of the wdmsplit interfaces only for a specific range (0 to -24 dBm). The software does not extrapolate for the other power levels (up to 17 dBm) around the hardware supported range.

  Condition: None.

  Workaround: None.

Resolved Caveats in Release 12.2(29)SV

- CSCsb26802

  Symptom: When a client or trunk laser fails, the **show facility-alarm status** command displays the `Line laser failure detected` error message. However, this error message does not indicate which laser has failed.

  Condition: This symptom is observed on Cisco ONS 15540 ESPx cards when there are transparent transponders.

  Workaround: None.

- CSCsb97958

  Symptom: Adding a Cisco ONS 15540 in to CiscoWorks Resource Manager Essentials 4.0 fails with `RICS0001` error.

Condition: This symptom is observed while adding a Cisco ONS 15540 that is running on Cisco IOS Release 12.2(18)SV2.

Workaround: None.

- CSCsb35798

  Symptom: The Cisco ONS 15540 ESPx node may reload on performing **shut**/**no shut** on the wavee or wavepatch interface.

  Conditions: This symptom is observed if the optical monitoring trap is enabled on the node.

  Workaround: None.

- CSCsc51288

  Symptom: Cisco Transport Manager (CTM) does not retrieve the software version of the standby CPU of Cisco ONS 15540 ESPx, and marks the related network element (NE) as unreachable.

  Conditions: This symptom is observed with Cisco IOS Release 12.2(24)SV or later. The symptom may not occur if the NE is lightly equipped (few transponder modules).

  Workaround: None.

- CSCed75110

  Symptom: If a protection switch module (PSM) is placed in subslot 0 of a LCMB, the optical supervisory channel (OSC) wave interface goes into an invalid state. The OSC recovers when the PSM module is removed from subslot0. If the chassis is reloaded with the PSM in subslot 0, the OSC wave interface will not be operational.

  Workaround: Do not place the PSM module in subslot0 of the LCMB if the OSC port on that LCMB is being used.

- CSCee70185

  Symptom: An informational warning is issued instead of a critical alarm when the line cards are shut down in response to a multiple fan failure event after issuing the **environment-monitor shutdown fan** command.

  Workaround: None.

- CSCsa71267

  Symptom: The Cisco ONS 15540 ESP system does not shutdown if the fan tray is removed or is faulty.

  Conditions: None.

  Workaround: None.

Resolved Caveats in Release 12.2(26)SV1

- CSCuk58617

  Symptom: The physical Performance Monitoring (PM) statistics may not be collected correctly.

  Condition: This symptom is observed on a Cisco ONS15500 series card that is configured for SNMP when optical monitoring traps are enabled.

  Workaround: None.

- CSCei25594

  Symptom: Memory leak may occur when CiscoView is used to monitor a router.

Condition: This condition may be seen on routers running 12.2(26)SV.

Workaround: None.

Resolved Caveats in Release 12.2(26)SV

- CSCeg84037

  Symptom: When a CPU switchover is performed on an ONS 15540 or ONS 15530 system, the memory utilization on the new primary increases by 10MB. In such a case, the memory utilization may go up to 85%. This problem is seen only with 12.2 based images.

  Workaround: None.

- CSCin88118

  Symptom: PSM APS switchover may rarely occur on an ONS 15540 system due to false low alarms reported for the wdmsplit interfaces.

  Condition: This occurs rarely when spurious low alarms are seen for the PSM wdm split interfaces.

  Workaround: None.

- CSCsa45294

  Symptom: Traffic is disrupted for one to two seconds on ONS 155xx transponders configured with Forward Laser Control, when a protection switchover occurs on a trunk Protection Switch Module (PSM). This exceeds the specification of 50ms maximum failover time for the optical transport layer.

  Workaround: Disable FLC on trunk-to-client direction of transponder, if feasible for the service. This workaround does not apply for ISC, ETR or CLO services.

  Resolution: This will be fixed in the future release of IOS software on ONS15530 and ONS15540, with a caveat that the following configuration will not be supported on the platform:

  – Transponder motherboard or linecard with on-board optical splitter module (even if the optical splitter is disabled by configuration)

  – Trunk protection with Protection Switch Module

  – Forward Laser Control enabled on transponder

- CSCsa46389

  Symptom: On an ONS 15540/15530 system with Protection Switch Module, if a CPU switch occurs with the APS state such that protect interface is active and working interface is standby, then after the new CPU comes up there will be an extra APS switch to working. This is seen with all ONS15540 and ONS15530 software based on 12.1 and 12.2.

  Workaround: None.

Resolved Caveats in Release 12.2(25)SV

- CSCee71928

  Symptom: The optical link fails to come up between two 8-port GBIC modules through the ONS15540 PSM DWDMs when forward laser control (FLC) is enabled.

  Workaround: Use a 16-port GBIC module or deactivate FLC.

- CSCin76822

Symptom: If a failed subcard is replaced by a new one, the **show diag online** output continues to indicate that there was a 'previous failure' for this subcard. This should have been cleared when the new card was inserted. This is specific to subcards, for motherboards the older failures are cleared when a new card is inserted.

Workaround: None.

- CSCin80680

  Symptom: The system crashes when the functional image reprogramming is in progress for any of the line cards and the command **show upgrade-information functional-image** is issued at the same time through vty lines.

  Workaround: None.

Resolved Caveats in Release 12.2(24)SV

- CSCee75578

  Symptom: The GE optical link fails to come up between two Catalyst 65xx 8-port GBIC modules through the Cisco ONS155xx transparent transponders when Forward Laser Control (FLC) is enabled on the system. The link fails to come up irrespective of the type of protection scheme.

  Workaround: Use a 16-port GBIC module on the Catalyst 65xx or deactivate FLC on the Cisco ONS 15540.

- CSCdz82276

  Symptom: A warning is issued if the card has an unknown functional image. Version compatibility checks need to be performed during system initialization. The hardware version compatibility should identify any mismatch between functional image versions and hardware versions. The software version compatibility should identify any mismatch between the functional image and software image.

  Workaround: None.

- CSCec45305

  Symptom: If the transparent interface on a multimode transponder module is configured for Sysplex ETR traffic (**encap sysplex etr** command), the **show interfaces transparent** command output shows that forward laser control is set to off. Forward laser control is automatically enabled for Sysplex ETR.

  Workaround: Add client input traffic and the trunk side laser will function.

- CSCec55713

  Symptom: The `Prot Switch Byte Failure - In Effect` alarm message appears on the console.

  Workaround: None.

- CSCec55713

  Symptom: The `Prot Switch Byte Failure - In Effect` alarm message appears on the console.

  Workaround: None.

- CSCec78648

  Symptom: The **show redundancy** command is not valid on specific versions of the Cisco ONS 15540 ESP software but the choice still exists.

Workaround: Use the **show redundancy summary** command.

- CSCee50294

  Symptom: Cisco IOS® devices running branches of Cisco IOS version 12.2S that have Dynamic Host Configuration Protocol (DHCP) server or relay agent enabled, even if not configured, are vulnerable to a denial of service where the input queue becomes blocked when receiving specifically crafted DHCP packets. Cisco is providing free fixed software to address this issue. There are also workarounds to mitigate this vulnerability. This issue was introduced by the fix included in CSCdx46180 and is being tracked by Cisco Bug ID CSCee50294.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20041110-dhcp.shtml.

  Workaround: None.

- CSCin69960

  Symptom: A receive failure might display a message that the laser is shut due to forward laser control.

  Workaround: None.

Resolved Caveats in Release 12.2(23)SV

- CSCec31146

  Symptom: If monitoring is disabled, Loss of Light on the local transparent interface results in Loss of Sync on the far side wave interface.

  Workaround: Enable monitoring on the transparent interface.

- CSCed38657

  Symptom: DWDM links set at a 196.608-Mbps rate, or an uncommon rate close to this, may not work properly on the 2.5-Gbps transponder module. Link initialization failures and bit errors may occur.

  Workaround: None.

- CSCee34107

  Symptom: APS behavior for the **aps clear** command is inconsistent with the standard behavior if the following conditions occur:

  – Traffic runs from the working link (link A) and you perform a manual switch to the protected link (link B), causing traffic to switch to link B.

  – You enter the **aps clear** command for the aps-group; link A becomes active, regardless of whether the APS group is configured revertively or nonrevertively.

  Workaround: None.

- CSCeb70408

  Symptom: The IDPROM values from the high band single-mode SFPs are not readable. The SFPs cannot be configured and cannot be used.

  Workaround: None.

Resolved Caveats in Release 12.2(22)SV

- CSCeb18103

  Symptom: The OSC wave interface does not come back up after resolving a trunk fiber break if laser safety control was configured after the trunk fiber break occurred.

  Workaround: None.

  Resolution: Upgrade the Cisco ONS 15540 mux/demux motherboard functional image to release 2.67 or later.

- CSCin60562

  Symptom: If a row is created in cApsChanConfigTable using createAndWait, a set operation on an instance of cApsChanConfigIfIndex might modify another instance of that object.

  Workaround: Use createAndGo to create the row.

- CSCin67971

  Symptom: If a one-way patch configuration is removed between a thru interface and a wdm interface, the system hangs for a long time and eventually crashes.

  Workaround: Configure two-way patches between the thru and wdm interfaces.

Resolved Caveats in Release 12.2(18)SV2

- CSCeb87507

  Symptom: In some instances the system crashes when it attempts to parse IP SNMP related commands.

  Workaround: None.

- CSCed22589

  Symptom: Link initialization failure due to Loss of Lock might occur for ESCON traffic on some transponder modules due to a transient failure of the clock recovery unit. Only some transponder modules are susceptible to this failure and not all. This is an initialization failure and not a run-time failure.

  Workaround: None.

Resolved Caveats in Release 12.2(18)SV1

- CSCec28182

  Symptom: Tracebacks related to processor hog issues are seen when reprogramming the 2.5-Gbps transponder module functional image.

  Workaround: None.

- CSCec59409

  Symptom: Issuing a **Ctrl-U** when connected to a raw TL1 port causes the system to crash.

  Workaround: If a TL1 port is unused, apply an IP ACL to the management Ethernet interface that blocks the incoming TCP connections to that port.

Resolved Caveats for Release 12.2(18)SV

- CSCdu53656

  A Cisco device running Cisco IOS software and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP is not enabled by default, and must be configured to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

- CSCea28131

  A Cisco device running Cisco IOS software and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP is not enabled by default, and must be configured to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

- CSCeb61427

  Symptom: The system crashes when the user exits from the console after the active processor card has been removed and inserted online and is switched back to being the active processor card.

  Workaround: None.

- CSCeb72528

  Symptom: Client Tx fault alarm is asserted when an SFP optics is inserted or upon a y-cable switchover.

  Workaround: Upgrade to Cisco IOS Release 12.1(12c)EV3 and transponder functional image version 1.A2 or higher.

- CSCec05746

  Symptom: In a point-to-point network topology setup where bidirectional PSM trunk fiber protection APS is configured, and the CDL (Converged Data Link) is configured for dcc and the controller type of the mux/demux module is 0x1104 (4-channel mux/demux module without OSC), APS cannot to track a valid ethernetdcc interface. Therefore the group cannot be associated.

  Workaround: Do not configure CDL as dcc for PSM APS if the corresponding mux/demux module does not have OSC ports (controller type 0x1104).

- CSCec22377

  Symptom: Continuous optical performance monitoring alarms cause memory leaks that lead to bus error exceptions and an unexpected reload.

  Workaround: None.

- CSCec31503

  Symptom: Unable to disable APS group through SNMP. The console or Telnet session hangs indefinitely after configuration mode is entered using the SNMP **set** command.

  Workaround: Do not disable the APS group through SNMP.

- CSCec31512

Symptom: When you enter the **send break** command on the active processor and keep the active processor in the ROM monitor (ROMMON) mode for a long time, the standby processor may reload because of a bus error exception.

Workaround: None.

Limitations and Restrictions

This section provides limitations and restrictions for Cisco ONS 15540 ESP hardware and software.

Transponder Modules

This section contains limitations and restrictions that apply to transponder modules.

- When you insert the standby transponder module in a y-cable protected configuration, remove the cable from the transponder module before inserting the transponder module into the shelf. Failure to remove the cable might result in errors that can affect the performance of the active signal received by the client equipment.
- CRC errors may occur with 2-Gbps Fibre Channel on single-mode transponders when high input power levels are received from the client laser sources.

  Data errors or link-down conditions for 2-Gbps Fibre Channel might occur when used with certain client laser sources. Transmitters in some client GBIC and SFP transceiver units might send large overshoots in optical power with signal bit transitions, causing momentary overload conditions on the transponder client side receiver. The average transmitted power level from the GBIC does not violate the overload specification of the transponder client side receiver, so a power meter does not detect the overload.

  The workaround is to attenuate the signal from the client equipment to a recommended level of -12 dBm when transmitting 2-Gbps Fibre Channel services.
- Error-free transmission of some D1 video signals (defined by the SMPTE 259M standard) and test patterns (such as Matrix SDI) cannot be guaranteed by the Cisco 15500 Series because of the pathological pattern in D1 video. This well-known limitation is usually overcome by the D1 video equipment vendor, who uses a proprietary, second level of scrambling. No standards exist at this time for the second level of scrambling.

Related Documentation

Use this release notes in conjunction with the following referenced publications:

- *Regulatory Compliance and Safety Information for the Cisco ONS 15500 Series*

  Provides the regulatory compliance and safety information for the Cisco ONS 15500 Series.
- *Cisco ONS 15540 ESP Planning Guide*

  Provides detailed information on the Cisco ONS 15540 ESP architecture and functionality.
- *Cisco ONS 15540 ESP Hardware Installation Guide*

  Provides detailed information about installing the Cisco ONS 15540 ESP.
- *Cisco ONS 15540 ESP Optical Transport Turn-Up and Test Guide*

  Provides acceptance testing procedures for Cisco ONS 15540 ESP nodes and networks.

- *Cisco ONS 15540 ESP Cleaning Procedures for Fiber Optic Connections*

  Provides processes and procedures for cleaning the fiber optic connectors and component interfaces of the Cisco ONS 15540 ESP.
- *Cisco ONS 15540 ESP Command Reference*

  Provides commands to configure and manage the Cisco ONS 15540 ESP.
- *Cisco ONS 15540 ESP System Alarms and Error Messages*

  Describes the system alarms and error messages for the Cisco ONS 15540 ESP.
- *Cisco ONS 15540 ESP Troubleshooting Guide*

  Describes how to identify and resolve problems with the Cisco ONS 15540 ESP.
- *Network Management for the Cisco ONS 15540 ESP*

  Provides information on the network management systems that support the Cisco ONS 15540 ESP.
- *Cisco ONS 15540 ESP TL1 Commands*

  Provides a full TL1 command and autonomous message set including parameters, AIDs, conditions and modifiers for the Cisco ONS 15540 ESP.
- *MIB Quick Reference for the Cisco ONS 15500 Series*

  Describes the Management Information Base (MIB) objects and explains how to access Cisco public MIBs for the Cisco ONS 15500 Series.
- *Cisco ONS 15540 ESP Software Upgrade Guide*

  Describes how to upgrade system images and functional images on the Cisco ONS 15540 ESP.

Document Conventions

This publication uses the following conventions:

Convention	Application
boldface	Commands and keywords in body text.
italic	Command input that is supplied by the user.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x | x | x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. The user must select one.
Ctrl	The control key. For example, where Ctrl + D is written, hold down the Control key while pressing the D key.
`screen font`	Examples of information displayed on the screen.
`boldface screen font`	Examples of information that the user must enter.
< >	Command parameters that must be replaced by module-specific codes.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Caution Means *reader be careful*. In this situation, the user might do something that could result in equipment damage or loss of data.

Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Where to Find Safety and Warning Information

For safety and warning information, refer to the *Cisco Optical Transport Products Safety and Compliance Information* document that accompanied the product. This publication describes the international agency compliance and safety information for the Cisco ONS 15xxx systems. It also includes translations of the safety warnings that appear in the ONS 15xxx system documentation.

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://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

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