Release Notes for Cisco ONS 15540 ESP for Cisco IOS Release 12.2(24)SV1

This document describes caveats for Cisco IOS Release 12.2(24)SV1 for the Cisco ONS 15540 ESP (Extended Services Platform).

Date: July 29, 2005

Text Part Number OL-4892-06 E0

Contents

This document includes the following information:

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

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

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
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

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

Component	Part Number	Description	Minimum Software Version Required
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
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

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

Component	Part Number	Description	Minimum Software Version Required
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
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

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

Component	Part Number	Description	Minimum Software Version Required
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
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(24)SV
<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

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

Feature Set	Introduced in This Release
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
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

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(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.

Resolved Caveats in Release 12.2(24)SV1

- CSCef68324

  Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml.

Open Caveats in Release 12.2(24)SV

- CSCeb79990

  Symptom: The **patch** commands saved on the system are not compatible with CTM (Cisco Transport Manager).

  Workaround: Remove the **patch** commands that show up out of order after the configuration is saved. Then reset the active processor card or switch to the standby processor card and reenter the **patch** commands.

- CSCed74239

  Symptom: In a point-to-point network with y-cable based APS configured, the protection path does not automatically come up if the working path is down.

  Workaround: Put a loopback on the client side to restore traffic to the protection path.

  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 turned on. Interface alarm flapping may cause hardware watchdog timeout, failed to switchover to standby processor card.

  Workaround: None

- 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.

Resolved Caveats in Release 12.2(24)SV

- 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 15530 software but the choice still exists.

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

- CSCed65285

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)

  This advisory will be posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml.

- CSCed65778

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)

  This advisory will be posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml.

- CSCed78149

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- 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.

- 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 ONS155xx.

- CSCin69960

  Symptom: A receive failure might display a message that the laser if 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

Refer to the following documents for more information about the Cisco ONS 15540 ESP:

- *Regulatory Compliance and Safety Information for the Cisco ONS 15500 Series*
- *Cisco ONS 15540 ESP Planning Guide*
- *Cisco ONS 15540 ESP Hardware Installation Guide*
- *Cisco ONS 15540 ESP Optical Transport Turn-Up and Test Guide*
- *Cisco ONS 15540 ESP Configuration Guide*
- *Cisco ONS 15540 ESP Command Reference*
- *Cisco ONS 15540 ESP System Alarms and Error Messages*
- *Cisco ONS 15540 ESP Troubleshooting Guide*
- *Network Management for the Cisco ONS 15540 ESP*
- *Cisco ONS 15540 ESP TL1 Command Reference*
- *MIB Quick Reference for the Cisco ONS 15500 Series*
- *Cisco ONS 15540 ESP Software Upgrade Guide*

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 on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

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

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

You can submit comments 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

http://www.cisco.com/tac

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

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

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your 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.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation 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.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—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.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:

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

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *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 online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- *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

- Training—Cisco offers world-class networking training. Current offerings in network training are listed 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.