Release Notes for Cisco ONS 15540 ESP for Cisco IOS Release 12.1(12c)EV2

This document describes caveats for Cisco IOS Release 12.1(12c)EV2 for the Cisco ONS 15540 ESP (Extended Services Platform).

Date: June 16, 2004

Text Part Number: OL-3341-05

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 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 and Design Guide*.

CISCO SYSTEMS

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

System Requirements

This section describes the system requirements for Cisco IOS Release 12.1(12c)EV 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 7.

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
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

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

Component	Part Number	Description	Minimum Software Version Required
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
Mux/demux modules with OSC	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
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
Pluggable transceivers for extended range transponder modules	15500-XVRA-01A2	ESCON and OC-3 1310-nm MM MT-RJ	12.1(11b)E
	15500-XVRA-01A2	ESCON/SONET OC-3/SDH STM-1 transceiver - 1310-nm MTRJ	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 (2 Gbps) 850-nm MM MTLC	12.1(11b)E
	15500-XVRA-02C3	Fibre Channel (2 Gbps) 1310-nm SM MTLC	12.1(11b)E
	15500-XVRA-07B1	SONET OC-12 1310-nm SM MTLC	12.1(11b)E
	1550-XVRA-06B1	SONET OC-12 1310-nm MTLC	12.1(11b)E
	15500-XVRA-07B1	SONET OC-48 1310-nm SM MTLC	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
Single port 10-Gigabit Ethernet transponder	15540-10GE-03B301	10-GE 1310nm SM client with SC and ITU laser Ch 1	12.1(10)EV2
	15540-10GE-03B302	10-GE 1310nm SM client with SC and ITU laser Ch 2	12.1(10)EV2
	15540-10GE-03B303	10-GE 1310nm SM client with SC and ITU laser Ch 3	12.1(10)EV2
	15540-10GE-03B304	10-GE 1310nm SM client with SC and ITU laser Ch 4	12.1(10)EV2
	15540-10GE-03B305	10-GE 1310nm SM client with SC and ITU laser Ch 5	12.1(10)EV2
	15540-10GE-03B306	10-GE 1310nm SM client with SC and ITU laser Ch 6	12.1(10)EV2
	15540-10GE-03B307	10-GE 1310nm SM client with SC and ITU laser Ch 7	12.1(10)EV2
	15540-10GE-03B308	10-GE 1310nm SM client with SC and ITU laser Ch8	12.1(10)EV2
	15540-10GE-03B309	10-GE 1310nm SM client with SC and ITU laser Ch 9	12.1(10)EV2
	15540-10GE-03B3010	10-GE 1310nm SM client with SC and ITU laser Ch 10	12.1(10)EV2
	15540-10GE-03B3011	10-GE 1310nm SM client with SC and ITU laser Ch 11	12.1(10)EV2
	15540-10GE-03B3012	10-GE 1310nm SM client with SC and ITU laser Ch 12	12.1(10)EV2
	15540-10GE-03B3013	10-GE 1310nm SM client with SC and ITU laser Ch 13	12.1(10)EV2
	15540-10GE-03B3014	10-GE 1310nm SM client with SC and ITU laser Ch 14	12.1(10)EV2
	15540-10GE-03B3015	10-GE 1310nm SM client with SC and ITU laser Ch 15	12.1(10)EV2
	15540-10GE-03B3016	10-GE 1310nm SM client with SC and ITU laser Ch 16	12.1(10)EV2
	15540-10GE-03B3017	10-GE 1310nm SM client with SC and ITU laser Ch 17	12.1(10)EV2
	15540-10GE-03B3018	10-GE 1310nm SM client with SC and ITU laser Ch 18	12.1(10)EV2
	15540-10GE-03B3019	10-GE 1310nm SM client with SC and ITU laser Ch 19	12.1(10)EV2
	15540-10GE-03B3020	10-GE 1310nm SM client with SC and ITU laser Ch 20	12.1(10)EV2
	15540-10GE-03B3021	10-GE 1310nm SM client with SC and ITU laser Ch 21	12.1(10)EV2
	15540-10GE-03B3022	10-GE 1310nm SM client with SC and ITU laser Ch 22	12.1(10)EV2
	15540-10GE-03B3023	10-GE 1310nm SM client with SC and ITU laser Ch 23	12.1(10)EV2
	15540-10GE-03B3024	10-GE 1310nm SM client with SC and ITU laser Ch 24	12.1(10)EV2
	15540-10GE-03B3025	10-GE 1310nm SM client with SC and ITU laser Ch 25	12.1(10)EV2
	15540-10GE-03B3026	10-GE 1310nm SM client with SC and ITU laser Ch 26	12.1(10)EV2
	15540-10GE-03B3027	10-GE 1310nm SM client with SC and ITU laser Ch 27	12.1(10)EV2
	15540-10GE-03B3028	10-GE 1310nm SM client with SC and ITU laser Ch 28	12.1(10)EV2
	15540-10GE-03B3029	10-GE 1310nm SM client with SC and ITU laser Ch 29	12.1(10)EV2
	15540-10GE-03B3030	10-GE 1310nm SM client with SC and ITU laser Ch 30	12.1(10)EV2
	15540-10GE-03B3031	10-GE 1310nm SM client with SC and ITU laser Ch 31	12.1(10)EV2
	15540-10GE-03B3032	10-GE 1310nm SM client with SC and ITU laser Ch 32	12.1(10)EV2

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 12.1(12c)EV
<Information deleted>
```

Upgrading the System Image

To ensure proper system functioning, follow the system image upgrading procedure described in the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

> **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	12.1(12c)EV2	12.1(12c)EV1	12.1(12c)EV	12.1(10)EV2 & 12.1(10)EV1	12.1(12c)E & 12.1(12c)E1	12.1(11b)E & 12.1(11b)E1	12.1(7a)EY2 & 12.1(7a)EY3
Gigabit Ethernet	X	X	X	X	X	X	X
Fast Ethernet	X	X	X	X	X	X	X
Ethernet	X	X	X	X	X	X	X
ATM OC-3/STM-1, OC-12/STM-4, and OC-48/STM-16	X	X	X	X	X	X	X

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

Feature Set	12.1(12c)EV2	12.1(12c)EV1	12.1(12c)EV	12.1(10)EV2 & 12.1(10)EV1	12.1(12c)E & 12.1(12c)E1	12.1(11b)E & 12.1(11b)E1	12.1(7a)EY2 & 12.1(7a)EY3
SONET[1]/SDH[2]	X	X	X	X	X	X	X
POS[3]	X	X	X	X	X	X	X
Coupling link	X	X	X	X	X	X	X
Fibre Channel (1 Gbps)	X	X	X	X	X	X	X
Fibre Channel (2 Gbps)	X	X	X	X	X	X	X
FDDI[4]	X	X	X	X	X	X	X
ESCON[5] SM (200 Mbps)	X	X	X	X	X	X	X
FICON[6] (800 Mbps)	X	X	X	X	X	X	X
Token Ring	X	X	X	X	X	X	X
SNMP	X	X	X	X	X	X	X
CiscoView	X	X	X	X	X	X	X
Cisco Transport Manager	X	X	X	X	X	X	X
IP packets	X	X	X	X	X	X	X
OSCP[7]	X	X	X	X	X	X	X
APS[8] protocol packets	X	X	X	X	X	X	X
Point-to-point	X	X	X	X	X	X	X
Hubbed ring	X	X	X	X	X	X	X
Meshed ring	X	X	X	X	X	X	X
IBM GDPS[9] ETR/CL[10]	X	X	X	X	X	X	X
IBM GDPS[9] coupling link	X	X	X	X	X	X	X
CDL over 10 GE	X	X	X	X			

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 12.1. The new features are sorted by release number.

New Features in Release 12.1(12c)EV2

The following new feature is available for the Cisco ONS 15540 ESP in Cisco IOS Release 12.1(12c)EV2:

- **show optical interface brief** command

New Features in Release 12.1(12c)EV1

The following new feature is available for the Cisco ONS 15540 ESP in Cisco IOS Release 12.1(12c)EV1:

- Supports TL1 commands

New Features in Release 12.1(12c)EV

No new features are available for the Cisco ONS 15540 ESP in Cisco IOS Release 12.1(12c)EV.

New Features in Release 12.1(10)EV3

No new features are available for the Cisco ONS 15540 ESP in Cisco IOS Release 12.1(10)EV3.

New Features in Release 12.1(10)EV2

The following new features are available for the Cisco ONS 15540 ESP in Cisco IOS Release 12.1(10)EV2:

- Hardware:
  - Unprotected dual subslot motherboard for Cisco ONS 15540 ESP
  - 10-GE transponder module
  - ITU direct insertion module
- Software:
  - CDL over 10 GE

New Features in Release 12.1(12c)E1

No new features are available for the Cisco ONS 15540 ESP in Cisco IOS Release 12.1(12c)E1.

New Features in Release 12.1(12c)E

No new features are available for the Cisco ONS 15540 ESP in Cisco IOS Release 12.1(12c)E.

New Features in Release 12.1(11b)E1

No new features are available for the Cisco ONS 15540 ESP in Cisco IOS Release 12.1(11b)E1.

New Features in Release 12.1(11b)E

The following new features are available for the Cisco ONS 15540 ESP in Cisco IOS Release 12.1(11b)E:

- Extended range transponder modules supporting the following transceivers:
    - ESCON and SONET OC-3 MM (1310 nm)
    - Gigabit Ethernet and Fibre Channel (1 Gbps) MM (850 nm)
    - Gigabit Ethernet and Fibre Channel (1 Gbps) SM (1310 nm)
    - Fibre Channel (2 Gbps) MM (850 nm)
    - Fibre Channel (2 Gbps) SM (1310 nm)
    - SONET OC-12 SM (1310 nm)
    - SONET OC-48 SM (1310 nm)

New Features in Release 12.1(7a)EY3

The following new software features are available for the Cisco ONS 15540 ESP in Cisco IOS Release 12.1(7a)EY3:

- Cisco IOS software on the processor.

- Autoconfiguration at startup.

- Autodiscovery of network neighbors.

- Online diagnostics.

- Processor redundancy provided by arbitrations of processor status and switchover in case of failure without loss of connections.

- Autosynchronization of startup and running configurations.

- Support for in-service software upgrades.

- Support for per-channel APS (Automatic Protection Switching) in point-to-point and ring topologies using redundant subsystems that monitor link integrity and signal quality.

- Unidirectional and bidirectional 1+1 path switching.

- System configuration and management through the CLI (command-line interface), accessible through an Ethernet connection or console terminal.

- Optical power monitoring on the transport side, digital monitoring on both client and transport side, and per-channel transponder in-service and out-of-service loopback (client and transport sides).

- Optional out-of-band management of other Cisco ONS 15540 ESP systems on the network through the OSC (optical supervisory channel).

- Support for network management systems that use SNMP. Its capabilities include configuration management, fault isolation, topology discovery, and path trace.

New Features in Release 12.1(7a)EY2

The following new features are available for the Cisco ONS 15540 ESP in Cisco IOS Release 12.1(7a)EY2:

- Cisco IOS software on the processor.

- Autoconfiguration at startup.

- Autodiscovery of network neighbors.

- Online diagnostics.

- Processor redundancy provided by arbitrations of processor status and switchover in case of failure without loss of connections.

- Autosynchronization of startup and running configurations.

- Support for in-service software upgrades.

- Support for per-channel APS (Automatic Protection Switching) in point-to-point and ring topologies using redundant subsystems that monitor link integrity and signal quality.

- Unidirectional and bidirectional 1+1 path switching.

- System configuration and management through the CLI (command-line interface), accessible through an Ethernet connection or console terminal.

- Optical power monitoring on the transport side, digital monitoring on both client and transport side, and per-channel transponder in-service and out-of-service loopback (client and transport sides).

- Optional out-of-band management of other Cisco ONS 15540 ESP systems on the network through the OSC (optical supervisory channel).

- Support for network management systems that use SNMP. Its capabilities include configuration management, fault isolation, topology discovery, and path trace.

Caveats

This section lists the caveats and corrected caveats for each release. Use Table 3 and Table 4 to determine the status of a particular caveat. In the tables, "C" indicates a corrected caveat, and "O" indicates an open caveat.

Table 3   Caveat Matrix for the Cisco ONS 15540 ESP

DDTS Number	12.1(12c)EV2	12.1(12c)EV1	12.1(12c)EV	12.1(10)EV3
CSCdu53656	C	O	O	O
CSCdv33165	C	C	C	O
CSCdv37024	C	C	C	C
CSCdv90351	O	O	O	O

Table 3   Caveat Matrix for the Cisco ONS 15540 ESP (continued)

DDTS Number	12.1(12c)EV2	12.1(12c)EV1	12.1(12c)EV	12.1(10)EV3
CSCdw26675	C	C	C	C
CSCdw32072	C	C	C	C
CSCdw49750	C	C	C	C
CSCdw65903	C	C	C	C
CSCdw66715	C	C	C	C
CSCdw71880	C	C	C	C
CSCdw80987	C	C	C	C
CSCdw82701	C	C	C	C
CSCdw87421	C	C	C	C
CSCdx07666	C	C	C	O
CSCdx09167	C	C	C	C
CSCdx27201	C	C	C	C
CSCdx31068	C	C	C	C
CSCdx32408	C	C	C	C
CSCdx32438	C	C	C	C
CSCdx37144	C	C	C	C
CSCdx42595	C	C	C	C
CSCdx70683	O	O	O	O
CSCdx77331	C	C	C	C
CSCdx80804	C	C	C	C
CSCdx81765	C	C	C	C
CSCdx82558	C	C	C	C
CSCdx85761	C	C	C	C
CSCdy03245	C	C	C	C
CSCdy08228	C	C	C	C
CSCdy10401	C	C	C	C
CSCdy20002	C	C	C	C
CSCdy20010	C	C	C	C
CSCdy20022	C	C	C	C
CSCdy20792	C	C	C	C
CSCdy23001	C	C	C	C
CSCdy23025	C	C	C	C
CSCdy23325	C	C	C	C
CSCdy30497	C	C	C	C
CSCdy40429	C	C	C	C
CSCdy40864	C	C	C	C

Table 3   Caveat Matrix for the Cisco ONS 15540 ESP (continued)

DDTS Number	12.1(12c)EV2	12.1(12c)EV1	12.1(12c)EV	12.1(10)EV3
CSCdy40882	C	C	C	C
CSCdy44129	O	O	O	O
CSCdy49146	C	C	C	C
CSCdy49249	C	C	C	C
CSCdy53288	C	C	C	C
CSCdy58197	C	C	C	O
CSCdy61641	C	C	C	C
CSCdy62752	C	C	C	C
CSCdy63359	C	C	C	C
CSCdy65411	C	C	C	C
CSCdy78546	C	C	C	C
CSCdy79161	C	C	C	C
CSCdy79659	C	C	C	C
CSCdy79812	C	C	C	C
CSCdy81888	C	C	C	C
CSCdy83757	C	C	C	C
CSCdy85563	C	C	C	C
CSCdy87237	C	C	C	C
CSCdy88154	C	C	C	C
CSCdz00116	C	C	C	C
CSCdz02296	C	C	C	C
CSCdz02340	C	C	C	C
CSCdz03989	C	C	C	C
CSCdz06004	C	C	C	C
CSCdz06602	C	C	C	C
CSCdz08774	C	C	C	C
CSCdz12919	C	C	C	C
CSCdz13538	C	C	C	C
CSCdz13673	C	C	C	C
CSCdz14420	C	C	C	C
CSCdz18757	C	C	C	C
CSCdz18815	C	C	C	C
CSCdz19099	C	C	C	C
CSCdz20508	C	C	C	C
CSCdz22455	C	C	C	C
CSCdz25739	C	C	C	O

Table 3   Caveat Matrix for the Cisco ONS 15540 ESP (continued)

DDTS Number	12.1(12c)EV2	12.1(12c)EV1	12.1(12c)EV	12.1(10)EV3
CSCdz28582	C	C	C	C
CSCdz28903	C	C	C	C
CSCdz29723	O	O	O	O
CSCdz31593	O	O	O	O
CSCdz33752	C	C	C	C
CSCdz36420	C	C	C	C
CSCdz36424	C	C	C	O
CSCdz36823	C	C	C	C
CSCdz37698	C	C	C	C
CSCdz37968	C	C	C	C
CSCdz38075	C	C	C	C
CSCdz38448	C	C	C	O
CSCdz38968	C	C	C	C
CSCdz39112	C	C	C	O
CSCdz39793	C	C	C	O
CSCdz40675	C	C	C	
CSCdz41160	C	C	C	O
CSCdz42547	C	C	C	O
CSCdz42565	C	C	C	O
CSCdz43279	C	C	C	O
CSCdz56523	C			
CSCdz58866	C	C	C	O
CSCdz60081	C	C		
CSCdz62553	C	C	C	
CSCdz66609	O	O	O	O
CSCdz75109	C	C	C	
CSCdz76974	C	C		
CSCdz77034	C	C		
CSCdz79336	O	O	O	
CSCdz80042	O	O	O	
CSCdz83169	C	C	O	
CSCdz85458	O	O	O	
CSCea04546	C	C		
CSCea03957	C	C		
CSCea16511	C			
CSCea28131	C			

Table 3   Caveat Matrix for the Cisco ONS 15540 ESP (continued)

DDTS Number	12.1(12c)EV2	12.1(12c)EV1	12.1(12c)EV	12.1(10)EV3
CSCea41710	C	C		
CSCea60957	C	O		
CSCea92296	C	O	O	O
CSCeb20229	O			
CSCeb31264	O			
CSCeb37281	O			
CSCeb54866	O			
CSCeb55150	O			

Table 4   Caveat Matrix for the Cisco ONS 15540 ESP

DDTS Number	12.1(10)EV2	12.1(10)EV1	12.1(13)E1	12.1(12c)E3	12.1(12c)E1	12.1(11b)E1	12.1(7a)EY3	12.1(7a)EY2
CSCdv33165	O	O	O	O	O	O	O	O
CSCdv37024	C	C	C	C	C	C	O	O
CSCdv90351	O	O	O	O	O	O	O	O
CSCdw26675	C	C	C	C	C	C	O	O
CSCdw32072	C	C	C	C	C	C	O	O
CSCdw49750	C	C	C	C	C	C	O	O
CSCdw65903	C	C	C	C	C	C	C	
CSCdw66715	C	C	C	C	C	C	O	O
CSCdw71880	C	C	C	C	C	C	O	O
CSCdw80987	C	C	C	C	C	C		
CSCdw82701	C	C	C	C	C	O		
CSCdw87421	C	C	C	C	C	O		
CSCdx07666	O	O	O	O	O			
CSCdx09167	C	C	C	C	C	O		
CSCdx27201	C	C	C	C	C	C		
CSCdx31068	C	C	C	C	C	O		
CSCdx32408	C	C	C	C	C	O		
CSCdx32438	C							
CSCdx37144	C							
CSCdx42595	C	C						
CSCdx70683	O	O	O	O	O			
CSCdx77331	C	C	C	C	C	O		
CSCdx80804	C	C	C	C	C	O		
CSCdx81765	C	C	C	C	C	O		

Release Notes for Cisco ONS 15540 ESP for Cisco IOS Release 12.1(12c)EV2 ■

Table 4   Caveat Matrix for the Cisco ONS 15540 ESP (continued)

DDTS Number	12.1(10)EV2	12.1(10)EV1	12.1(13)E1	12.1(12c)E3	12.1(12c)E1	12.1(11b)E1	12.1(7a)EY3	12.1(7a)EY2
CSCdx82558	C	C	C	C	C	O		
CSCdy10401	C	O	C	O	O			
CSCdy20002	O	O	O	O	O			
CSCdy20010	O	O	O	O	O			
CSCdy23001	O	O	O	C	O			
CSCdy23025	O	O	O	O	O			
CSCdy23325	O	O	O	O	O			
CSCdy40429	C	C	C	C				
CSCdy40864	O	O						
CSCdy40882	O	O						
CSCdy44129	O	O						
CSCdy49146	C	C	C	C				
CSCdy49249	O	O						
CSCdy53288	O	O						
CSCdy58197	O	O						
CSCdy61641	O	O						
CSCdy62752	O	O						
CSCdy63359	O	O						
CSCdy65411	O	O						
CSCdy78546	O	O						
CSCdy79161	O	O						
CSCdy79659	O	O						
CSCdy79812	O	O						
CSCdy81888	O	O						
CSCdy83757	O	O						
CSCdy85563	O	O						
CSCdy87237	O	O						
CSCdy88154	O	O						
CSCdz00116	O	O						
CSCdz02296	O	O						
CSCdz02340	O	O						
CSCdz03989	O	O						
CSCdz06004	O	O						
CSCdz06602	O	O						
CSCdz08774	O	O						
CSCdz12919	O	O						

Table 4   Caveat Matrix for the Cisco ONS 15540 ESP (continued)

DDTS Number	12.1(10)EV2	12.1(10)EV1	12.1(13)E1	12.1(12c)E3	12.1(12c)E1	12.1(11b)E1	12.1(7a)EY3	12.1(7a)EY2
CSCdz13538	O	O						
CSCdz13673	O	O						
CSCdz14420	O	O						
CSCdz18757	O	O						
CSCdz18815	O	O						
CSCdz19099	O	O						
CSCdz20508	O	O						
CSCdz22455	O	O						
CSCdz28582	O	O						
CSCdz33752	O	O						
CSCdz36420	O	O						
CSCdz36823	O	O						
CSCdz37698	O	O						
CSCdz38075	O	O						

This section describes the caveats in the Cisco ONS 15540 ESP.

- CSCdu53656

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order 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, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

- CSCdv33165

  Symptom: If you attempt to change or edit a threshold in the threshold list that is already associated with an interface, the threshold is applied to that interface even when no changes are made to it.

  Workaround: Issue the **clear counters** command.

- CSCdv37024

  Symptom: If CiscoView files are extracted on a Flash disk (disk0: or disk1:), the package does not work.

  Workaround: Install CiscoView on a Flash PC Card (slot0: or slot1:).

- CSCdv90351

  Symptom: When there is a constant stream of loss of sync alarms, a port fail notification is not generated.

Although both signal failure and signal degrade thresholds are applied, only signal degrade is observed. The signal failure threshold is monitored by hardware registers. When the signal failure threshold is exceeded, the hardware normally generates a port fail notification. Because the loss of sync alarms are constant, the threshold exceeded cannot generate a port fail notification. The signal degrade is reported because it is monitored by software and does not need any notifications from hardware.

Workaround: Disable and reenable monitoring once with the **no monitor/monitor enable** command sequence to generate the port fail notification.

- CSCdw26675

  Symptom: Upon switchover, the active processor card might become nonresponsive. The processor card Active LED remains on, even though it is no longer actively controlling the system.

  Workaround: OIR the processor card to correct the fault.

- CSCdw32072

  Symptom: The ROM monitor might continuously loop in an attempt to autoboot a missing system image.

  Continuous looping happens when autoboot is configured in the configuration register (0x2102), but the system image corresponding to the **system boot** *filename* command in the startup configuration is missing and no alternate **system boot** *filename* command is configured for an existing system image.

  During normal system functioning, the system first checks for system image file names in the startup configuration **system boot** *filename* commands. If there are none, or the images are not valid, the system checks the Flash device in slot0: and then bootflash for loadable images before stopping its attempts to autoboot.

  Workaround: Configure at least one **system boot** *filename* command for an existing system image on both processor cards before reloading either processor card.

  If autoboot looping occurs, issue a console **send break** command during the first few seconds of a reload attempt to stop autobooting. Then manually boot the system using a valid system image in Flash memory or on the network.

  Upgrade the processor card ROMMON image to release 12.1(11r)E3 or later.

- CSCdw49750

  Symptom: If during a netboot attempt the processor card fails to netboot or the peer processor card changes its active/standby state, any further changes to the peer processor card Active/Standby state are ignored until a **reset** command is issued at the processor card ROMMON prompt.

  Workaround: Issue a **reset** command at the ROMMON prompt after failing to netboot.

  Upgrade the processor card ROMMON image to Release 12.1(11r)E3 or later.

- CSCdw65903

  Symptom: An error can occur with management protocol processing. See the following URL for more information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

  Workaround: None

- CSCdw66715

  Symptom: Following a Cisco IOS software crash, a second ROMMON exception might cause the original stack trace to be lost. This happens if a pending PCI (peripheral component interconnect) bus interrupt was in progress but was not handled before the IOS crash.

  Workaround: Upgrade the processor card ROMMON image to Release 12.1(11r)E3 or later.

- CSCdw71880

  Symptom: The following errors might occur:

  - The 100 Mbps LED for the NME (Network Management Ethernet) port might be on even if the port is connected to an 10 Mbps source. This LED should be on only when connected to a 100 Mbps source.

  - The full duplex LED might not stay on even when the port is connected to a full duplex source.

  - Autonegotiation of speed and duplex mode might not work when switched from a 10 Mbps source to 100 Mbps source.

  - Autonegotiation of speed and duplex mode might not work when switched from a 100 Mbps source to a 10 Mbps source.

  Workaround: None.

- CSCdw80987

  Symptom: The system power cycles and the standby processor card startup configuration is not synchronized with the active processor card startup configuration. If this occurs, then the previous standby processor card might become the active processor card and a different set of connections might be set up.

  The standby processor card startup configuration can become outdated when it is in maintenance mode.

  Workaround: Remove the standby processor card from the shelf when it is not in use.

  Upgrade the processor card ROMMON image to Release 12.1(11r)E3 or later.

- CSCdw82701

  Symptom: Loopback cannot be configured on the wave interface of an extended range transponder module if no transceiver is present. The **loopback** command is accepted but the loopback is not configured.

  Workaround: Insert a transceiver before configuring the loopback on the wave interface.

- CSCdw87421

  Symptom: When laser safety control is enabled on the OSC wave 0 interface or wave 1 interface, the OSC trunk laser does not shut down when a fiber cut occurs.

  Workaround: None

- CSCdx07666

  Symptom: Loss of signal may be encountered before SD (signal degrade) and SF (signal failure) thresholds are exceeded and traffic may still continue to pass transparently.

  The loss of signal detection is taken from the OE conversion subsystem, which is different from the source of the SD and SF counters. The OE conversion is not gated by its loss of light indication so the data and clock extraction continues and the signal is regenerated transparently. The loss of light sensitivity is a characteristic of the OE conversion unit and it may vary from unit to unit but is always < –30 dBm.

  Workaround: None.

- CSCdx09167

  Symptom: The alarm LED is not raised or cleared by SD/SF indications.

  Workaround: None.

- CSCdx27201

Symptom: If the configuration register autoboot field is set to either 0x1 or 0x2 and the first file in bootflash memory is not a loadable system image, then the system continues to try to reboot.

Workaround: Use the **send break** command on the console CLI to stop the autoboot cycling, and then manually boot a loadable system image. Make sure the first image in bootflash memory is a valid system image.

Upgrade the processor card ROMMON image to Release 12.1(11r)E3 or later.

- CSCdx31068

   Symptom: With APS y-cable protection, SD condition on the working channel does not clear the lower priority manual-switch condition on the protection channel. This causes the manual switch to persist after the SD condition was removed and APS to switch back to the working channel.

   Workaround: None.

- CSCdx32408

   Symptom: No alarm is raised when the customer installed 2.5-Gbps transponder module channel does not match the channels supported by the transponder module.

   Workaround: None.

- CSCdx32438

   Symptom: When the Rx port fiber is removed, ingress alarms are reported and cleared repeatedly. The alarm should not clear and the alarm should be reported only once.

   Workaround: None.

- CSCdx37144

   Symptom: Processor card gets into a nonresponsive state.

   Workaround: None.

- CSCdx42595

   Symptom: No alarm is raised when the 2.5-Gbps transponder module channel does not match the channels supported by the mux/demux module.

   Workaround: None.

- CSCdx70683

   Symptom: The reprogram for the standby processor card fails.

   Workaround: Run the reprogram on the active processor card, enable the processor switchover after switchover, and then run the reprogram on the new active processor card. Remove and reinsert the processor card for the new FPGA to become effective.

- CSCdx77331

   Symptom: CTM is flooded with traps every second when hardware port flap alarms occur.

   Workaround: None.

- CSCdx80804

   Symptom: The **encapsulation fastethernet** command fails on multimode transponder modules. The **clock rate 100000** command succeeds but pings over the signal fail intermittently.

   Workaround: None.

- CSCdx81765

   Symptom: The OSC intermittently drops IP packets because of an erroneous calculation of the FCS-16 (frame check sequence 16).

Workaround: None.

- CSCdx82558

  Symptom: The system image on the standby processor card cannot be upgraded to a new system image because the format of the redundancy messages from the active processor card are not recognized on the standby processor card. The standby processor card fails to boot and returns to ROMMON mode.

  Workaround: None.

- CSCdx85761

  Symptom: Multiple %METOPT-2-PORTFAIL messages are seen when using the y-cable APS configuration with single AFOV. However, this does not affect the functionality.

  Workaround: None.

- CSCdy03245

  Symptom: Topology neighbor configuration is lost on mux/demux motherboard OIR.

  Workaround: The topology neighbor is viewable after reconfiguring the wdm interface.

- CSCdy08228

  Symptom: Interface reports up/up even when there is no light source connected.

  Workaround: Issue a **shutdown/no shutdown** command on the interface.

- CSCdy10401

  Symptom: The transparent interface of an extended range transponder module continues to report good signal quality even after the transceiver is removed and reinserted.

  Workaround: Issue a **shutdown**/**no shutdown** command sequence on the transparent interface.

- CSCdy20002

  Symptom: A transparent interface carrying Gigabit Ethernet traffic and configured with 1-Gbps Fibre Channel encapsulation shows good quality signal on the **show interfaces transparent** command output and does not assert any ingress alarms. The wave interface assert loss of lock and loss of sync alarms.

  Workaround: Remove and reinsert the 2.5-Gbps transponder module to bring it to the correct state.

- CSCdy20010

  Symptom: LOF (loss of frame) alarms are not reasserted after a **shutdown**/**no shutdown** command sequence on both the transparent and wave interfaces on the 2.5-Gbps transponder module.

  Workaround: Disable and reenable monitoring on the transparent interface to reassert the alarms.

- CSCdy20022

  Symptom: The **show facility-alarm status** command output does not report existing LoF/LoSync/LoLock alarms after OIR/hw-mod power off/on.

  Workaround: Disable and enable monitoring will reassert existing alarms in the **show facility-alarm status**.

- CSCdy20792

  Symptom: After removing and reinserting (OIR) of a 2.5-Gbps transponder module, the laser frequency is not programmed to the 2.5-Gbps transponder module correctly, resulting in a wavelength filter mismatch and the wavelength not coming out of the filter.

  Workaround: Configure the wave interface for the alternate frequency and then program it back to the desired frequency using the **laser frequency** command.

- CSCdy23001

  Symptom: A line laser failure alarm is asserted but not cleared when an extended range transponder module is removed and reinserted. The **show facility-alarm status** command output shows a message similar to the following:

  ```
  Source: TranspdrSC 2/3  Severity: MAJOR Description: 2    Line laser failure detected
  ```

  Workaround: None.

- CSCdy23025

  Symptom: The SF (signal failure) alarms are not cleared from the **show facility-alarm status** command output after monitoring is disabled.

  Workaround: None.

- CSCdy23325

  Symptom: An ingress LOF alarm on a transparent interface is not asserted when an SEF (severely errored frames) alarm is present due to the alarm priority handling error in the driver.

  Workaround: A **shutdown**/**no shutdown** command sequence on the transparent interface reasserts the ingress LOF alarm.

- CSCdy30497

  Symptom: The line card motherboard functional image version in the **show hardware** command output should return the hexadecimal value.

  Workaround: None.

- CSCdy40429

  Symptom: Under some situations the erratas of the system controller used on the processor card (GT64120A) can cause the following conditions:

  – Software forced crash due to memory ECC errors

  – Bus error exception

  – Corruption of data

  Workaround: None.

- CSCdy40864

  Symptom: The active processor card resets the standby processor card because of a compatibility problem detected in the system images.

  Workaround: None.

- CSCdy40882

  Symptom: Information appears in **show hardware** command output for processor cards that have been removed.

  Workaround: None.

- CSCdy44129

  Symptom: If a client interface is configured for CDL but is connected to a non-CDL device, the CDL message channel is down.

  Workaround: Ensure that the client interface is configured correctly.

- CSCdy49146

  Symptom: Under some circumstances, single bit ECC errors occur and are corrected by the system controller, but are not recorded; the user is unaware of these occurrences.

Workaround: None.

- CSCdy49249

  Symptom: If a module is inserted during a processor card switchover, then the module and its interfaces might not come up properly.

  Workaround: Remove and reinsert module after switchover is complete.

- CSCdy53288

  Symptom: The system might crash when using the **is_optical_ifstatus_up** command; this is an intermittent problem.

  Workaround: None.

- CSCdy58197

  Symptom: In a configuration where two Cisco ONS 15530 systems are linked to a Cisco ONS 15540 ESP through 10-GE connections, the tengigethernetphy interface on one side is administratively shut down and the ESCON ports are shut down. However, the ESCON ports associated with the other Cisco ONS 15530 remain up.

  Workaround: Shut down the tengigethernetphy interface associated with the second Cisco ONS 15530.

- CSCdy61641

  Symptom: Following a processor card crash and switchover, a **show redundancy** command issued on the new active processor card shows "Reported Switchover Reason" as "Not known". A **show version** command issued on the standby processor card that crashed shows additional troubleshooting information.

  Workaround: None.

- CSCdy62752

  Symptom: A few kinds of software exceptions on the active processor card can disable the ability for the standby processor card to reset the active processor card if the active processor card becomes nonresponsive.

  Workaround: None.

- CSCdy63359

  Symptom: The **getmany** command on the ifMIB causes the system to hang in a loop.

  Workaround: None.

- CSCdy65411

  Symptom: Mode-mismatch events or traps are set or generated 15 minutes after the misconfiguration that causes it is configured on the system.

  Workaround: None.

- CSCdz76974

  Symptom: The signal monitoring information is missing for the GE encapsulation in the **show interface** output.

  Workaround: None.

- CSCdy78546

  Symptom: From SNMP, ptopoConnEntry can be created with entPhysicalIndex, which does not correspond to any valid interface on the system.

  Workaround: None.

- CSCdy79161

  Symptom: Configuring both the client side and the trunk side for loopback on the 10-GE transponder module disrupts the traffic flow.

  Workaround: Reconfigure the 10-GE transponder module with loopback only on the client side or the trunk side, not both. Remove and reinsert the 10-GE transponder module to restore traffic.

- CSCdy79659

  Symptom: Incorrect OPM alarm status information for the standby wavepatch interface displays in the **show interfaces** command output.

  Workaround: None.

- CSCdy79812

  Symptom: CDL HEC counters are displayed in the **show interfaces tengigethernetphy** command output when CDL is disabled.

  Workaround: None.

- CSCdy81888

  Symptom: Traffic disruption on bootup or switchover occurs if 10-Gbps ITU trunk card client side is CDL disabled but has **cdl defect-indication force hop-endpoint** configured on both the client and trunk.

  Workaround: Use the **no cdl defect-indication force hop-endpoint** command on the client side.

- CSCdy83757

  Symptom: Unable to manage a system configured with EIGRP after a processor card switchover.

  Workaround: Connect to the console port and remove the passive-interface configuration in EIGRP configuration.

- CSCdy85563

  Symptom: The DI error message does not indicate DI bit status.

  Workaround: None.

- CSCdy87237

  Symptom: Line laser failure is not reported in the **show facility-alarm status** command output when the SFP optics in an extended range transponder module is removed and inserted online.

  Workaround: None.

- CSCdy88154

  Symptom: Some interfaces are not available to the NMS station because the agent does not create them when the module is removed and reinserted.

  Workaround: Reload the system after removal and reinsertion of the modules.

- CSCdz00116

  Symptom: APS message channel configured for UDP/IP does not work over more than two IP hops. The UDP/IP packet is dropped at the end of the second hop.

  Workaround: None.

- CSCdz02296

  Symptom: The **show patch detail** command output does not reflect the correct patch status for the ITU direct insertion module and the mux/demux module after the online removal and insertion of a 10-GE transponder module.

Workaround: None.

- CSCdz02340

  Symptom: Traceback @optical_idb_wave_ethernet_phy_report.

  Workaround: None.

- CSCdz03989

  Symptom: Both active and standby lasers in a bidirectional y-cable APS configuration on modules in subslot 0 turn on erroneously.

  Workaround: None,

- CSCdz06004

  Symptom: The **redundancy reload shelf** command on the active processor card can cause a switchover if the standby processor card is in ROM monitor mode.

  Workaround: Use the **reload** command to reload the active processor card, if the standby processor card is in ROM monitor mode.

- CSCdz06602

  Symptom: All OPM interval entries are not returned by the **getnext** command.

  Workaround: None.

- CSCdz08774

  Symptom: ciscoFlashDeviceChangeTrap is not generated when a removable Flash device is removed or inserted.

  Workaround: None.

- CSCdz12919

  Symptom: When the forward laser control is enabled on the 10-GE transponder module and the waveethernetphy interface laser is shut by this safety feature, the laser soft-start procedure has to be followed when the laser is enabled again.

  Workaround: None.

- CSCdz13538

  Symptom: The egress loss of signal alarm is not reasserted in the **show facility-alarm status** command output after using a **hw-module subslot power** command to turn the module power off or on.

  Workaround: None.

- CSCdz13673

  Symptom: The wave interface remains down when the signal quality is GOOD after using a **hw-module subslot power** command to turn the module power off or on.

  Workaround: None.

- CSCdz14420

  Symptom: The Rx power display in some cases is off by 4dBm in comparison with the real reading using power meter.

  Workaround: Use a calibrated 2.5-Gbps transponder module.

- CSCdz18757

Symptom: The default laser frequencies of the 2.5-Gbps transponder modules in odd numbered subslots (for example, x/1 or x/3) are not restored correctly after the second online removal and insertion. The laser frequencies are stored correctly for the first online removal and insertion only.

For example, when inserting a 2.5-Gbps transponder module (channel n and channel n+1) to subslot x/1 the first time, the default laser frequency is n+1 (correct). Remove this 2.5-Gbps transponder module and insert another (channel m and channel m+1); the default laser frequency becomes m (incorrect; it should be m+1).

Workaround: Remove and reinsert the 2.5-Gbps transponder module.

- CSCdz18815

Symptom: While performing an **aps switch force** command on a splitter APS group for 10-GE transponder modules, an erroneous alarm clear message displays for a different slot/subslot card that is not part of the APS group.

Workaround: None.

- CSCdz19099

Symptom: The Rx power display in some cases is off by 4dBm in comparison with the real reading using power meter.

Workaround: Use calibrated 2.5-Gbps transponder modules.

CSCdz20508

Symptom: The wavepatch interfaces are stuck in the down state after using the **shutdown/no shutdown** command sequence on the corresponding wave interface with splitter APS after loss of light occurs.

Workaround: None.

- CSCdz22455

Symptom: System crashes due to PCI master abort while doing a Sandisk removal and insertion.

Workaround: None.

- CSCdz25739

Symptom: The low warning threshold alarm is not cleared in the **show facility-alarm status** command output.

Workaround: None.

- CSCdz28582

Symptom: After a fiber cut, the OSC interface remains up with the signal quality good.

Workaround: Issue the **shutdown/no shutdown** command sequence.

- CSCdz28903

Symptom: For the Sysplex protocol, forward laser control does not work after removing and reinserting the 2.5-Gbps transponder module and reprogramming the functional image.

Workaround: Using the **no encapsulation** and **encapsulation sysplex etr** commands on the transparent interface programs it correctly.

- CSCdz29723

Symptom: When APS communication goes down, and an APS failure is subsequently detected, APS might switch over even though the communication is down. Based on this type of failure, a unidirectional switchover might occur. For IBM Sysplex CLO/ETR applications, a unidirectional switchover might lead to data corruption.

Workaround: None.

- CSCdz31593

    Symptom: In a point-to-point bidirectional configuration, when the trunk Rx on both NEs are pulled and one of them is later replaced, APS might fluctuate between working and protection. Under certain conditions the driver declares both working and protection as down when the wave interface goes down.

    In bidirectional APS this essentially means that the local side may inform the remote side that Working/Protection is down when it is not really down. APS has the ability to settle down on the good side; however, due to the bidirectional message (DO-NOT-REVERT in this case) from the far side; the local side switches away from the good side, and the cycle repeats. Note that this problem does not always happen, and requires certain timing in order to happen.

    Workaround: Use a force switch or lockout to force the receive to the good side or temporarily change the direction from bidirectional to unidirectional after disabling the APS group.

- CSCdz33752

    Symptom: In bidirectional APS, if both NEs have the same priority request, the master/slave determination fails, leading to both claiming the control and resulting in not sending a REVERSE-REQUEST.

    Workaround: None.

- CSCdz36420

    Symptom: In a preconfigured APS group (when the interfaces do not exist), if the group is configured for revertive mode, it cannot be enabled.

    Workaround: Enable the group after the interfaces are defined in the APS group are created or remove the revertive configuration from the pre-configured APS group and then enable the group.

- CSCdz36424

    Symptom: Attempting to read a Flash device formatted on another system causes advisory messages to be continuously printed to the console.

    Workaround: None.

- CSCdz36823

    Symptom: The processor crashes after midnight with optical performance monitoring on when an interface capable of performance monitoring is shutdown before 00-00hrs and unshut after midnight.

    Workaround: None.

- CSCdz37698

    Symptom: Both working and protection client Tx are active in a y-cable APS configuration.

    Workaround: None.

- CSCdz37968

    Symptom: The **hw-module subslot power on/off** command should not be supported for 10-GE transponder modules.

    Workaround: None.

- CSCdz38075

    Symptom: Data traffic is disrupted during the processor card switchover when the splitter APS is configured.

    Workaround: None.

- CSCdz38448

    Symptom: In y-cable bidirectional APS configuration using 10-GE transponder modules, whenever many CVRD errors are received on the standby trunk due to a bad signal (but still signal quality is GOOD in **show interfaces** command output), all four FDI-H/E and BDI-H/E bits in the DECCSR register might get latched. This generates interrupts and the console is flooded with messages for that interface such as the following:

    ```
    00:15:17: %APS-3-PORT_FAIL: External Port Fail On WaveEthernetPhy10/1
    ```

    Workaround: Improve the quality of the signal by removing some attenuation and/or cleaning the optical connectors so that CVRD errors are not seen.

- CSCdz38968

    Symptom: Spurious memory access occurs on online removal and reinsertion of a 10-GE transponder module.

    Workaround: None.

- CSCdz39112

    Symptom: When an invalid channel number is detected by the OSCP client while it processes the client message received from a peer, OSCP does not free the message buffer. This results in buffer starvation over a period of time and connectivity on the Network Management interface and backplane Ethernet (IPC and OSCP) interface are lost.

    Workaround: None.

- CSCdz39793

    Symptom: The optical alarms are not asserted or cleared correctly when the wave interface is in the administrative down state.

    Workaround: Issue the **shutdown/no shutdown** command sequence on the active wavepatch, or issue the **no shutdown** command on wave interface to clear the false alarms.

- CSCdz40675

    Symptom: Receiver power low alarm and warning are not asserted on the wavepatch interface after switchover from the active wavepatch interface to the standby wavepatch interface.

    Workaround: None.

- CSCdz41160

    Symptom: Continuous "SRC poll failure" messages are generated after removing a calibrated 2.5-Gbps transponder module and inserting a uncalibrated 2.5-Gbps transponder module or ITU direct insertion module.

    Workaround: None.

- CSCdz42547

    Symptom: Using the **no shutdown** command on the tengigethernetphy or waveethernetphy interfaces (which is DOWN due to loss of lock) brings the interface state to UP, even though the loss of lock is still asserted.

    Workaround: Issue the **shutdown/no shutdown** command sequence on the interface for it to show the DOWN state.

- CSCdz42565

    Symptom: Loss of sync is not reasserted on a tengigethernetphy interface after a **shutdown/no shutdown** command sequence has been issued on the interface, or on an online removal and reinsertion of the 10-GE transponder module.

Workaround: None.

- CSCdz43279

    Symptom: The ethernetdcc interface for 10-GE transponder module is not in the admin down state on the initial online removal and reinsertion of the module.

    Workaround: None.

- CSCdz56523

    Symptom: Loss of lock persists on a client interface that runs Sysplex CLO/ETR protocols.

    Workaround: Issue the **shutdown/no shutdown** command sequence on the client interface to clear the loss of lock.

- CSCdz58866

    Symptom: The threshold group line is missing in the **show interfaces waveethernetphy** command output.

    Workaround: None.

- CSCdz60081

    Symptom: The hardware reports spurious loss of lock errors when the signal quality is good for the Sysplex ETR encapsulation after online removal and insertion of the 2.5-Gbps transponder module.

    Workaround: Issue a **no encapsulation** command and configure the encapsulation back to Sysplex ETR.

- CSCdz62553

    Symptom: The tengigethernetphy interface is getting BDI-H while the in-band message channel is disabled.

    Workaround: None.

- CSCdz66609

    Symptom: A traffic loss of 30 to 45 seconds might occur when a y-cable APS configuration with protection switchover is used with the Catalyst 6000 family.

    Workaround: Disable autonegotiation and enable debounce timer with 100 ms delay on Catalyst 6000 family using the **set port debounce mod/port enable** command sequence.

- CSCdz75109

    Symptom: When y-cable APS is configured, shutting off the power to the transponder module using the **hw-module subslot power off** command brings the power back on again immediately.

    Workaround: Remove the APS configuration and perform power off.

- CSCdz76974

    Symptom: The signal monitoring information is missing for the GE encapsulation in the **show interfaces** command output.

    Workaround: None.

- CSCdz77034

    Symptom: When both wavepatch interfaces are in an ADMIN DOWN state, the signal quality is unknown but the **show facility-alarm status** command reports Loss of Signal.

    Workaround: None.

- CSCdz79336

Symptom: APS switchover time (50 ms) is not guaranteed for loss of lock, loss of sync, or loss of frame. It is only guaranteed for loss of light.

Workaround: None.

- CSCdz80042

Symptom: The output of the **show interfaces waveethernetphy** command sometimes shows a high receiver power value when there is no input signal connected to the card.

Workaround: OIR the card.

- CSCdz83169

Symptom: Could not get a wave power reading graph with CiscoView 2.0/2.1 for an uncalibrated 2.5-Gbps transponder module.

Workaround: Use a calibrated 2.5-Gbps transponder module.

- CSCdz85458

Symptom: When the 10-GE transponder module (waveethernetphy) laser is down due to a forward laser control action, removing the forward laser control configuration does not turn the laser back on.

Workaround: None.

- CSCea03957

Symptom: OPM (optical power monitoring) feature does not work on uncalibrated 2.5-Gbps transponders modules.

Workaround: None.

- CSCea04546

Symptom: Cannot disable SNMP-server traps for TTY messages on a global basis.

Workaround: Configure traps on a per SNMP-server host basis.

- CSCea16511

Symptom: The standby processor in the CiscoView shelf display shows a 100-Mbps connection when the port is connected to a 10-Mbps hub or switch.

Workaround: None.

- CSCea28131

A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order 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, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

- CSCea41710

Symptom: The optical power monitoring alarms and configuration are missing across the 2.5-Gbps transponder module online removal and insertion.

Workaround: None.

- CSCea60957

Symptom: A spurious memory access at manopt_tl1_report_aps_defect occurs during the processor switchover when APS is configured.

Workaround: None.

- CSCea92296

   Symptom: The transponder module traceback messages might flood the console, causing processor usage to increase to the point that it becomes unresponsive to the console and to network access.

   Workaround: OIR the transponder module or the entire line card motherboard if all the transponder modules on the line card motherboard are failing. Ensure that all modules and line cards are seated properly and locked or screwed down.

- CSCeb20229

   Symptom: When a client loss of signal (loss of light/loss of lock) condition occurs on an extended range transponder module, typically by disconnecting the client from the transponder module or when the client device halts transmission briefly during an initialization sequence, the following might occur:

   - Laser degrade or laser wavelength deviation alarms may be asserted by the system and displayed on the console. These messages can be ignored.

   - The laser output power might drop for a few seconds and then recover. This might cause loss of light conditions at the far-end trunk receiver. The ITU laser power might fluctuate up and down until the client signal is reconnected.

   Neither of these conditions affect the functioning or life span of the laser. The laser power output will stabilize and return to normal operation when a valid client signal is connected.

   Workaround: Enable forward laser control using the **laser control forward enable** command on the wave interface. Or keep the wave interface shutdown when there is no client signal, but issue the **no shutdown** command on the wave interface when the client signal is reconnected.

- CSCeb31264

   Symptom: The extended range transponder configured with FDDI encapsulation when connected with FDDI ports on a Catalyst 5000 causes the Catalyst 5000 port to take more than seven seconds to initialize if an Rx fiber break and insertion is done at the transponder client receive end.

   Workaround: None.

- CSCeb37281

   Symptom: With particular OC-48 SFPs in a Y cable APS setup with extended range transponders, the Tx default on the SFP does not allow the client laser to enable because of the BLC.

   Workaround: None.

- CSCeb54866

   Symptom: MPL for splitter and y cable APS protection schemes should indicate losync/loframe/lolock instead of lolight

   Workaround: None.

- CSCeb55150

   Symptom: The OPM alarms (low warning and low alarm) are not being reasserted after issuing a the shutdown/no shutdown command sequence on the wavepatch x/y/0 interface.

   Workaround: OIR the subcard to reassert the alarms.

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.

• If both processor cards are removed, traffic through the system is affected as follows:

 – For Type 2 extended range transponder modules, traffic is shut down.

 – For 10-GE transponder modules, traffic is shut down.

 – Type 1 SM transponder modules and MM transponder modules do not operate reliably. The traffic might be affected.

 – In the shutdown state, the Status LED on the line card motherboard turns orange.

Note Traffic on pass through optical channels (which passively pass through the mux/demux modules) are not affected by the removal of the processor cards.

Related Documentation

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

• *Cisco ONS 15540 ESP Planning and Design Guide*

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

• *Cisco ONS 15540 ESP Hardware Installation Guide*

• *Cisco ONS 15540 ESP Configuration Guide and Command Reference*

• *Optical Transport Turn-Up and Test Guide*

• *Cisco ONS 15540 ESP Troubleshooting Guide*

• *Cisco ONS 15540 ESP MIB Quick Reference*

- *Glossary of Optical Networking Terms*

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

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 Networking Products MarketPlace:

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

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments 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

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

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

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.

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

- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

- Priority level 1 (P1)—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.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

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

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

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

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

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

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

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

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

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

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- 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://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* 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/go/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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

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

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

---

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