



# Release Notes for Cisco ONS 15454 SDH Release 5.0.4

---



## Note

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

---

## October, 2007

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15454 SDH multiplexer. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to the “Release 5.0.2” version of the *Cisco ONS 15454 DWDM Installation and Operations Guide*; and the “Release 5.0” version of the *Cisco ONS 15454 SDH Procedure Guide*; *Cisco ONS 15454 SDH Reference Manual*; *Cisco ONS 15454 SDH Troubleshooting Guide*; and *Cisco ONS 15454 SDH TLI Command Guide*. For the most current version of the *Release Notes for Cisco ONS 15454 Release 5.0.4*, visit the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/ong/15454sdh/sdhreInt/index.htm>

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

[http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)

## Contents

- [Changes to the Release Notes, page 3](#)
- [Caveats, page 3](#)
- [Resolved Caveats for Release 5.0.4, page 30](#)
- [New Features and Functionality, page 40](#)
- [Related Documentation, page 70](#)



---

### Corporate Headquarters:

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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

[Obtaining Documentation, page 70](#)

[Obtaining Technical Assistance, page 71](#)

# Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15454 SDH Release 5.0.4* since the production of the Cisco ONS 15454 SDH System Software CD for Release 5.0.4.

The following changes have been added to the release notes for Release 5.0.4.

## Changes to Caveats

The following caveats have been added.

[DDTS # CSCeh08430, page 11](#)

[DDTS # CSCeg42512, page 15](#)

[DDTS # CSCei04981, CSCeg42532, page 15](#)

[DDTS # CSCei64727, page 15](#)

## Caveats

Review the notes listed below before deploying the ONS 15454 SDH. Caveats with DDTS tracking numbers are known system limitations that are scheduled to be addressed in a subsequent release. Caveats without DDTS tracking numbers are provided to point out procedural or situational considerations when deploying the product.

## Hardware

### STM1E-12 Card Support

The STM1E-12 card is not supported in this release. This card will be supported in a future release. Caveats herein pertaining to this card also do not apply.

### DDTS # CSCed18803

Rarely, the non-enhanced Muxponder unit does not pass Jitter Tolerance test from Trunk port to client port as per ITU-T G.825, 2 Mb/s mask, at the 10 Hz specific setpoint. The Muxponder should be configured with G.709 Off, FEC Off and Trunk signal provided by external Jitter test box, and the unit client port output monitored for errors, to see this issue. This issue will be resolved in a future release. Note, however, that in normal network configurations the muxponder is operated with G.709 and FEC turned on, and the jitter tolerance tests pass.

### DDTS # CSCuk48503

Under specific conditions the non-enhanced MXPDP does not pass the Telcordia GR-253/G.825 Jitter generation mask test on 10G TX Trunk port. The 2.5 G TX Client jitter generation is always within mask and does not exhibit this issue. This occurs only when, in SONET mode, there is no FEC, no G.709, and client interfaces are looped back, with non-synchronous clocking, and the jitter testbox TX connected to

Trunk RX port, while the jitter testbox RX is connected to the Trunk TX port. The jitter testbox TX clock recovers from RX with an additional 5 ppm offset added. This issue will be resolved in a future hardware release.

## DDTS # CSCea78210

The TXP\_MR\_2.5G and TXPP\_MR\_2.5G cards do not support TX Optical power performance monitoring on the trunk port. To see this, go to the Optics Performance Monitoring tab of the TXP\_MR\_2.5G or TXPP\_MR\_2.5G card, and select the trunk port. TX Optical Pwr is not shown. This is as designed.

## DDTS # CSCdw92634

SDH DS3-I and E3 electrical cards only support a VC4 J1 trace string setting for all VC4s together. You cannot set the J1 byte for individual VC4s. This issue is a limitation of hardware.



**Note**

---

VC3 J1 strings can be set individually, but the optical cards cannot monitor the VC3 J1 string.

---

## DDTS # CSCdw14501

Interconnection Equipment failure alarms may be generated at 55 degrees C, and 72 volts. When the operating environment is at 55 degrees C and 72 volts, interconnection equipment failure alarms for the following cards can occur:

- STM16SH
- STM64LH
- STM16LH

The alarms could potentially occur on any of these boards, as well: OC48AS, GigE, OC192 or OC192LR. This issue will be resolved in a future release.

## DDTS # CSCdw50903

E1-14 boards with second source components can incur bit errors under extreme environmental conditions. When these boards operate under voltage and temperature stress conditions and a temperature ramp rate of 1 degree per minute, the boards could exhibit dribbling bit errors at high temperatures: BER = 5.5e-6. To avoid this, you must apply the temperature ramp rate at 0.5 degree per minute. This ramp rate complies with the NEBS standard; however, this issue will be revisited in a future release.

## Upgrades

### DDTS # CSCec42769 Database Corruption with ONS 15454 SDH Release 4.0, 4.0.1, 4.1



**Caution**

---

Before you upgrade to Release 5.x from Release 4.0, 4.0.1, or 4.1, you must read this caveat and run the SDH Circuit Repair Utility (VcCheck) provided on the software CD (also available on CCO).

---

The XCVXL card on the ONS 15454 SDH allows the intermixing of VC12 and VC3 payloads within a single VC4. When a VC4 contains only one VC12 tributary and at least one VC3 tributary and the VC12 is deleted, the database becomes corrupt.

The database load process on the ONS 15454 SDH occurs during a TCC2/TCC2P reboot, TCC2/TCC2P protection switch, software activation, or database restore. When the database is loaded containing this corruption the load process fails, causing the corrupt database to be deleted from the TCC2/TCC2P flash memory. The previous saved database is then loaded instead. When all saved databases on a TCC2/TCC2P contain the corruption, the TCC2/TCC2P will load with the default provisioning, and all existing provisioning will be lost.

If this issue occurs you will see a loss of either some or all provisioning after a TCC2/TCC2P switch or reset.

To ensure that your network is not vulnerable to this issue, you must first determine if the issue already exists within your network, and if so, correct it. You can detect the issue by using the SDH Circuit Repair Utility (VcCheck) provided on the ONS 15454 SDH Release 4.1.3, 4.6.x, or 5.x software CDs. The VcCheck tool is also available for download from CCO. Once you have alleviated immediate risk from the issue, you must upgrade to Release 5.x, Release 4.6.1, or maintenance Release 4.1.3 (or any later release) to avoid further risk.

The VcCheck utility and its associated README file (in the same directory with the tool) provide details on how to temporarily alleviate this issue before upgrading to a release in which the issue is resolved.

This issue is resolved in Releases 4.6 and later, and in maintenance Releases 4.1.3 and later (caveated herein because of the upgrade issue).

## Maintenance and Administration



### Caution

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



### Note

In releases prior to 4.6 you could independently set proxy server gateway settings; however, with Release 4.6.x and forward, this is no longer the case. To retain the integrity of existing network configurations, settings made in a pre-4.6 release are not changed on an upgrade to Release 5.x. Current settings are displayed in CTC (whether they were inherited from an upgrade, or they were set using the current GUI).

## DDTS # CSCeh03525

If there are tunnel circuits in nodes prior to an upgrade, CTC might display some PARTIAL tunnel circuits after upgrading those nodes from Release 5.0 or earlier. These PARTIAL circuits should be empty circuits, with no cross-connects, so traffic will not be affected. After verifying that the PARTIAL tunnel circuits have no cross-connect (you can look at the "Circuit Edit" window), delete the empty circuits. This issue will be resolved in a future release.

**DDTS # CSCeh08148**

When deleting more than 25 circuits at a time some circuits might not be deleted. If this occurs, delete those circuits that were mistakenly left undeleted again. This issue will be resolved in Release 6.0.

**DDTS # CSCeh08293**

Some low order VT SD and SF BER level thresholds are displayed with values when no values should be present. Only ONS 15310-CL nodes should display these thresholds for Release 5.0. In Release 6.0, all nodes equipped with XCVXC cards will support low order VT thresholds.

**DDTS # CSCeg43238**

Rarely, on a large network (having more than 5 nodes), if you select multiple required links as routing preferences while attempting to create 42 E1-42 VC12 circuits using the autorange circuit creation tool, you will not be allowed to finish the task. To recover from this issue, run the auto creation again to finish the remaining circuits. This issue will be resolved in a future release.

**DDTS # CSCee27990**

During activation (to a new load) or revert (to a previous load), CTC might lose connection with the node, requiring that you restart CTC. Deleting the browser cache when restarting CTC might result in an error: "EID-2197 CORBA failure. Unable to proceed." If this occurs, close the browser, reopen it, and then restart CTC. This issue will be resolved in a future release.

**DDTS # CSCef89692**

Sometimes, in a 1:N protection group, a locked-out working card carries traffic. This issue can occur when you lock out a working card, reseal that card, reseal the protect card, and then, while the protect card is booting up, remove another working card. After the protect card comes up, it starts protecting the traffic for the removed card and the locked-out working card carries its own traffic. This issue will be resolved in a future release.

**DDTS # CSCef53317**

A traffic hit can occur during a clock reference switch. To see this issue, complete the following steps.

- 
- Step 1** Set up two ONS 15454 SDH nodes with STM16 SNCP (call the nodes STM16-1 and STM16-2).
  - Step 2** Set up two ONS 15454 SDH nodes with MXP\_MR\_2.5G\_10G (call the nodes MXP-1 and MXP-2).
  - Step 3** Place MXP-1 and MXP-2 in Transparent Termination Mode.
  - Step 4** Ensure that STM16-1 is connected to MXP-1 client 1.
  - Step 5** Ensure that STM16-2 is connected to MXP-2 client 1.
  - Step 6** Ensure that MXP-1 trunk is connected to MXP-2 trunk.
  - Step 7** Connect a traffic generator to MXP\_MR\_2.5G\_10G Port 3 (client) of MXP-1 and feed a PRC clock.
  - Step 8** Set MXP-1 Clock Reference 1 to MXP\_MR\_2.5G\_10G Port 3, leaving the other two clock references as INTERNAL.

- Step 9** Provision circuits such that a combination of VC4-4C, VC12, VC3 and VC4 traffic flows between STM16-1 and STM16-2 through MXP-1 and MXP-2.
- Step 10** Gradually inject increasingly negative frequency offset through the traffic generator, in steps of 3 ppm, where you perform the next decrement step only when the node returns to NORMAL state.

---

When the clock offset reaches around 17 ppm, Clock Reference 1 fails and MXP-1 switches to Clock Reference 2. During the clock switch a traffic hit might occur for less than one second. The same is behavior can occur when injecting positive frequency offset. This issue will be resolved in a future release.

## DDTS # CSCuk49106

The amplifier gain set point shown by CTC and the actual measured amplifier gain differ. The following steps illustrate this issue.

- 
- Step 1** Reduce the insertion loss of the span just before the amplifier.
- Step 2** Execute the APC procedure.

---

The APC procedure does not check consistency between the gain set point and the real gain, but rather only verifies the amplifier total output power. As a workaround, manual setting can be performed to align these values, although the discrepancy does not impact the normal functioning of the amplifier. This issue will not be resolved.

## DDTS # CSCuk52850

In a fiber cut scenario on the LINE-RX, with OSC and channels provisioned, transient LOS-P or LOS-O alarms might be raised. This issue will be resolved in Release 6.0.

## DDTS # CSCef54670

The SQUELCHED condition is not raised when a non-enhanced MXP card is in MS termination mode. To see this issue perform the following steps.

- 
- Step 1** Set up one ONS 15454 SDH node with MXP\_2.5G\_10G (MXP-1).
- Step 2** Provision MXP-1 Port 1 (client) with any payload.
- Step 3** Set MXP-1 Port 1 (client) and Port 5 (trunk) to the UNLOCKED state.

---

LOS and LOS-P alarms are reported on MXP-1 Port 1 (client). The SQUELCHED condition is not reported on MXP-1 Port 1 (client) because AIS is sent out the client port instead. This is as designed.

## DDTS # CSCef05162

Clearing the displayed statistics for a port will also clear the displayed history for that port. Clearing the displayed statistics for all ports will also clear the displayed history for all ports. There is no warning message from the TCC2. If History information is to be retained, do not clear displayed statistics for any port without first documenting the displayed history information for the associated port. This issue will not be resolved.

## DDTS # CSCef29516

The ALS pulse recovery min value is 60 instead of 100. If this occurs, increase the value to 100. This issue will not be resolved.

## DDTS # CSCeb36749

In a Y-Cable configuration, if you remove the client standby RX fiber; a non-service affecting LOS is raised, as expected. However, if you then remove the trunk active RX fiber; a non-service affecting LOC is raised, but the previously non-service affecting LOS on the client port is now escalated to a service affecting alarm, in spite of no traffic having been affected. It is not known when or if this issue will be resolved.

## DDTS # CSCee82052

After setting the node time (either manually or via NTP) you must wait for the endpoint of the interval to be reached before the end time will reflect the recently-set node time. Until this has occurred, the date time stamp for the end of the retrieved interval remains 12/31/69. This issue has been closed and will not be resolved.

## DDTS # CSCeb39359

When changing NE timing from extern/mix to Line timing, a Transient IEF alarm may be reported against the standby XC10G. This issue will be resolved in a future release.

## DDTS # CSCea81001

When a fault condition exists against a circuit or port that is in the OOS-MT or OOS-AINS state (or when you are using the "Suppress Alarms" check box on the CTC Alarm Behavior pane), the alarm condition is not assigned a reference number. If you were to place the circuit or port in service at this time, in the absence of the reference number, the CTC alarm pane would display the condition with a time stamp indicating an alleged, but incorrect, time that the autonomous notification was issued. Clicking the CTC alarm "Synchronize" button at this stage will correct the alarm time stamp. There is no way to remedy the lack of reference number. This issue will be resolved in Release 6.0.

## DDTS # CSCdz62367

When replacing a failed working E1-42 card in a 1:1 or 1:N protection configuration with the protect card carrying the switched traffic, bit errors, less than 50ms in duration, are possible on the activated protection card. This issue will not be resolved.

## DDTS # CSCdy10030

CVs are not positively adjusted after exiting a UAS state. When a transition has been made from counting UAS, at least 10 seconds of non-SES must be counted to exit UAS. This issue will not be resolved.

## DDTS # CSCdx35561

CTC is unable to communicate with an ONS 15454 SDH that is connected via an Ethernet craft port. CTC does, however, communicate over an SDCC link with an ONS 15454 SDH that is Ethernet connected, yielding a slow connection. This situation occurs when multiple nodes are on a single Ethernet segment and the nodes have different values for any of the following features:

- Enable OSPF on the LAN
- Enable Firewall
- Craft Access Only

When any of these features are enabled, the proxy ARP service on the node is also disabled. The ONS 15454 SDH proxy ARP service assumes that all nodes are participating in the service.

This situation can also occur immediately after the aforementioned features are enabled. Other hosts on the Ethernet segment (for example, the subnet router) may retain incorrect ARP settings for the ONS 15454 SDHs.

To avoid this issue, all nodes on the same Ethernet segment must have the same values for Enable OSPF on the LAN, Enable Firewall, and Craft Access Only. If any of these values have changed recently, it may be necessary to allow connected hosts (such as the subnet router) to expire their ARP entries.

You can avoid waiting for the ARP entries to expire on their own by removing the SDCC links from the affected ONS 15454 SDH nodes. This will disconnect them for the purposes of the proxy ARP service and the nodes should become directly accessible over the Ethernet. Network settings on the nodes can then be provisioned as desired, after which the SDCC can be restored. This issue will not be resolved.

## DDTS # CSCdy11012

When the topology host is connected to multiple OSPF areas, but CTC is launched on a node that is connected to fewer areas, the topology host appears in CTC, and all nodes appear in the network view, but some nodes remain disconnected. This can occur when the CTC host does not have routing information to connect to the disconnected nodes. (This can happen, for example, if automatic host detection was used to connect the CTC workstation to the initial node.)

CTC will be able to contact the topology host to learn about all the nodes in all the OSPF areas, but will be unable to contact any nodes that are not in the OSPF areas used by the launch node. Therefore, some nodes will remain disconnected in the CTC network view.

To work around this issue, if no firewall enabled, then the network configuration of the CTC host can be changed to allow CTC to see all nodes in the network. The launch node must be on its own subnet to prevent network partitioning, and craft access must not be enabled. The CTC host must be provisioned with an address on the same subnet as the initial node (but this address must not conflict with any other node in the network), and with the default gateway of the initial node. CTC will now be able to contact all nodes in the network.

If a firewall is enabled on any node in the network, then CTC will be unable to contact nodes outside of the initial OSPF areas. This issue will not be resolved.

## DDTS # CSCdy57891

An LOP-P alarm can be inadvertently cleared by an LOS that is raised and cleared. On STM-N cards, when an LOP condition and an LOS condition are both present on the input, an LOS will be raised. However, upon clearing the LOS with the LOP still present, the LOP alarm is not raised. An AIS-P condition will be visible. This issue will not be resolved.

## DDTS # CSCdw38283

If a node has one good BITS reference and is running in a normal state, and you configure a second BITS reference, then reconfigure the second reference within 30 seconds of applying the first configuration, the node will enter FAST START SYNC mode. To avoid this problem, wait a minute before configuring the second reference a second time. This issue is a hardware limitation, and there are no current plans to resolve it.

## DDTS # CSCdw23208

Table 1 summarizes B1, B2, and B3 error count reporting for SDH optical cards. Note that not all reporting is done according to ITU specifications. In particular, ITU specifies error counts for B1 and B3 as the number of blocks with errors (refer to ITU-T G.826 for paths and ITU-T G.829 for RS and MS).

**Table 1** Error Count Reporting

Specification/Card Comparison	B1	B2	B3
ITU Specification	block	bit	block
STM1	block	bit	block
STM4	bit	bit	bit
STM16 trunk	bit	bit	bit
STM16 AS	block	bit	bit
STM64	block	bit	bit
STM1-8	bit	bit	bit
STM4-4	bit	bit	bit

## DDTS # CSCdw82689

After creating 509 VLANs and provisioning many Ethernet circuits, Ethernet circuit provisioning can become very slow, or possibly fail. Ethernet traffic may also incur an outage of a few minutes. To avoid this problem, delete any VLANs that are created but not used, and do not recreate them. There is no resolution planned for this issue.

## DDTS # CSCdv10824: Netscape Plugins Directory

If you use CTC, JRE, and the Netscape browser with a Microsoft Windows platform, you must ensure that any new installation of Netscape uses the same Netscape directory as the previous installation did, if such an installation existed. If you install Netscape using a different path for the plugins directory, you will need to reinstall JRE so that it can detect the new directory.

## “Are you sure” Prompts

Whenever a proposed change occurs, the “Are you sure” dialog box appears to warn the user that the action can change existing provisioning states or can cause traffic disruptions.

## Common Control and Cross Connect Cards

### DDTS # CSCeh08430

Rarely, short line card data hits can occur intermittently on a variety of circuits when the active TCC2P card is removed while the XC-VXC-10G card is being used. This issue is under investigation.

### DDTS # CSCee94587

Rarely, a TCC2/TCC2P side switch might cause long traffic hits on E1-42, DS3I, or E3 cards. Circuits recover, so no recovery procedure is required. Perform a TCC2/TCC2P soft reset in the case of a software upgrade. This issue will be resolved in a future release.

### DDTS # CSCef72623

Rarely, TCC2/TCC2P card removal can result in 3 to 28 ms data path traffic hits. This issue will be resolved in a future release.

### DDTS # CSCec82148

Rarely, traffic hits can occur on TCC2/TCC2P card removal. To avoid this issue, remove the card quickly. To recover from this issue, soft reset the TCC2/TCC2P card. This issue will be resolved in Release 6.0.

## Ethernet Polarity Detection

The TCC2/TCC2P does not support Ethernet polarity detection. The TCC+ and TCCI both support this feature. If your Ethernet connection has the incorrect polarity (this can only occur with cables that have the receive wire pairs flipped), the TCC+/I will work, but the TCC2/TCC2P will not. In this event, a standing condition, “LAN Connection Polarity Reverse Detected” (COND-LAN-POL-REV), will be raised (a notification will appear on the LCD, and there will be an alarm raised). This issue will most likely be seen during an upgrade or initial node deployment. To correct the situation, ensure that your Ethernet cable has the correct mapping of the wire wrap pins. For Ethernet pin mappings, consult the user documentation.

## Active Cross Connect or TCC2/TCC2P Card Removal

Active cross connect or TCC2/TCC2P cards should not be removed. If the active cross connect or TCC2/TCC2P card must be removed, to minimize network interruption you can first perform an XCVXL side switch and then remove the card once it is in standby, or you can perform a lockout on all circuits that originate from the node whose active cross connect or active TCC2/TCC2P will be removed (performing a lockout on all spans will also accomplish the same goal).

**Caution**


---

If you mistakenly remove an active cross connect or TCC2/TCC2P card and you subsequently lose traffic on some interface cards, you may need to physically reset these cards if they fail to regain traffic.

---

## Optical IO Cards

### DDTS # CSCee17695 and CSCed26246

Rarely, an STM1-8 card might fail to read MFG EEPROM and will show MEA in CTC. This issue can be reproduced by power cycling the node several times, by quickly removing and reinserting a fuse, or when the fuse is removed for several minutes and then replaced; however, the issue is not likely to be due to the power cycling. If a card enters this state, remove and reseal it, or cycle power again to recover STM1-8 operation. This issue will be resolved in a future release.

### DDTS # CSCdw44431

Cisco ONS 15454 optical cards are not provisioned for particular path labels (C2 bytes). Consequently, they cannot raise a PLM condition. However, the ONS 15454 electrical card that terminates traffic ensures that the C2 byte is correct for the type of traffic carried. If the C2 byte is incorrect, this card raises a PLM condition that is reported against the optical port of ingress. An optical card will not raise a PLM against traffic that passes through a node, though it will appear to raise a PLM against traffic with the wrong C2 byte that is terminated on an electrical card within the node. It is not known at this time when or if this issue will be resolved.

**Note**


---

Optical cards do ensure that the C2 byte is nonzero (Equipped), and will raise a UNEQ condition if the C2 byte is 0 (Unequipped).

---

### DDTS # CSCdw57215

In a configuration with STM16 Any Slot cards and an VC4-8c circuit, provisioned between G1000-4 cards with traffic going over the STM16 span, extracting the G1000-4 card at one end of the VC4-8c circuit before deleting the circuit can result in a traffic hit on all existing SDH circuits defined over that same span. There are no issues if the circuit is deleted prior to the removing the G1000-4 card.

## Electrical IO Cards

### DDTS # CSCeg38898

E1 VC12 traffic with 1:N protection takes double traffic hits with a hard reset. The following example illustrates the issue:

- 
- Step 1** Set up a four node STM16 SNCP.
  - Step 2** Create an E1 1:N protection group in Node 1 and provision a VC12 circuit from one of the working cards to an E1 card in Node 2.

- Step 3** Remove the working card from Node 2 and traffic switches to the protect card, taking hits below 60 ms. Just before the working card finishes booting, however, another hit might occur.
- 

This issue is not seen in MSSP provisioned circuits. This issue will be resolved in a future release.

### **DDTS # CSCeg80233**

Long traffic hits can occur on E1-42 when using cross connect FIT cards. This can occur when, on the FIT card, you toggle the 155 mhz clock going to the E1-42 cards to the off position. This issue will be resolved in a future release.

### **DDTS # CSCeg81428**

Rarely, a long traffic hit (117 ms) can occur on E1-42 after an XC side switch. In multinode BLSR setups, switching the cross connect cards repeatedly might cause traffic hits greater than 60 ms. To avoid this issue side switch the XC only when needed (and not repeatedly). This issue will not be resolved.

### **DDTS # CSCeg19255**

Rarely, DS3I VC3 traffic takes a hit greater than 60 ms during a cross connect card soft reset. This issue will be resolved in a future release.

### **DDTS # CSCeg38898**

In a four node, STM16 SNCP, if you have an E1 1:N protection group with a VC12 circuit from one of the working cards of one node to an E1 card in another node, and you remove the working card in the second node, when traffic switches to the protect card, the traffic might take a second hit just before the working card finishes booting (after the first, expected, less than 60 ms traffic hit). This issue will be resolved in a future release.

### **DDTS # CSCeg31417**

In certain configurations with two four-node, two-fiber, STM-64 MS-SPRings interconnected by a third, two-node, two-fiber, STM-16 MS-SPRing, with E1-42/VC12 monitor circuits and a path protection circuit between two E1-42 cards, the far end E1-42 switch time might be 60-70 ms upon removal of the near end working card. This can occur in situations where the near end E1-42 card is part of a 1:N protection group. To avoid this issue, set path protection holdoff time to 100 ms, or apply path protection protection lockout. This issue will be resolved in a future release.

### **DDTS # CSCeg65307**

When cross connect cards are unstable (when cards are removed and reinserted, or side switching occurs), power-up initialization can sometimes fail while the cross connect cards are switching or rebooting, causing the Failed LED for an E1-42 card to remain lit. If this occurs, reseal the affected card. This issue will be resolved in Release 6.0.

## DDTS # CSCeg13517

If you have a VC3 circuit with DS3I on both ends, you might see DS3 LOF instead of DS3 AIS. You will see MS-AIS and TU-AIS. If you disable the ports on both STM-16 AS cards in a BLSR and have your VC3 circuits in a daisy chain configuration, this can be an issue. Do not daisy chain circuits, and do not disable ports in a BLSR without locking out the ring. This issue will be resolved in a future release.

## DDTS # CSCef67059

Bit errors can occur on E1-42 line cards passing traffic, when other E1-42 line cards are initially inserted into adjacent slots. Specifically, inserting line cards into adjacent slots or 1:N protect slots (Slots 3 and 15) can cause hits on Ports 1-14. Also, when the card in the 1:N protection slot is passing traffic, inserting E1-42 line cards into adjacent slots can cause bit errors. The bit errors characteristically last less than 5 ms. After the card is inserted, no further bit errors occur. Ports 15-42 behave differently. No bit errors occur on a line card residing in a non-1:N slot if adjacent line cards are inserted. Bit errors will only occur for these ports if line cards are inserted into the 1:N protection slots (Slots 3 and 15). Bit errors might also occur if traffic passes through the 1:N protected slot, and you insert a line card into any other working slot. A future version of E1-42 hardware will resolve this issue.

## Interoperability with SONET DS3i-N-12

When provisioning circuits in SDH to interoperate with SONET DS3i-N-12, you must create a VC4 containing VC3s as a payload in the exact order in which they will attach to port groups on the SONET side.

## DDTS # CSCea52722

With DS3-I cards in a 1:2 protection group, when the protect card is active and in the WTR condition, removing another working card from the protection group clears the WTR condition. To work around this issue, remove the working card from the protection group when the protect card is in the standby state. This issue will be resolved in Release 6.0.

## DDTS # CSCdw80652

When one traffic card in a DS3I 1:N protection group is reset, and then another card is reset, there will be a loss of traffic on the second card, after the first card completes its reset, lasting until the second card completes its reset. This only occurs when the protect card tries to handle the traffic of a card that is resetting, and that card is carrying traffic because when it reset the protect card was carrying traffic for another card. This loss of traffic occurs because the protect card attempts to set its relays to handle the traffic of the working card, but the relays on the working card are also set to carry the traffic, and since the card is resetting, no software is running to switch its relays. This issue most frequently presents itself when testing a double-failure scenario: resetting two cards in a protection group. Wait until the first card completes its reset sequence before resetting the second card to prevent this problem. Configuring cards in 1:1 instead of 1:N protection should also avoid the problem. This issue will not be resolved.

## DWDM Cards

### DDTS # CSCeg42512

Occasionally, jumbo packets are not counted in the Performance Monitoring tab for the TXP-MR-10E. This issue can occur with Ethernet traffic running on a TXP-MR-10E, where the trunk side of the card is set up for 10E LAN with G.709 and FEC. JUMBO packets (2500 bytes) flow through the client port, but the oversized packet counter is not incremented. This is a hardware issue that cannot be resolved.

### DDTS # CSCei04981, CSCeg42532

The ifInErrorBytePkts counter for TXP-MR10-E cards running Ethernet traffic might fail to report negative or inconsistent numbers. This issue will be resolved in a future release.

### DDTS # CSCei64727

The GFP-CSF alarm might oscillate on the MXP-MR-2.5G card. This issue can occur when you have two MXP-MR-2.5G cards connected back to back, and you generate either a loss of signal, or a loss of sync at the near end client receive port. This should result in a GFP-CSF alarm at the far end for the duration of the condition; however, the GFP-CSF alarm is intermittently raised and cleared.

Although this issue has been seen predominantly in a Y cable protected configuration, it can also occur in an unprotected configuration, with any payload type. In a Y cable configuration with Distance Extension on, this issue is easily reproducible and continuous protection switches can occur due to the oscillating alarm. This issue will be resolved in a future release.

### DDTS # CSCuk56009

Connecting client ports of two TXP-MR-10E boards in termination mode, MS-EOC Multiplex Section Termination Failure alarms are present. This can occur when ETSI TXP-MR-10E boards are configured in Terminated mode (Multiplex Section). The client ports of one transponder are connected to the clients ports of the other transponder, and the LDCC is set on the client ports. The MS-EOC Multiplex Section Termination Failure alarms do not clear on both client ports. This issue will be resolved in a future release.

### DDTS # CSCuk56210

If, on a TXP-MR-10E card client port, the “synch msg” option is deselected (SSM-OFF) and then reselected, the message synchronization remains OFF. This can occur when you have two TXP-MR-10E cards connected via their trunk ports, the client port is the timing source for the node, and Synch messages are ON. When Synch messages are turned off from CTC, and then ON, the SSM-OFF message remains. To recover from this issue perform a software reset of the affected card. This is non-traffic affecting. This issue will be resolved in a future release.

## DDTS # CSCuk56032

Facility Loopback on a TXP-MR-10E trunk port can cause a traffic outage. This can occur when you have two TXP-MR-10E cards on two ETSI systems connected to each other on trunk ports, with running traffic, and a GCC is created, then a Facility (LINE) loopback is set on the Trunk port of one TXPs. Traffic goes down permanently and the following conditions are reported by the transponder where the loopback has been set:

- ODUK-OCI-PM, NR, ODUk: Open Connection Indication
- PTIM, NR, Payload Type Identifier Mismatch
- OTUK-IAE, MN, OTUk: Incoming Alignment Error

The other transponder raises following alarms:

- OTUK-LOF: OTUk Loss Of Frame
- GCC-EOC: GCC Termination Failure.

Releasing the Facility loopback restores the original situation with traffic running fine. This issue will be resolved in a future release.

## DDTS # CSCef15415

RMON TCAs are not raised on the TXPP\_MR\_2.5G client port after a hardware reset. To see this issue, provision two nodes with TXPP\_MR\_2.5G (TXP-1 and TXP-2) as follows.

- 
- Step 1** Connect the TXP-1 DWDM-A trunk to the TXP-2 DWDM-A trunk.
  - Step 2** Connect the TXP-1 DWDM-B trunk to the TXP-2 DWDM-B trunk.
  - Step 3** Create an external fiber loopback on the TXP-1 client.
  - Step 4** Connect the TXP-2 client to a traffic generator.
  - Step 5** Provision 1G FC payload on the TXP-1 and TXP-2.
  - Step 6** Ensure that traffic is running smoothly.
  - Step 7** Provision RMON thresholds using TL1 for all TXPP\_MR\_2.5G ports (client and trunks).
  - Step 8** Apply a hardware reset to the TXPP\_MR\_2.5G.
- 

After the card reboots, only DWDM-A and DWDM-B (trunk) port RMON TCAs are raised in the CTC History pane. RMON TCAs for port 1 (client) are not raised. This issue will not be resolved.

## DDTS # CSCef15452

RMON TCAs are not raised when the RMON history is cleared on TXPP\_MR\_2.5G card. To see this issue, provision two nodes with TXPP\_MR\_2.5G (TXP-1 and TXP-2) as follows.

- 
- Step 1** Connect the TXP-1 DWDM-A trunk to the TXP-2 DWDM-A trunk.
  - Step 2** Connect the TXP-1 DWDM-B trunk to the TXP-2 DWDM-B trunk.
  - Step 3** Create an external fiber loopback on the TXP-1 client.
  - Step 4** Connect the TXP-2 client to a traffic generator.

- Step 5** Provision 1G FC payload on the TXP-1 and TXP-2.
- Step 6** Ensure that traffic is running smoothly.
- Step 7** Provision RMON thresholds using TL1 for all TXPP\_MR\_2.5G ports (client and trunks).
- Step 8** While the traffic is running reset the RMON history by clicking the Clear button in the CTC Payload PM pane.

---

RMON TCAs are not raised for any port. This issue will not be resolved.

## DDTS # CSCef50726

Receive client fiber removal can cause a switch from the protect to the active in a TXPP\_MR\_2.5G. To see this issue, perform the following steps.

- 
- Step 1** Set up two nodes with TXPP\_MR\_2.5G (call the nodes TXP-1 and TXP-2).
  - Step 2** Ensure that TXP-1 DWDM-A trunk is connected to TXP-2 DWDM-A trunk with a 100 Km span.
  - Step 3** Ensure that TXP-1 DWDM-B trunk is connected to TXP-2 DWDM-B trunk with a 0 Km span.
  - Step 4** Ensure that TXP-1 client has an external fiber loopback.
  - Step 5** Connect the TXP-2 client to a traffic generator.
  - Step 6** Provision TXP-1 and TXP-2 with FICON 1G payload.
  - Step 7** Ensure that traffic is running smoothly on the protected span.
  - Step 8** Remove the receive client fiber at the near end.
- 

This causes the far end trunk to switch from protect to working span. Similarly, removal of the receive Client fiber at far end causes the near end trunk to switch from the protect to the working span. (Note that the traffic is already lost due to the receive client fiber pull.) To work around this issue, manually switch via CTC from the working to the protect span. This issue will not be resolved.

## DDTS # CSCef13304

Incorrect ALS initiation causes a traffic outage on an FC payload. This issue can be seen by performing the following steps.

- 
- Step 1** Set up two nodes with TXPP\_MR\_2.5G (call these nodes TXP-1 and TXP-2).
  - Step 2** Connect the TXP-1 DWDM-A trunk to the TXP-2 DWDM-A trunk.
  - Step 3** Connect the TXP-1 DWDM-B trunk to the TXP-2 DWDM-B trunk.
  - Step 4** Provision the TXP-1 client with an external fiber loopback.
  - Step 5** Connect the TXP-2 client to a traffic generator.
  - Step 6** Ensure that TXP-1 and TXP-2 have 1G FC payload provisioned.
  - Step 7** Enable ALS on TXP-1 trunk port and set it to “Manual Restart.”
  - Step 8** When traffic is running, remove the receive and transmit fibers on TXP1 port 1 (client). Traffic goes down and shutdown on TXP-1 port 2 (trunk) displays “No.”

**Step 9** Reconnect the fibers for TXP-1 port 1 (client).

---

ALS is now initiated on TXP-1 port 2 (trunk) and the laser shuts down. Traffic never comes back.



**Note** This issue is restricted to the TXPP\_MR\_2.5G card.

---

To recover from this situation, perform a manual restart or disable the ALS in this configuration. This issue will not be resolved.

## DDTS # CSCuk51184

When downloading Release 4.7 to nodes with Release 4.6 installed, The 15454-32MUX-O and 15454-32DMX-O report an AWG Temperature fail low alarm that subsequently clears. This also occurs when downgrading from Release 4.7 to Release 4.6, where the AWG Temperature alarm fail is high. This issue cannot be resolved.

## DDTS # CSCec22885

AS-MT is not enabled in Port 3 when a loopback is applied. To see this issue, on the TXPP card, make the following 3 changes before clicking Apply:

---

- Step 1** Change Port 2 to OOS-MT from IS.
  - Step 2** Change Port 3 to OOS-MT from IS.
  - Step 3** Change Port 2 to facility or terminal loopback.
- 

Now, when you click Apply, CTC issues the error message: "Error applying changes to row2 peer trunk port must not be IS." Port 3 is still IS and the loopback changes are not applied. You must place Port 3 in the OOS-MT state, apply the changes, and then change the loopback to recover.

This error occurs only when all three of the above changes are attempted at the same time.

To avoid this issue, first change both the trunk ports to OOS-MT, click Apply, and then place port 2 in loopback and click Apply again. This issue will not be resolved.

## DDTS # CSCed76821

With Y-cable provisioned for MXP-MR-2.5G cards, if you remove the client receive fiber on one side, the far end takes greater than 100 ms to switch away from the affected card. It is not known or has not been determined when or if this issue will be resolved.

## DDTS # CSCef44939

Under certain conditions you may be unable to provision an Express Order Wire (EOW) circuit using an MXP\_2.5G\_10G or TXP\_MR\_10G card trunk port. This can occur as follows.

---

- Step 1** Provision an MXP\_2.5G\_10G or TXP\_MR\_10G card within a node.

- Step 2** Disable OTN.
  - Step 3** Provision DCC on both client and trunk ports.
  - Step 4** Go to the Network view **Provisioning > Overhead Circuits** tab.
- 

During the EOW circuit provisioning only the MXP/TXP client ports are listed for the selection. This issue will not be resolved.

### **DDTS # CSCuk51185**

After a soft reset of an OSCM or OSC-CSM card, a CONTBUS-IO alarm is raised. This issue will not be resolved.

### **DDTS # CSCuk50144**

Neither E1 nor E2 circuits are available for EOW circuits on TXP\_MR\_2.5 TXT in Section and Line Termination mode. This issue will be resolved in a future release.

### **DDTS # CSCee45443**

When the FICON bridge does not receive the expected number of idle frames between data packets it will transition to SERV MODE. The MXP-MR-2.5G should not be used in scenarios where there is a FICON Bridge in place. This issue will be resolved in a future release.

### **DDTS # CSCec40684**

After a database restore TXPP trunk ports might report SF, resulting in a traffic outage. The SF occurs when you restore the database and then put the port OOS for DWDM cards; then the operating mode in the database is different from the current operating mode. To avoid this issue, either put the DWDM port OOS before restore the database, or, after restoring the database, reset the DWDM cards. This issue will not be resolved.

### **DDTS # CSCec51270**

Far end traffic does not switch in line termination mode with .G709 off. This can occur with non-revertive Y-cable, and DCC enabled, under certain specific conditions. To avoid this issue, turn on .G709 when in line mode. This issue will not be resolved.

### **DDTS # CSCuk42668**

TXP-MR-2.5G F1-UDC may not be passed through in a line-terminated configuration with OTN off. This can occur with clean, OC-3/STM-1, line-terminated traffic, with OTN disabled, when you create a D1-D3 tunnel, a D4-D12 tunnel, and an F1-UDC from client to client. This issue will not be resolved.

## DDTS # CSCuk42752

If you go to the Overhead Circuits Tab in network view and select any User Data, F1 or User Data D4-D12 circuit type, no nXP cards are available for selection in the Endpoints. However, user Data type circuits can still be made end-to-end (where “end-to-end” refers to external cards, such as AIC to AIC) if the nXP cards are put in Transparent mode. This issue will not be resolved.

## DDTS # CSCeb49422

With TXPP cards, a traffic loss up to six seconds can occur during a DWDM protection switch. This behavior may be exhibited during protection switches by certain third-party fiber channel switches due to loss of buffer credits resulting in a reconvergence of the fiber channel link. This issue will not be resolved.

## DDTS # CSCeb53044

The 2G Fiber Channel (FC) payload data type in the TXP\_MR\_2.5G and TXPP\_MR\_2.5G cards does not support any 8B/10B Payload PM monitoring. This is by design.

## DDTS # CSCeb32065

Once engaged, the ALR will not restart on the trunk lines of a TXP or TXPP card. This occurs whenever ALR engages on the trunk lines of a TXP or TXPP card and the recover pulse width is provisioned to less than 40 seconds. This is a function of the trunk laser turn-on time, and the limiting recovery pulse width will vary by card. To avoid this issue, provision the pulse width to 40 seconds or more.

## DDTS # CSCeb37346

Near end and far end PMs might increment simultaneously on TXPP-2.5G cards. This can occur when two nodes have TXPP-2.5G cards and two nodes have STM16 cards in a four node network, where both TXPP-2.5G cards have STM16 SFPs on them, and are in MS (Line Termination) mode. By default, the TXPP-2.5G cards are in Splitter protection: the first DWDM port is working and the second is protect. If you remove the receive fiber of the first DWDM port on one TXPP-2.5G card, both near and far end counts begin to increment. The far end counts should not increment in this case. This issue is seen only when the Txpd cards have G709 and FEC on. If the cards have G709 and FEC off, only the near end counts will increment, as expected.

## DDTS # CSCeb26662 and CSCea88023

With TXP-MR-2.5G cards, when the current 1 day Optics PM rolls over, the information is inaccurate. This issue will not be resolved.

## DDTS # CSCuk42588

With ALS mode configured as “Auto Restart” or “Manual Restart,” it is possible the ALS Pulse Duration Recovery time can be set to values out of ITU-T recommendation G.664. You can use values out of the range defined in ITU-T recommendation G.664 only in order to interoperate with equipment that lasers cannot turn on or off within the required pulse time. To stay within the specification, you can set this value to 2 seconds and up to 2.25 seconds.

## DDTS # CSCea81219

On the TXPP, the default value for Tx Power High for TCAs & Alarms is too high for the trunk ports. Since Tx Power TCA and Alarm are not supported for trunk ports, this caveat is for informational purposes only.

## DDTS # CSCeb24815

With TXP-MR-2.5G cards, ratios are calculated incorrectly after clearing statistics. This is because after you clear statistics the entire time period becomes invalid. Once the time period rolls over again, values will be reliable for the new period.

## DDTS # CSCeb27187

During a Y-Cable protection switch, the client interface sends 200,000 to 300,000 8B/10B errors towards the attached Catalyst 3550 switch. The switch reacts to this large amount of 8B/10B errors by reinitializing the interface and spanning tree. The end result is that a protection switch can lead to a 30-45 second traffic hit if the switch is running spanning tree (default mode). This is expected behavior.

## DDTS # CSCea87290

In a Y-Cable protection group, if GCCs are defined on both cards, both cards' active LEDs will be green.

## DDTS # CSCeb12609

For the TXPP, attenuating Port 2 Rx signal, SD, and SF alarms are not declared before LOC is raised. This is due to the intrinsic design of the optical interface, which allows required BER performances with dispersion and OSNR penalties.

This can occur when Port 2 is in back to back or has low dispersions and high OSNR.

## DDTS # CSCea68773

The ACTV/STBY LED shows AMBER when a 2.5G transponder is first connected. The DWDM cards introduced a new design: When all the ports are OOS on a card, the card is considered to be in standby mode.

## Data IO Cards

### DDTS # CSCeg90341

A greater than 2 second traffic hit can occur with 255 subinterfaces on DRPRI. This issue can occur when the GEC member interface is shut/fiber-pull. This issue will be resolved in Release 6.0.

## DDTS # CSCeg86115

When traffic is switched from one GEC member to the other GEC member in a DRPRI node, the traffic hits could be between 400 ms and 2 seconds. This issue can occur when one of the GEC member interfaces goes down. This issue will be resolved in Release 6.0.

## DDTS # CSCeg87785

A greater than 200 ms traffic hit can occur when an active DRPRI node is reset. This issue can occur with a soft or hard reset of ML1000 in a DRPRI setup. For manual resets, shut down the Gig ports before issuing reload to avoid this issue. This issue will be resolved in Release 6.0.

## DDTS # CSCeh06954

When multicast/flood traffic is added to a ring and the ring wraps on the node where the traffic is added, ML Series RPR convergence times might be greater than 50 ms. This issue will be resolved in Release 6.0.

## DDTS # CSCef46191

A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) might block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

All other device services will operate normally.

The detail advisory is available at:

<http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml>

## DDTS # CSCeg15044

IOS does not allow telnet connections when there are simultaneous Telnet requests, even though there might be unused tty lines available. If this issue occurs, a “No Free TTYs error” message is displayed. This issue will be resolved in a future release.

## SONET and SDH Card Compatibility

Tables 2, 3, and 4 list the cards that are compatible for the ONS 15454 SONET and ONS 15454 SDH platforms. All other cards are platform specific.

**Table 2** *SDH Data Cards that are SONET Compatible*

Product Name	Description
15454E-G1000-4	4 port Gigabit Ethernet Module - need GBICs
15454E-E100T-12	12 port 10/100BT Ethernet Module
15454E-E1000-2	2 port Gigabit Ethernet Module - need GBICs

**Table 2 SDH Data Cards that are SONET Compatible (Continued)**

Product Name	Description
15454E-ML100T-12	10/100 Mbps Ethernet card, 12 ports, RJ-45, L2/L3 switching, SDH/ETSI system, includes console cable
15454E-ML1000-2	1000 Mbps Ethernet card, 2 SFP slots, L2/L3 switching, SDH/ETSI system

**Table 3 SONET Data Cards that are SDH Compatible**

Product Name	Description
15454-G1000-4	4 Port Gigabit Ethernet
15454-E100T-G	10/100BT, 12 circuit, compatible w/ XC, XCVT and XC10G
15454-E1000-2-G	Gigabit Ethernet, 2 circuit, GBIC - G
15454-ML100T-12	10/100 Mbps Ethernet card, 12 ports, RJ-45, L2/L3 switching, SONET/ANSI system, includes console cable
15454-ML1000-2	1000 Mbps Ethernet card, 2 SFP slots, L2/L3 switching, SONET/ANSI system

**Table 4 Miscellaneous Compatible Products**

Product Name	Description
15454-BLANK	Empty slot Filler Panel
15454-GBIC-LX	1000Base-LX, SM or MM, standardized for 15454/327
15454-GBIC-SX	1000Base-SX, MM, standardized for 15454/327
15454-FIBER-BOOT=	Bag of 15 90 degree fiber retention boots
15454-SFP-LC-SX	1000BASE, SX, short-reach, multimode, small form factor pluggable (SFP), LC connectors
15454-SFP-LC-LX	1000BASE, LX, long-reach, single mode, SFP, LC connectors
15454-CONSOLE-02	Cable, console, ML-Series, RJ-11 plug to RJ-45 jack, 22in/55.9cm long, SONET/ANSI system
15454E-CONSOLE-02	Cable, console, ML-Series, RJ-11 plug to RJ-45 jack, 22in/55.9cm long, SDH/ETSI system

**E1000-2/E100T**

Do not use the repair circuit option with provisioned stitched Ethernet circuits. It is not known at this time when or if this issue will be resolved.

## Single-card EtherSwitch

Each E100/E1000 card can be configured as a single-card EtherSwitch configuration to allow VC4-4c of bandwidth to be dropped at each card. The following scenarios for provisioning are available:

VC4-4c

VC4-2c, VC4-2c

VC4-2c, VC4, VC4

VC4, VC4, VC4, VC4

When configuring scenario 3, the VC4-2c must be provisioned before either of the VC4 circuits.

## Multicard EtherSwitch

When deleting and recreating Ethernet circuits that have different sizes, you must delete all VC4 circuits provisioned to the EtherSwitch before you create the new circuit scenario. (See the preceding “Single-card EtherSwitch” section on page 6 for details on the proper order of circuit creation.) Enable front ports so that the VLANs for the ports are carried by the largest circuit first. A safe approach is to enable the front port before you create any circuits and then retain the front port VLAN assignment afterwards. If you break the rules when creating a circuit, or if you have to delete circuits and recreate them again, delete all circuits and start over with the largest first.

## DDTS # CSCeg30605

The diagnostics information provided for ML cards in the diagnostic file is incomplete. This issue will be resolved in a future release.

## DDTS # CSCed96068

If an ML-Series card running Software Release 4.6.2 or later is interoperating with an ML-Series card running Software Release 4.6.0 or 4.6.1, then the `pos vcat resequence disable` command must be added to the configuration of the ML-Series card running R4.6.2 or later.

## DDTS # CSCec52443

On an ML-series RPR ring circuit deletion or creation causes an approximately 200 ms traffic loss. Traffic loss is expected to be less than 50 ms for RPR. To avoid this issue, from the ML-series CLI, perform a “shutdown” on both ends of the circuit prior to circuit changes. This issue will not be resolved.

## DDTS # CSCec52372

You must issue a “shut” command to both ends of a POS circuit before placing the circuit OOS, and issue IS before a “no shut” command. Placing a POS circuit OOS without shutting down can cause long traffic hits. This issue will not be resolved.

## DDTS # CSCec51252

You must issue a “shut” on both ends of affected POS circuits before performing a maintenance action on those circuits. If a POS circuit is restored without first issuing the shut commands, traffic loss is greater than 50 ms. When a maintenance action is taken, one end of the circuits could come up before the other. During that time, traffic is lost because the other end is not up yet. This issue will not be resolved.

## DDTS # CSCeb25778

When a MAC-SA is seen for the first time, it is learned, but may age out in less than 5 minutes. If the same MAC-SA is seen again before the first ages out, the entry will age out after 5 minutes, as expected. This issue will not be resolved.

## DDTS # CSCin43669

Timer expiration can cause a system crash when you attempt to remove 250 Shared Packet Ring (SPR) subinterfaces using the “no int spr1” command, while Cisco Discovery Protocol (CDP) is also enabled. To avoid this issue, either turn off CDP, issue the command, and then turn CDP back on; or remove the SPR subinterfaces explicitly. This issue will not be resolved.

## DDTS # CSCea36829

The broadcast packet count is always 0 for the SPR interface. The ML100 and ML1000 hardware does not support counting broadcast packets. This issue will not be resolved.

## DDTS # CSCeb21996

When the POS interface is removed from SPR due to a defect, while SPR is configured in immediate mode, the defect type may not be reported. This only occurs if the defect is set and clears in less than 50 ms.

## DDTS # CSCdz49700

ML-series cards do not appear in the Cisco Discovery Protocol (CDP) adjacencies and do not participate in the Spanning-Tree Protocol. All packets are counted as multicast.

The ML-series cards always forward Dynamic Trunking protocol (DTP) packets between connected devices. If DTP is enabled on connected devices (which might be the default), DTP might negotiate parameters, such as ISL, that are not supported by the ML-series cards. All packets on a link negotiated to use ISL are always counted as multicast packets by the ML-series card, and STP and CDP packets are bridged between connected devices using ISL without being processed. To avoid this issue, disable DTP and ISL on connected devices. This functionality is as designed.

## DDTS # CSCdz68649

Under certain conditions, the flow-control status may indicate that flow control is functioning, when it is not. Flow-control on the ML-series cards only functions when a port-level policer is configured. A port-level policer is a policer on the default and only class of an input policy-map. Flow-control also only functions to limit the source rate to the configured policer discard rate, it does not prevent packet discards due to output queue congestion.

Therefore, if a port-level policer is not configured, or if output queue congestion is occurring, policing does not function. However, it might still mistakenly display as enabled under these conditions. To avoid this issue, configure a port-level policer and prevent output queue congestion. This issue will not be resolved.

## DDTS # CSCdz69700

Issuing a **shutdown/no shutdown** command sequence on an ML1000 port clears the counters. This is a normal part of the startup process and there are no plans to change this functionality.

## DDTS # CSCea01675

Packets without an 802.1q VLAN tag are classified as COS 0. This issue will not be resolved.

## DDTS # CSCin29274

When configuring the same static route over two or more interfaces, use the following command:

```
ip route a-prefix a-networkmask a.b.c.d
```

Where *a.b.c.d* is the address of the outgoing gateway, or, similarly, use the command:

```
ip route vrf vrf-name
```

Do not try to configure this type of static route using only the interface instead of the address of the outgoing gateway. This issue will be resolved in a future release.

## DDTS # CSCin32057

If no BGP session comes up when VPN Routing/Forwarding (VRF) is configured and all interfaces have VRF enabled ensure that at least one IP interface (without VRF) is configured and add an IP loopback interface on each node.

## DDTS # CSCdy55437

The maximum MAC Address Learn Rate for the ML-Series cards is 1300 MAC addresses per second. This number varies based on the ML-Series control and forwarding plane loads. If the forwarding and control planes are heavily loaded, the maximum MAC Address Learn Rate could be as low as 100 MAC addresses per second. To correct a situation where an ML-Series card has stopped learning MAC addresses, reduce the load on these cards. This load limit is by design.

## DDTS # CSCdy47284

Oversize frames are not supported on ML100 Fast Ethernet ports. Oversize frames cause egress traffic to incur CRC, line, and fragment errors on these ports. To avoid this issue, do not send jumbo packets to ML far end ports. This is as designed.

## Alarms

### DDTS # CSCed28167

When a VC\_LOW\_PATH\_TUNNEL only contains unidirectional circuits, an AU-LOP critical alarm is raised. This can occur when a bidirectional tunnel goes through at least three nodes, and the AU-LOP alarm is shown on the intermediate node on the direction not used. Tunnels are bidirectional. If a tunnel does not have traffic in both directions, it will be alarmed. The alarm will be cleared when a bidirectional circuit is added to the tunnel. This issue will be resolved in a future release.

### DDTS # CSCef63240

Rarely, an LP TIM alarm displays its severity as NR instead of MJ in CTC. This can occur when a VC3 circuit is created on Port 5 and IO has detected a VC4 PLM alarm. This issue will be resolved in a future release.

### DDTS # CSCee29901

A CARLOSS alarm can take up to 3 minutes to be reported depend of the number of VLANs configured on a node. When the alarm does appear, if you clear this major alarm, the severity changes to minor, but then the alarm disappears. The alarm severity change behavior will not be changed.

## MS-SPRing Functionality

### DDTS # CSCeh08553

A two-fiber MS-SPRing protection switch generates an AU-LOP alarm on a one way VC12 circuit. This issue will be resolved in a future release.

### DDTS # CSCee65471

Rarely, during a software upgrade of a passthrough node in an MS-SPRing, the VC3 traffic on a DS3I card might incur a traffic hit. This issue will be resolved in a future release.

### DDTS # CSCeg39930

An IDRI circuit shows up as unprotected if the circuit is manually routed, but you choose the wrong path first and then correct it when CTC displays an error message saying the path is not valid. To recover from this situation, restart your CTC session. This issue will be resolved in a future release.

## DDTS # CSCee65471

Rarely, during software upgrade of passthrough node in MS-SPRing, the VC3 traffic on a DS3I card might incur a hit. This issue will be resolved in a future release.

## DDTS # CSCdz66275

When creating a MS-SPRing from the network view, the node default values for reversion are not initially used. To see this, starting with no preferences file, log into a node with CTC, and set the node default values for MS-SPRing reversion. Now, in Network view, use the MS-SPRing wizard to create a MS-SPRing. The node level default values are initially ignored while the wizard is still in operation. If you encounter this issue, you may need to change values as appropriate for your network while you are still using the MS-SPRing wizard. Once the wizard is finished, these values are saved to a preferences file and will be used henceforth. This issue will not be resolved.

## DDTS # CSCdw53481

Two MS-Rs are not allowed to coexist. If you execute a manual ring switch command on one side of an MS-SPRing node and apply another manual ring switch command on other side of the node, the second manual ring switch command is rejected. This works as designed. The implementation complies with Telcordia GR-1230, R6-102.

## DDTS # CSCdx45851

On a four fiber MS-SPRing, restoring the database for all nodes at the same time could cause VC4-16c traffic to fail to switch. Do not restore the database for multiple nodes simultaneously. The proper procedure for restoring the database for multiple nodes is to restore one node at a time. This procedure is documented in the user documentation.

## DDTS # CSCdx19598

A rare hardware failure on an STM16AS card transmitter can trigger SEF on the receiving STM16AS card in a four fiber MS-SPRing (or BLSR) configuration. The BER calculations are suspended when SEF is detected, so SD or SF is never raised. Likewise SEF is not considered a signal failure condition like LOS or LOF, so a protection switch will not occur. If this occurs, use the CTC GUI to force a protection switch on the MS-SPRing (or BLSR). This issue will not be resolved.

## DDTS # CSCdv53427

In a two ring, two fiber MS-SPRing (or BLSR) configuration (or a two ring MS-SPRing or BLSR configuration with one two fiber and one four fiber ring) it is possible to provision a circuit that begins on one ring, crosses to a second ring, and returns to the original ring. Such a circuit can have protection vulnerabilities if one of the common nodes is isolated, or if a ring is segmented in such a way that two non-contiguous segments of the circuit on the same ring are each broken. There are two possible workarounds for this issue:

1. Manually route the circuit to avoid the “one circuit over two ring” routing scenario.
2. When routing the circuit automatically, select the Using Required Nodes/Spans option in the Circuit Routing Preference screen, then select the appropriate spans to avoid the “one circuit over two ring” routing scenario.

This issue will be resolved in a future release.

## Database Restore on an MS-SPRing

When restoring the database on an MS-SPRing, follow these steps:

- 
- Step 1** To isolate the failed node, issue a force switch toward the failure node from the adjacent east and west nodes.
  - Step 2** If more than one node has failed, restore the database one node at a time.
  - Step 3** After the TCC2/TCC2P has reset and booted up, ensure that the “MS-SPRing Multi-Node Table update completed” event has occurred for all nodes in the ring.
  - Step 4** Release the force switch from each node.
- 

## SNCP Functionality

### DDTS # CSCeh28924

E3/DS3i PortGroup traffic fails to switch after upgrading from Unprotected to SNCP. This issue can occur anytime when the port group is upgraded from Unprotect to SNCP. To work around this issue the protected circuit can be created from the beginning instead of attempting to upgrade to SNCP from unprotected. This issue will be resolved in Release 6.0.

### DDTS # CSCee53579

Traffic hits can occur in an unprotected to SNCP topology upgrade in unidirectional routing. If you create an unprotected circuit, then upgrade the unprotected circuit to a SNCP circuit using Unprotected to SNCP wizard, selecting unidirectional routing in the wizard, the circuit will be upgraded to a SNCP circuit. However, during the conversion, traffic hits on the order of 300 ms should be expected. This issue will be resolved in a future release.

### DDTS # CSCec15064

A path protection/SNCP circuit with a defect signal present (for example, AIS-P or AIS-V) on the protect path will produce RDI-P or RDI-V upstream of the detection point, but these signals will not be detected or indicated. This issue will be resolved in a future release.

### DDTS # CSCeb37707

With a VT SNCP circuit, if you inject signals with a thru-mode test set into one path of the circuit in a particular order, you may not see the appropriate alarms. This can occur when you first inject LOP-P, then clear, then inject LOP-V. This issue will be resolved in Release 6.0.

## Active XCVXL or TCC2/TCC2P Card Removal

As in MS-SPRing and 1+1, you must perform a lockout on SNCP before removing an active cross connect or TCC2/TCC2P card. The following rules apply to SNCP.

Active XCVXL cards should not generally be physically removed. If the active cross connect or TCC2/TCC2P card must be removed, you can first perform an XCVXL side switch or TCC2/TCC2P reset and then remove the card once it is in standby, or you can perform a lockout on all circuits that originate from the node whose active cross connect card or active TCC2/TCC2P will be removed (performing a lockout on all spans will also accomplish the same goal). No lockout is necessary for switches initiated through CTC or through TL1.

## Performance Monitoring

### DDTS # CSCef28522

When you inject errors on a splitter protection card in the node's working port, CVL and ESL are incremented for the working and protect far end ports. This issue will not be resolved.

## Online Help

### DDTS # CSCeg63382

When you have never previously installed the online user manuals on your workstation (PC or UNIX) and you click the Help > User Manuals menu in CTC, there is no error message instructing you to install the online manuals. You must install the online help from the software or documentation CD prior to selecting it from the menu. An error message for the case in which the help is not installed will be provided in a future release.

## Resolved Caveats for Release 5.0.4

This section highlights resolved caveats for Release 5.0.x. Resolved caveats for DWDM Release 4.7 are also included.

## Maintenance and Administration

### DDTS # CSCeg67387

You cannot create a VC3 circuit after creating the maximum number of VC12 circuits. This issue is resolved in Release 5.0.2.

**DDTS # CSCeg44049**

Empty tunnels might be created while creating PCA VT circuits using routing constraints and preference to create tunnels (you will see multiple alarms, some of which might fail to clear, associated with the tunnel, which by their presence indicate the tunnel's existence). If an empty tunnel is inadvertently created, delete it. This issue is resolved in Release 5.0.2.

**DDTS # CSCef70730**

An AICI user data D4-D12 (DCC) overhead circuit might not pass data correctly. This can occur for both AICI DCC-A and DCC-B circuits. Though CTC indicates the circuit is established correctly, the underlying overhead timeslot connections are not set properly for the user data D4-D12 (DCC) overhead circuits. This issue does not occur with user data F1 (UDC) overhead circuits, however, for which timeslots are set and the circuit behaves correctly. This issue is resolved in Release 5.0.2.

**DDTS # CSCeg23728**

On a path protection(SNCP) DRI configuration, if you create circuits to consume the complete bandwidth of the DRI omni-spans, then create a new VC12 circuit with DRI protection using autorouting, circuit creation fails, but an empty VC12-Tunnel is created, which raises Critical AU-LOP alarms. To correct this, delete the empty tunnel raising alarms. This issue is resolved in Release 5.0.2.

**DDTS # CSCef18649**

LDCC and MS-DCC do not work at OC12/STM4 line rates (client and trunk side). Use SDCC or RS-DCC (D1..D3) at OC12/STM4 line rates. This issue is resolved in Release 5.0.1.

**DDTS # CSCef47990**

Certain PM values are not displayed in CTC. In particular, if you perform an FC link down and up and observe FC LinkRecovery counts, the count will not appear to increase. This issue is resolved in Release 5.0.

**DDTS # CSCef57989**

Invalid idles are transmitted in a splitter switch. To see this issue perform the following steps.

- 
- Step 1** Set up two MXPP cards connected to each other.
  - Step 2** Provision the client port as FICON ISL 1G with DE on and Auto detect credit on.
  - Step 3** Connect the client port to an MDS switch.
  - Step 4** Provision a manual switch.
- 

NOS is transmitted by both MXPPs and OLS is received by these cards from the MDS at both ends. However, then the MXPP sends some invalid idles. This issue is resolved in Release 5.0.

**DDTS # CSCuk52914**

Reports of the ports regulated by APC contain some useless ports. The wrong ports are the Channel RX ports of MUX, WSS and AD-xC boards. The behavior is common to the CTC and TL1 interfaces. A MUX, WSS, or AD-xC board must be present in the system and a circuit be provisioned passing through them to see this issue. This issue is resolved in Release 5.0.

**DDTS # CSCuk53088**

A splitter protect group might incur a double switch when the protect trunk port is placed in service. The double switch will occur if the working trunk port is already in service and is currently incurring alarms or defects. When the protect trunk is placed in service it will become active. If there are any defects on the trunk (for example, no receive signal) the splitter will immediately switch back to working.

**Note**


---

The double switch will not occur if the working port is error-free.

---

Apply a FORCE-TO-WORKING or a LOCKOUT-OF-PROTECT switch command before placing the protect trunk in service to avoid this issue. This issue is resolved in Release 5.0.

**DDTS # CSCef53655**

When importing an NE default file, errors are raised for the following defaults.

- FC-MR.config.port.distanceExtension.NumGFPBuffers
- MXP-MR-2\_5G.config.fc.distanceExtension.NumGFPBuffers

. This issue is resolved in Release 5.0.

**DDTS # CSCea78364**

Simultaneous failure of working and protect cards in 1:N protection groups may not be alarmed as service affecting. This can occur when the working card of the protection group has been removed from the chassis, and the protect card of the protection group is subsequently issued a Manual Reset. Since the working and protect facilities are impaired, the Improper removal alarm should clear and be reissued as a Critical and service affecting condition. This issue is resolved in Release 5.0.

**DDTS # CSCee39968**

The Timing Report in the Maintenance window of CTC fails to update the report of a new timing failure after a previous reference has failed. For example, if you inject LOS and then switch to injecting LOF, the Timing Report fails to display the LOF against the reference, or only displays the failure briefly, upon clearing. This issue is resolved in Release 5.0.

**DDTS # CSCed27389**

Under certain conditions, you cannot unlock a cross-connect from CTC and TL1. If you lock a cross-connect, then quickly click the SWITCH button, the Clear is sent only to the protect XC side. This causes the Unlock command to fail. This issue is resolved in Release 5.0.

**DDTS # CSCec17281**

When the “Status” field for a circuit in the circuit table shows “INCOMPLETE,” this can be interpreted as an alarm or traffic-affecting condition on the circuit. On SNCP and MS-SPRing circuits, a circuit is shown as INCOMPLETE if either the working or protect path is missing a network span or connection, even if traffic is flowing without error on the other, redundant path. This can lead to confusion, since the meaning of “INCOMPLETE” is not well-defined. You can see this if you, for example, introduce LOS on a span in a MS-SPRing network such that traffic is switched to another path around the ring. Ignore the INCOMPLETE circuit status in such cases and instead look for any alarms in the network. This issue is resolved in Release 5.0. The circuit Status is defined more clearly in Release 5.0.

**DDTS # CSCec21668**

Do not create more than three VC3 or VC12 circuits in auto-range mode. The VC3 or VC12 circuits can be created in batches of three, or manually. When you create more than three VC3 or VC12 circuits in auto-range mode, CTC creates the first three circuits and then issues the error message:

“Exception: Source is not fully specified”

This can occur with an SDH node when you wish to create more than three VC3 or VC12 circuits in auto-range mode. This issue is resolved in Release 5.0.

**DDTS # CSCed27389**

In some instances, you might not be able to unlock a cross-connect from both CTC and TL1. After locking the cross-connects, if you quickly click the SWITCH button, the unlock command might fail. This issue is resolved in Release 5.0.

**DDTS # CSCef75019**

In the CTC node view **Provisioning > Security > Access** tabs, the option to enable SSH access instead of telnet does not function. This issue is resolved in Release 5.0.

**Common Control and Cross Connect Cards****DDTS # CSCei01183**

If near line rate traffic is addressed at a TCC+ or XTC shelf controller, so much CPU will be devoted to reading packets off the line that the card will intentionally reset itself. The time to reset will vary from minutes to hours depending on the Ethernet bus traffic load. If this issue occurs, you will see the node in CTC go gray, and the TCC+ or XTC reset. This failure has been reproduced by connecting an Ethernet switch to the working and protect shelf controllers and turning spanning tree off on the switch. Any broadcast traffic received in such a configuration will loop infinitely. This issue is resolved in maintenance Releases 4.0.4, 5.0.4 and later.

**DDTS # CSCei16460**

A common control card reset can occur under the following three conditions.

1. The node has OSPF enabled on the LAN and the DCC area comes up before the LAN area.

2. In the DCC area, there is at least one other node running OSPF in the same LAN area and this node is up in both the LAN and DCC area.
3. There is either a router with static routes configured and advertised by OSPF; or there is a node with LAN a connection, but OSPF is disabled.

This issue has been only seen in Release 5.0.2. To avoid this issue, disable OSPF on the LAN. This issue is resolved in Releases 5.0.4 and 5.0.5.

## DDTS # CSCeg48922

When removing a standby XCVXL card, if the card in the BLSR node has set the wrong KByte source, the span card sends out the wrong KBytes and causes MS-AIS to be raised on the trunk card of the adjacent node. Performing some other provisioning to the trunk card will correct the KByte source if this issue occurs. This issue is resolved in Release 5.0.2.

## DWDM Cards

### DDTS # CSCeh46305

An MEA alarm will be reported on an ESCON TXP-MR-2.5G card after a Release 4.6 to 5.0 upgrade. This can occur when a TXP-MR-2.5G card is equipped with ESCON SFP and Release 4.6.2. Perform an upgrade to Release 5.0, and after the upgrade, CTC reports an MEA on the client port SFP. To avoid this issue, prior to upgrading, demote the alarm severity in the profile. This issue is resolved in Releases 5.0.4 and 5.0.5.

### DDTS # CSCeg44632

Do not specify the PPM AID in INIT-SYS commands; rather, use the SLOT AID only. An INIT-SYS command addressing a PPM AID is not a supported feature, and causes reload of the entire card. You should not be able to initialize a pluggable module. This issue is resolved in Release 5.0.2.

### DDTS # CSCef22599

In Release 4.7 it is not possible to configure a Y-Cable protection group when DE is enabled. This issue is resolved in Release 5.0.

### DDTS # CSCuk52818

An unsupported state for the PPM module is reported when upgrading the software from Release 4.6.1 to 4.7. This can occur when you preprovision a TXP\_MR\_2.5G card using Release 4.6.1, insert in a different card in the preprovisioned slot, then activate to Release 4.7 from CTC. The PPM reports IS,AINS/OOS-AUMA,UAS&UEQ, which is not an allowed state. The correct state should be IS,AINS/OOS-AUMA,UEQ.

To recover from this incorrect state reporting, manually delete the PPM and recreate it. This issue is resolved in Release 5.0.

## DDTS # CSCef53322

The MXP\_2.5G\_10G Client fails to indicate a bad signal, or LOS. To see this issue, complete the following steps.

- 
- Step 1** Set up two ONS 15454 SDH nodes with STM16 SNCP (STM16-1 and STM16-2) (call the nodes STM16-1 and STM16-2).
  - Step 2** Set up two ONS 15454 SDH nodes with MXP\_MR\_2.5G\_10G (call the nodes MXP-1 and MXP-2).
  - Step 3** Place MXP-1 and MXP-2 in Transparent Termination Mode.
  - Step 4** Ensure that STM16-1 is connected to MXP-1 client 1.
  - Step 5** Ensure that STM16-2 is connected to MXP-2 client 1.
  - Step 6** Ensure that MXP-1 trunk is connected to MXP-2 trunk.
  - Step 7** In MXP-1, change MXP-1 MXP\_MR\_2.5G\_10G Client 1 and Trunk port states to
  - Step 8** UNLOCKED-AUTOMATIC-IN-SERVICE. Set the Automatic in Service Timer to 15 min for
  - Step 9** Client 1 and the Trunk port. CTC displays decrementing of the Automatic in Service Timer in node view > **Maintenance** > **AINS Soak** tab.
  - Step 10** Remove the receive fiber of both the Client 1 and Trunk ports. The trunk port Automatic in Service Timer indicates a Bad Signal.
- 

The client port Automatic in Service Timer continues to count and fails to indicate the Bad Signal even when not receiving any signal. After 15 minutes the client port changes its state to UNLOCKED. This issue is resolved in Release 5.0.

## DDTS # CSCef43317

For TXP-MR-2.5G cards, the LCD panel displays five wavelengths instead of four. The fifth wavelength is a duplicate of the fourth. This issue is resolved in Release 5.0.

## DDTS # CSCef37516

Port LEDs remains red with no alarms reported in the following scenario.

- 
- Step 1** For two nodes with TXP\_MR\_2.5G (TXP-1 and TXP-2):
  - Step 2** Connect the TXP-1 trunk to the TXP-2 trunk.
  - Step 3** Connect the TXP-1 and TXP-2 clients to a traffic generator.
  - Step 4** Provision STM16 payload for TXP-1 and TXP-2.
  - Step 5** Provision TXP-1 and TXP-2 in transparent mode with G.709 on.
  - Step 6** Enable Manual ALS for TXP-1 and TXP-2.
  - Step 7** Ensure that traffic is up and running.
  - Step 8** For TXP\_MR\_2.5G TXP-1 and TXP-2 nodes remove the Pluggable Port Modules (PPMs) and replace them with GIGE/FC PPMs.

- Step 9** Connect a traffic generator to the TXP\_MR\_2.5G TXP-1 client and loop back the TXP\_MR\_2.5G TXP-2 client with an external fiber.
  - Step 10** On the TXP\_MR\_2.5G TXP-1 node, set the client and trunk ports to OOS state.
  - Step 11** Using CTC, delete the STM16 PPM and provision a GIGE PPM payload.
  - Step 12** Set the client and trunk ports to IS state.
  - Step 13** Repeat the same operation on the TXP\_MR\_2.5G in the TXP-2 node.
- 

When you have completed these steps and traffic is up and running, CTC shows that there are no alarms or conditions, while the client and trunk LEDs are still red. To recover from this state, perform a hardware reset on the affected card. This issue is resolved in Release 5.0.

## DDTS # CSCed05006

In the Defaults pane, when you change the default ALS mode for the TXP/TXPP\_2.5G\_10G cards to “Manual Restart for Test,” CTC issues an error message. The mode can be successfully changed but you must click Reset to proceed with further changes to defaults. Changes to other defaults on that pane may have to be reapplied. To prevent the error, change the default pulse width at the same time as changing the default ALS mode to “Manual Restart for Test.” The default pulse width must be in the appropriate range for this mode (80-100). This issue is resolved in Release 4.7.

## DDTS # CSCec78443

You cannot provision an end-to-end circuit through a TXP regen group (a pair of transponders connected back to back via the client interface that provide for regeneration for DWDM) with G.709 on, and in line termination on the TXP cards, which are feeding traffic to the regen group. To avoid this issue turn G709 off for all TXPs. This issue is resolved in Release 4.7.

## DDTS # CSCeb25490

Occasionally CTC displays a LO-TXPOWER alarm when SMT4 and STM1 SFP is installed at the client port of a TXP or TXPP card. The LO-TXPOWER alarm is displayed when the alarm threshold is set to the default value in the TX POWER LOW field of the Optical Threshold in the CTC provisioning window. To work around this issue, lower the alarm threshold value (TX POWER LOW (dBm)) of Optical Threshold in the CTC provisioning window. This issue is resolved in Release 4.7.

## Optical IO Cards

### DDTS # CSCeg23427

From the STM1E (E4) card view > Provisioning > SDH Thresholds subtab, no CV appears to be available for the user to change the threshold value. This is because the threshold is actually shown as EB instead of CV. This issue can occur with an STM1E port provisioned as E4. When viewing the SDH Thresholds subtab, consider “EB” to represent CV. This issue is resolved in Release 5.0.2.

## DDTS # CSCed15073

Rarely, a Working Switch to Protect (WKSWPR) condition resulting from loss and recovery of power to the node can become stuck when there are multiple 1+1 protection groups provisioned on a single OC3 IR/STM1 SH 1310-8 card. This issue is resolved in Release 5.0.

## DDTS # CSCef61339

A monitor circuit in the IS-AINS state might fail to switch to IS in an STM-16 and STM-64 SNCP-DRI ring with E1-42 circuits. This issue is resolved in Release 5.0.

## Electrical IO Cards

### DDTS # CSCeg62711

On DS1/E1 cards, PM TCAs fail to appear, or appear against a lower port number than expected. This issue is resolved in Release 5.0.2.

### DDTS # CSCef72687

When a one way circuit is created on an SDH electrical card, and the direction of the circuit is toward the backplane from the port, where the LP and HP PMs are measured from the backplane in the direction of the port, though there is no circuit present in that direction, the VC3 and VC12 PMs might count anyway. This issue is resolved in Release 5.0.1.

### DDTS # CSCeg53995

For E1-42, if you switch traffic to the protect card, then lock out the protect card, rarely, a 60 to 600 ms traffic hit might occur. To avoid this, switch traffic away from the protect card first, then lock out the protect card. This issue is resolved in Releases 6.0, 5.0.2, and 5.0.1.

### DDTS # CSCeg51806

When both the protect E1-42 card and Slot 17 working E1-42 card are removed and the protect card is then reinserted, the protect card might not take over for Slot 17 when it boots. This can also occur when the protect card is Slot 3 and working card is Slot 4. Avoid removing both cards at the same time, or reinsert the working card first. This issue is resolved in Releases 6.0, 5.0.2, and 5.0.1.

### DDTS # CSCef59642

In a 1:N protection group with E1-42 cards, the Wait to Restore (WTR) timer might not be overridden by a user initiated switch. To see this, in a 1:N protection group with E1-42 cards, reset a working card and wait for it to boot up. After the working card boots up a WTR timer is started. While the WTR is active apply a switch to working. The traffic does not switch until the WTR timer expires. The expected behavior is that the switch to working should cancel the WTR timer and the traffic should switch immediately when the switch command is applied. This issue is resolved in Release 5.0.1.

## DDTS # CSCed89610

The E1-42 LOSS-L threshold in CTC is not displayed or provisionable. The three other line-related thresholds are displayed properly. This issue is resolved in Release 5.0.

## DDTS # CSCef59835

In E1-42 card view, if you select Provisioning > SDH Thresholds, the VC4 button is greyed out. Hence, the E1-42 VC4 threshold is not provisionable. This issue is resolved in Release 5.0.

## Data IO Cards

### DDTS # CSCeg90674

Occasionally when RPR is configured over path protection and a fiber is removed there might be up to a 20 second traffic hit as a result. This issue is resolved in Release 5.0.2.

### DDTS # CSCea20962

No warning is displayed when applying OOS to ML drop ports on the circuit provisioning window. This issue is resolved in Release 5.0.

### DDTS # CSCef62420

On ML100t and ML1000, defects might not be detected and alarms not be reported on a POS port. This can occur when you provision a circuit to POS 0, provision another circuit to POS 1, and then delete the circuit on POS 1. To work around this issue, delete and reprovision the POS 0 circuit. This issue is resolved in Release 5.0.

## MS-SPRing Functionality

### DDTS # CSCeg64837

Rarely, when you build a new BLSR/MS-SPRing, or add nodes to an existing ring, an APSC-IMPROPER alarm might fail to clear. Issue an exerciser command (ring or span) on the span that raised the alarm in order to clear it. This issue is resolved in Release 5.0.2.

### DDTS # CSCef77848

Rarely, when upgrading from a two fiber to four fiber MS-SPRing configuration, the network map might continue to display the "L" on the link after the lockout is cleared. If this occurs, restart your CTC session. This issue is resolved in Release 5.0.1.

**DDTS # CSCec34856**

When you create a circuit over MS-SPRing or DRI, the resource usage in the Maintenance > Cross-Connect > Resource Usage tab will display the incorrect VC# for the circuit you created. Use the Circuit Edit > Monitors window to view the correct VC#. This issue is resolved in Release 5.0.

**DDTS # CSCea81000**

In a two-fiber or four-fiber MS-SPRing, MS-RFI is not reported for an LOS or LOF with a ring lockout in place on a different span. This issue is resolved in Release 5.0.

**DDTS # CSCeb09217**

Circuit states are not updated after a span update. If you update a four node OC-12/STM-4 two-fiber MS-SPRing to a four node OC-192/STM-64 two-fiber BLSR, the previous PCA circuits should be shown as two-fiber MS-SPRing protected, but they are shown as “UNKNOWN” protected. If you relaunch CTC this situation is corrected. This issue is resolved in Release 5.0.

**SNCP Functionality****DDTS # CSCee68239**

Low order circuits cannot be created over Integrated SNCP DRI. Circuit creation fails with an xUpsrSelectorPayloadMismatch error. This issue is resolved in Release 5.0.

**Performance Monitoring****DDTS # CSCef72828**

No TCA is generated for AISS E1 path. The default threshold in CTC is zero. This can be changed in the GUI, but is never used by the card. Thus threshold crossings on this PM do not generate a TCA. This issue is resolved in Release 5.0.1.

**SNMP****DDTS # CSCeg45934**

When NMS sends a query to retrieve E4 Line PM parameters ES, SES, UAS and CV for an E4 interface on an STM1E12 card, SNMP does not show PM counts for E4 interfaces. On an STM1E12 card, Ports 9-12 can be configured as either STM1 or E4. If any of the ports from 9-12 are configured as E4 and an SNMP get request is sent to the node to retrieve E4 line PM parameters, SNMP will not show any data for E4 PM parameters. To avoid this issue, use other management interfaces to query E4 parameters. This issue is resolved in Release 5.0.2.

## DDTS # CSCec75857

There is no SNMP return value for `dsx1TotalTable` when you configure an ONS 15454 with DSX 1 day stats, then query the node. This issue is resolved in Release 5.0.

## TL1

### DDTS # CSCeg87471

Do not set the TID for an ENE to more than 19 characters. Setting the TID for an ENE to 20 characters or more and then issuing a TL1 command on the GNE to execute on the ENE will result in TL1 agent connectivity issues on the ENE. Specifically, if you set the TID on the ENE to 20 characters, reboot the TCC, then try to connect to that ENE from a GNE this will result in a loss of TL1 connectivity to the GNE. This issue is resolved in Release 5.0.2.

# New Features and Functionality

This section highlights new features and functionality for Releases 5.0.x. (Release 4.7 features are also included for ease of access.) For detailed documentation of each of these features, consult the user documentation.

## New Hardware

### TCC2P Card

The Advanced Timing, Communications, and Control Plus (TCC2P) card is an enhanced version of the TCC2 card. The primary enhancements are Ethernet security features and 64K composite clock BITS timing (SONET only).

The TCC2P card performs system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection/resolution, SONET SOH DCC/GCC termination, and system fault detection for the ONS 15454. The TCC2P also ensures that the system maintains Stratum 3 (Telcordia GR-253-CORE) timing requirements. It monitors the supply voltage of the system.

The TCC2P card requires Software Release 4.0 or later.

The LAN interface of the TCC2P card meets the standard Ethernet specifications by supporting a cable length of 328 ft (100 m) at temperatures from 32 to 149 degrees Fahrenheit (0 to 65 degrees Celsius). The interfaces can operate with a cable length of 32.8 ft (10 m) maximum at temperatures from -40 to 32 degrees Fahrenheit (-40 to 0 degrees Celsius).

### TCC2P Functionality

The TCC2P card supports multichannel, high-level data link control (HDLC) processing for the DCC. Up to 84 DCCs can be routed over the TCC2P card and up to 84 section DCCs can be terminated at the TCC2P card (subject to the available optical digital communication channels). The TCC2P selects and processes 84 DCCs to facilitate remote system management interfaces.

The TCC2P also originates and terminates a cell bus carried over the module. The cell bus supports links between any two cards in the node, which is essential for peer-to-peer communication. Peer-to-peer communication accelerates protection switching for redundant cards.

The node database, IP address, and system software are stored in TCC2P nonvolatile memory, which allows quick recovery in the event of a power or card failure.

The TCC2P performs all system-timing functions for each ONS 15454. The TCC2P monitors the recovered clocks from each traffic card and two BITS ports for frequency accuracy. The TCC2P selects a recovered clock, a BITS, or an internal Stratum 3 reference as the system-timing reference. You can provision any of the clock inputs as primary or secondary timing sources. A slow-reference tracking loop allows the TCC2P to synchronize with the recovered clock, which provides holdover if the reference is lost.

The TCC2P supports 64/8K composite clock and 6.312 MHz timing output on ONS 15454 SONET nodes.

The TCC2P monitors both supply voltage inputs on the shelf. An alarm is generated if one of the supply voltage inputs has a voltage out of the specified range.

Install TCC2P cards in Slots 7 and 11 for redundancy. If the active TCC2P fails, traffic switches to the protect TCC2P. All TCC2P protection switches conform to protection switching standards when the bit error rate (BER) counts are not in excess of  $1 * 10^{\text{exp} - 3}$  and completion time is less than 50 ms.

The TCC2P card has two built-in RJ-45 Ethernet interface ports for accessing the system: one on the front faceplate for on-site craft access and a second on the backplane for user interfaces. The rear Ethernet interface is for permanent LAN access and all remote access via TCP/IP as well as for Operations Support System (OSS) access. The front and rear Ethernet interfaces have different IP addresses that are in different subnets.

Two EIA/TIA-232 serial ports, one on the faceplate and a second on the backplane, allow for craft interface in TL1 mode.

Cisco does not support operation of the ONS 15454 with only one TCC2P card. For full functionality and to safeguard your system, always operate with two TCC2P cards.

When a second TCC2P card is inserted into a node, it synchronizes its software, its backup software, and its database with the active TCC2P. If the software version of the new TCC2P does not match the version on the active TCC2P, the newly inserted TCC2P copies from the active TCC2P, taking about 15 to 20 minutes to complete. If the backup software version on the new TCC2P does not match the version on the active TCC2P, the newly inserted TCC2P copies the backup software from the active TCC2P again, taking about 15 to 20 minutes. Copying the database from the active TCC2P takes about 3 minutes. Depending on the software version and backup version the new TCC2P started with, the entire process can take between 3 and 40 minutes.

## Environmental/Compliance

The TCC2P meets the following environmental and compliance standards.

- I-Temp
- Heat dissipation of 26 watts maximum
- EMI/ESD compliant

For TCC2P card-level indicators, card specifications, communication interfaces, system timing, and other details consult the user documentation.

## DWDM Cards

### 32-Channel Demultiplexer Card

The 32-Channel Demultiplexer card (32DMX) is a single-slot optical demultiplexer. The card receives an aggregate optical signal on its COM RX port and demultiplexes it into 32 100-GHz-spaced channels. The 32DMX card can be installed in Slots 1 to 6 and in Slots 12 to 17.

The 32DMX card is designed specifically for use in ONS 15454 MSTP nodes. The 32DMX card operates in conjunction with the 32WSS card to create a software-controlled node with ROADM functionality. ROADM functionality requires two 32DMX single-slot cards and two 32WSS double-slot cards (six slots in the ONS 15454 chassis).

Both the 32DMX card and 32WSS card use Planar Lightwave Circuit (PLC) technology to perform wavelength-level processing.

The 32DMX has the following two types of ports.




---

**Note** For port type descriptions and uses, consult the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

---

- Common Receive (COM RX) port
- Drop ports (1-32)

### 32-Channel Wavelength Selective Switch Card

The 32-Channel Wavelength Selective Switch (32WSS) card performs channel add/drop processing within the ONS 15454 MSTP node. The 32WSS operates in conjunction with the 32DMX to implement Reconfigurable OADM (ROADM) functionality. Equipped with ROADM functionality, the ONS 15454 MSTP can be configured to add or drop individual optical channels using CTC, Cisco MetroPlanner, and CTM.

A ROADM node uses two 32WSS cards (two slots each) and two 32DMX cards (one slot each), for a total of six slots in the chassis. The 32WSS card can be installed in slots 1-2, 3-4, 5-6, or in slots 12-13, 14-15, or 16-17. A terminal site can be configured using only a 32WSS card and a 32DMX card plugged into the east or west side of the shelf. The 32WSS has the following six types of ports.




---

**Note** For port type descriptions and uses, consult the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

---

- ADD ports (1-32)
- EXP RX port
- EXP TX port
- COM TX port
- COM RX port
- DROP TX port

## Client Cards

### MXP\_MR\_2.5G and MXPP\_MR\_2.5G Muxponder Cards

Two new 2.5 Gbps 100 GHz datamux cards, the MXP\_MR\_2.5G and MXPP\_MR\_2.5G, are available for the ONS 15454. These cards can be used for data and SAN applications in a DWDM network. The cards are capable of translating the client input GE and FC optical signal into an optical signal with an optical frequency on the 100 GHz spacing frequency grid, as defined in ITU-T G.692. The cards are available in card protected and unprotected versions.

Long transmission distances are achieved through the use of flat gain optical amplifiers.

The 2.5-Gbps Multirate Muxponder-100 GHz-Tunable 15xx.xx-15yy.yy (MXP\_MR\_2.5G) card aggregates a mix and match of client Storage Area Network (SAN) service client inputs (GE, FICON, and Fibre Channel) into one 2.5 Gbps STM-16/OC-48 DWDM signal on the trunk side. It provides one long-reach STM-16/OC-48 port per card and is compliant with Telcordia GR-253-CORE.

The 2.5-Gbps Multirate Muxponder-Protected-100 GHz-Tunable 15xx.xx-15yy.yy (MXPP\_MR\_2.5G) card aggregates various client SAN service client inputs (GE, FICON, and Fibre Channel) into one 2.5 Gbps STM-16/OC-48 DWDM signal on the trunk side. It provides two long-reach STM-16/OC-48 ports per card and is compliant with ITU-T G.957 and Telcordia GR-253-CORE.

Because the cards are tunable to one of four adjacent grid channels on a 100 GHz spacing, each card is available in eight versions, with 15xx.xx representing the first wavelength and 15yy.yy representing the last wavelength of the four available on the board. In total, 32 DWDM wavelengths are covered in accordance with the ITU-T 100GHz grid standard, G.692, and Telcordia GR-2918-CORE, Issue 2. Card versions and their corresponding wavelengths are documented in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

#### Client Interface

The client interface supports the following payload types.

- GE
- 1G FC
- 2G FC
- 1G FICON
- 2G FICON



#### Note

ESCON is not supported for Releases 4.7 or 5.0.x, and FICON support is limited (see the caveat for DDTS # CSCee45443 for applicable Release 4.7/5.0.x FICON limitations). The changes required to support ESCON and to eliminate the FICON limitations will be made available in a future release with a software upgrade.

Because the client payload cannot oversubscribe the trunk, a mix of client signals can be accepted, up to a maximum limit of 2.5 Gbps. Client interface data rates and encapsulation methods are documented in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

All of the client interfaces supported use the Transparent Generic Framing Procedure (GFP-T) encapsulation method. (For data rates, see the *Cisco ONS 15454 DWDM Installation and Operations Guide*.) The current version of the GFP-T, G.7041, supports transparent mapping of 8B/10B block-coded protocols, including Gigabit Ethernet, Fibre Channel, and FICON.

In addition to the GFP mapping, 1 Gbps traffic on port 1 or port 2 of the high-speed SERDES is mapped to an STS-24c channel. If two 1 Gbps client signals are present at port 1 and port 2 of the high-speed SERDES, the port 1 signal is mapped into the first STS-24c channel and the port 2 signal into the second STS-24c channel. The two channels are then mapped into an STM-16/OC-48 trunk channel.

GFP-T performance monitoring is available via remote monitoring (RMON), and trunk PM is managed according to Telcordia GR-253 and ITU G.783/826. Client PM is achieved through RMON for FC and GE.

### Client to STS Mapping

Only Contiguous concatenation is supported for the MXP\_MR\_2.5G and MXPP\_MR\_2.5G (no VCAT).

Port one supports:

- 1GE and 1G-FC mapped over first STS-24c payload
- 2G-FC mapped over STS-48c

Port two supports:

- 1GE and 1G-FC mapped over second STS-24c payload

### Muxponder Protection

MXP\_MR\_2.5G card protection is accomplished using Y-cable protection. Two MXP\_MR\_2.5G cards can be joined in a Y-cable protection group, which provides protection against failures both on the fiber and in the muxponders. MXPP\_MR\_2.5G card protection is accomplished using splitter protection, which provides protection against failures due to fiber cuts or unacceptable signal degradation on the trunk side. Switching is performed only if the protect line is error free.

### Buffer-to-Buffer Credit Management

A buffer-to-buffer credit management scheme provides FC flow control. With this feature enabled, a port indicates the number of frames that can be sent to it (its buffer credit) before the sender is required to stop transmitting and wait for the receipt of a “ready” indication. The MXP\_MR\_2.5G and MXPP\_MR\_2.5 cards support FC credit based flow control with a buffer-to-buffer credit extension of up to 1600 km for 1G FC and up to 800 km for 2G FC. The feature may be enabled or disabled.

### Buffer-to-Buffer Distance Extension

Release 4.7/5.0.x can examine the B2B client credit and allow the client equipment to run at full rate even with hundreds of Km adopting proprietary exchange of memory information between the two cards.

This does not involve termination of the FC link. Only protocol error monitoring and flow control are terminated.

End systems interoperate through this solution transparently. The number of frames in transit cannot exceed the far end buffer capacity. “Ready” indicators (called R\_RDYs) are terminated locally and not part of flow control, so they do not waste WAN bandwidth. Release 4.7/5.0.x supports maximum FC throughput independent of attached FC Switch BB Credit Allocation. IDLE frames are terminated locally and regenerated at the far end.

### DWDM Laser Features

The MXP\_MR\_2.5G and MXPP\_MR\_2.5G support the following DWDM laser features.

- 2.5 Gb/s operation; tunable over four separate channels at 100 GHz spacing
- Integrated wavelength-locker
- Entire C band ITU wavelengths available (1528 to 1563 nm)

- 14 pin butterfly package with optical isolator
- Internal TEC with precision NTC thermistor
- Extended reach performances up to 360 Km with 2 dB dispersion power penalty

## MXP\_2.5G\_10E Card

The 2.5-Gbps–10-Gbps Muxponder–100 GHz–Tunable xx.xx-xx.xx (MXP\_2.5G\_10E) card is a DWDM muxponder for the ONS 15454 platform that supports full optical transparency on the client side. The card multiplexes four 2.5 Gbps client signals (4 x OC48/STM-16 SFP) into a single 10-Gbps DWDM optical signal on the trunk side. The MXP\_2.5G\_10E provides wavelength transmission service for the four incoming 2.5 Gbps client interfaces. The MXP\_2.5G\_10E muxponder passes all SONET/SDH overhead bytes transparently.

The digital wrapper function (ITU-T G.709 compliant) formats the DWDM wavelength so that it can be used to set up general communication channels (GCC) for data communications, enable forward error correction, or facilitate performance monitoring.

The MXP\_2.5G\_10E works with Optical Transparent Network (OTN) devices defined in ITU-T G.709. The card supports Optical Data Channel Unit 1 (ODU1) to Optical Channel Transport Unit (OTU2) multiplexing, an industry standard method for asynchronously mapping a SONET/SDH payload into a digitally wrapped envelope.



### Note

The MXP\_2.5G\_10E card is not compatible with the MXP\_2.5G\_10G card, which does not support full optical transparency.

The MXP\_2.5G\_10E features a 1550-nm laser on the trunk port and four 1310-nm lasers on the client ports and contains five transmit and receive connector pairs (labeled) on the card faceplate. The card uses a dual LC connector on the trunk side and uses SFP modules on the client side for optical cable termination. The SFP pluggable modules are short reach (SR) or intermediate reach (IR) and support an LC fiber connector.

### Key Features

The MXP\_2.5G\_10E card has the following high level features:

Four 2.5 Gbps client interfaces (OC-48/STM-16) and one 10 Gbps trunk. The four OC-48/STM-16 signals are mapped into a ITU-T G.709 OTU2 signal using standard ITU-T G.709 multiplexing.

**Onboard Enhanced Forward Error Correction (E-FEC) processor:** The processor supports both standard RS (specified in ITU-T G.709) and E-FEC, which allows an improved gain on trunk interfaces with a resultant extension of the transmission range on these interfaces. The E-FEC functionality increases the correction capability of the transponder to improve performance, allowing operation at a lower OSNR compared to the standard RS (237,255) correction algorithm. A new BCH algorithm implemented in E-FEC allows recovery of an input BER up to 1E-3.

**Pluggable client interface optic modules:** The MXP\_MP\_10E card has modular interfaces. Two types of optics modules can be plugged into the card: an OC-48/STM 16 SR-1 interface with a 7 km nominal range (for short range and intra-office applications) and an IR-1 interface with a range up to 40 km.

**High level provisioning support:** The MXP\_MP\_10E card is initially provisioned using Cisco MetroPlanner software. Subsequently, the card may be monitored and provisioned using CTC software.

**Link monitoring and management:** The MXP\_MP\_10E card uses standard OC-48 OH (overhead) bytes to monitor and manage incoming interfaces. The card passes the incoming SDH/SONET data stream and its overhead bytes transparently.

**Control of layered SONET/SDH transport overhead:** The card is provisionable to terminate regenerator section overhead. This is used to eliminate forwarding of unneeded layer overhead. It can help reduce the number of alarms and help isolate faults in the network.

**Automatic timing source synchronization:** The MXP\_MP\_10E normally synchronizes from the TCC2 card. If for some reason, such as maintenance or upgrade activity, the TCC2 is not available, the MXP\_MP\_10E automatically synchronizes to one of the input client interface clocks.

**Configurable squelching policy:** The card can be configured to squelch the client interface output if there is LOS at the DWDM receiver or if there is a remote fault. In the event of a remote fault, the card manages multiplex section alarm indication signal (MS-AIS) insertion.

### Client Interfaces

The MXP\_2.5G\_10E provides four intermediate- or short-range OC-48/STM-16 ports per card on the client side. Both SR-1 or IR-1 optics can be supported and the ports utilize SFP connectors. The client interfaces use four wavelengths in the 1310-nm, ITU 100-MHz spaced channel grid.

### DWDM Interface

The MXP\_MP\_10E serves as an OTN multiplexer, transparently mapping four OC-48/STM-16 channels asynchronously to ODU1 into one 10-Gbps trunk. The DWDM trunk is tunable for transmission over four wavelengths in the 1550-nm, ITU 100-GHz spaced channel grid.

### Multiplexing Function

The muxponder is an integral part of the optically transparent ROADM network in which data payload channels and wavelengths are processed exclusively at the optical level without electrical to optical (E-O) conversion. The key function of MXP\_MP\_10E is to multiplex 4 OC-48/STM16 signals onto one ITU-T G.709 OTU2 optical signal (DWDM transmission). The multiplexing mechanism allows the signal to be terminated at a far-end node by another MXP\_2.5G\_10E card.

The MXP\_2.5G\_10E card performs ODU to OTU multiplexing as defined in ITU-T G.709.

The output of the muxponder is a single 10-Gbps DWDM trunk interface defined using OTU2. It is within the OTU2 framing structure that FEC or E-FEC information is appended to enable error checking and correction.

The MXP\_2.5G\_10E card is synchronized to the TCC2 clock during normal conditions and transmits the ITU-T G.709 frame using this clock.

The MXP\_2.5G\_10E card supports Y-cable protection. Two MXP\_2.5G\_10E cards can be joined in a Y-cable protection group with one card assigned as the working card and the other defined as the protection card. This protection mechanism provides redundant bidirectional paths.

You can configure the Forward Error correction for the MXP\_2.5G\_10E in three modes: NO FEC, FEC, and E-FEC. So, as client side traffic passes through the MXP\_2.5G\_10E card, it can be digitally wrapped using FEC mode error correction or E-FEC mode error correction (or no error correction at all).

For further card details, specifications, and functionality, see the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## TXP\_MR\_10E Card

The 10-Gbps Transponder–100-GHz–Tunable xx.xx-xx.xx (TXP\_MR\_10E) card is a multirate transponder for the ONS 15454 platform. The card is fully backward compatible with the TXT\_MR\_10G card. It processes one 10-Gbps signal (client side) into one 10-Gbps, 100-GHz DWDM signal (trunk side) that is tunable on four wavelength channels (ITU-T 100-GHz grid).

The TXP\_MR\_10E card can be used in any of the twelve I/O slots in the ONS 15454, including both high-speed and multirate ports (Slots 1 to 6 and Slots 12 to 17 can be used). Two TCC2 cards must be present in the system for the board to function. TCC2 fault replacement can be performed without impacting the traffic.

The TXP\_MR\_10E port features a 1550-nm laser for the trunk port and a ONS-XC-10G-S1 XFP module for the client port and contains two transmit and receive connector pairs (labeled) on the card faceplate.

### Key Features

The key features of the TXP\_MR\_10G card are:

- A tri-rate XFP client interface
- OC-192/STM-64 (SR1)
- 10GE (10GBASE-LR)
- 10G-FC (1200-SM-LL-L)
- OC-192/STM-64 to G.709 OTU2 provisionable synchronous and asynchronous mapping

### Client Interface

The client interface is implemented by an on-board XFP module, a tri-rate transponder that provides a single port that can be configured in the field to support STM-64/OC-192 (with an SR-1 optics module that plugs into the XFP module), 10GE (10GBASE-LR), or 10G FC protocols. The XFP module supports 10 GE LAN PHY, 10 GE WAN PHY, STM-64, and OC-192/STM-64 client signals.

Two types of pluggable client-side optics modules are available for the XFP module on the TXP\_MR\_10E card: an OC-192/STM-64 SR-1/I-64.2 interface (ITU-T G.691) or an S-64.2 optical interface (ITU-T G.691). The SR-1 is a 1310-nm optical interface that uses LC connectors. SR-1 is typically used in short-reach intra-office applications with ranges typically up to 7 km.

### DWDM Trunk Interface

On the trunk side, the TXP\_MR\_10E card provides a 10 Gbps STM-64/OC-192 interface. Four tunable channels are available in the 1550-nm band on the 100-GHz ITU grid for the DWDM interface. The TXP\_MR\_10E card provides 3R transponder functionality for this 10 Gbps trunk interface, so, the card is suited for use in long range amplified systems. The DWDM interface is compliant with ITU-T G.707, ITU-T G.709, and Telcordia GR-253-CORE standards.

The TXP\_MR\_10E card supports Y-cable protection, which provides transponder equipment protection without client terminal equipment interface protection. A single client interface can be split between two transponder cards using a Y-protection device.

You can configure the Forward Error correction for the TXP\_MR\_10E in three modes: NO FEC, FEC, and E-FEC. So, as client side traffic passes through the TXP\_MR\_10E card, it can be digitally wrapped using FEC mode error correction or E-FEC mode error correction (or no error correction at all).



#### Note

Because the transponder has no visibility into the data payload and detect circuits, a TXP\_MR\_10E card does not display circuits under the card view.

### Client-to-Trunk Mapping

The TXP\_MR\_10E card can perform ODU2-to-OCh mapping, which allows operators to provision data payloads in a standard way across 10-Gbps optical links. For further card details, specifications, and functionality, see the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## Small Form-Factor Pluggables

The following small form-factor pluggables (SFPs and XFPs) are new for Release 4.7/5.0.x. For SFP and XFP installation or removal consult the document, *Installing GBIC, SFP and XFP Optical Modules in Cisco ONS 15454, 15327, 15600, and 15310 Platforms*.

### XFP

The 10 Gbps 1310 nm XFP transceiver is an integrated fiber optic transceiver that provides a high-speed serial link at the following signaling rates: 9.95 Gbps, 10.31 Gbps, 10.51 Gbps, and 10.66/10.71/11.10 Gbps which apply to 10GBASE-LR (fibre channel and Ethernet) as well as OC-192/STM-64 SONET-SDH. The XFP integrates the receiver and transmit path. The transmit side recovers and re-times the 10 Gbps serial data and passes it to a laser driver. The laser driver biases and modulates a 1310 nm DFB (distributed feed-back) laser, enabling data transmission over SMF through an LC connector. The receive side recovers and re-times the 10 Gbps optical data stream from a PIN photo detector, transimpedance amplifier and passes it to an output driver.

### SFP

Small Form-factor Pluggables (SFPs) are integrated fiber optic transceivers that provide high speed serial links from a port or slot to the network. Various latching mechanisms can be used on the SFP modules. There is no correlation between the type of latch to the model type (such as SX or LX/LH) and technology type (such as Gigabit Ethernet). See the label on the SFP for technology type and model.

## New Software Features and Functionality as of Release 5.0.2

### New DWDM Features

#### L-Band Support for Transponder Module

With Release 5.0.2 the TXP\_MR\_10E card is equipped with an L-band version of the trunk optical front-end. This allows the card to operate in the L-band frequencies, in addition to the C-band frequencies allowed with the previous TXP\_MR\_10E card design. The L-Band transponder may be tuned over 8 Lambda at 50 Ghz. The TXP\_MR\_10E card is equipped with either the L-band or the C-band version of the trunk optical front-end and operates at specific frequencies on the ITU grid for each version of the card.

#### OPT-BST-E Distance Extension Card

Release 5.0.2 implements a new booster amplifier card (OPT-BST-E). This card provides similar features and functionalities to those currently supported by the OPT-BST unit, but guarantees a 3dB higher optical power to address longer unregenerated distances using the ONS 15454 MSTP Transport Platform. The OPT-BST-E operates in both the ONS 15454 ANSI and ETSI chassis. The card operates in the same way the currently available OPT-BST unit operates and is supported by the same Intelligent Optical Transmission features and functionalities that are currently supported by the ONS 15454 MSTP (Releases 4.7 and 5.0). The card operates with the regular alarm and performance management already provided by the OPT-BST.

# New Software Features and Functionality as of Release 5.0

## TCC2P Card Software Support

Release 5.0 introduces several new software features, as described below, that support the TCC2P card.

### IP Addressing with Secure Mode Enabled

TCC2P cards provide a secure mode option allowing you to provision two IP addresses for the ONS 15454. One IP address is provisioned for the ONS 15454 backplane LAN port. The other IP address is provisioned for the TCC2P TCP/IP craft port. The two IP addresses provide an additional layer of separation between the craft access port and the ONS 15454 LAN. If secure mode is enabled, the IP addresses provisioned for the TCC2P TCP/IP ports must follow general IP addressing guidelines. In addition, TCC2P IP addresses must reside on a different subnet from the ONS 15454 backplane port and ONS 15454 default router IP addresses.

The IP address assigned to the backplane LAN port becomes a private address, which is used to connect the ONS 15454 GNE to an OSS (Operations Support System) through a central office LAN or private enterprise network. In secure mode, by default, the backplane's LAN IP address is not displayed in the CTC node view or to a technician directly connected to the node. This default can be changed to allow the backplane's address to be displayed on CTC only by a Superuser.



**Note**

---

Secure mode is not available if TCC2 cards are installed, or if only one TCC2P card is installed.

---

### Backwards Compatibility

The TCC2P card is backwards compatible with Releases 4.0 and forward. In these releases, the card is identified as TCC2 in the inventory. View the CLEI codes to determine the actual card type. The TCC2P card is displayed as TCC2P in CTC as of Release 5.0. For card compatibility, the same rules apply with the TCC2P as with the TCC2 when combined with TCC+/TCCI. Additionally, when combined with a TCC2, the TCC2P functions as a TCC2 card: Security/Clock options available with dual TCC2Ps are not available with mixed TCC2 and TCC2P nodes. A TCC2 will be MEA if inserted in a node requiring TCC2P (a node in which security/clock options are being used). The TCC2 card will not accept a “Secure” database at all. The TCC2 will accept a database marked for 64K clock selection (SONET only), but will default to DS1.

### In-Service Topology Upgrades

In Release 5.0.x in-service topology upgrades are supported for unprotected to path protection/SNCP, terminal to linear (add a node to a 1+1), and path protection/SNCP to 2F-BLSR/MS-SPRing. Release 5.0.x provides both manual methods and CTC wizards for completing these upgrades.



**Note**

---

Traffic hits resulting from an in service topology upgrade are less than 50 ms; however, traffic might not be protected during certain upgrades: in the case where you are upgrading from unprotected to SNCP/path protection, with unidirectional routing, traffic hits might be greater than 50 ms. Cisco recommends waiting for a maintenance window to perform the topology upgrade in this case.

---

## CTC Topology Upgrade Wizards

The following CTC topology upgrade wizards have been added for Release 5.0.x to support in service topology upgrades.

### Unprotected to Path Protection/SNCP

With this feature you can convert an unprotected circuit to path protection/SNCP, or you can convert unprotected segments of a partially protected circuit to path protection/SNCP.

### Path Protection/SNCP to Two Fiber BLSR/MS-SPRing

This feature creates a two fiber BLSR/MS-SPRing and converts all path protection/SNCP circuits on the selected ring to BLSR/MS-SPRing circuits.

### Terminal to Linear—Add a Node to 1+1

The wizard for this feature is invoked by right-clicking on a 1+1 link and then selecting the “terminal to linear” option. The option adds a node between a two nodes connected by a 1+1.

## Additional Support for In Service Topology Upgrades

### Circuit Routing

With Release 5.0.x you can choose between manually or automatically routing path protection/SNCP circuits for a topology upgrade.

The following circuit types are supported for topology upgrades.

- One way and two way
- Automatically-routed and manually-routed
- CTC-created and TL1-created
- Ethernet (unstitched)
- DWDM
- Multiple source and destination (both sources should be on one node and both drops on one node)
- VCAT/CCAT

### Circuit Merge and Reconfigure

The circuit merge and reconfigure features enable you to merge selected CTC, TL1, or Hybrid circuits into one or more discovered CTC circuits based on the alignment of the circuit cross-connects, rather than the circuit ID.

Circuit Merge merges m circuits into one circuit. This feature takes one master circuit and merges aligned circuits with the master.

Circuit Reconfigure merges m circuits into n circuits. This feature takes m circuits and reconfigures them based on cross-connect alignment. To merge circuits choose the Merge subtab of the Edit Circuits tab in CTC. To reconfigure circuits, choose the CTC Tools > Circuits tab, and select “Reconfigure Circuits...”

## Dual-ring Interconnect

Dual-ring interconnect (DRI) topology provides an extra level of path protection for circuits on interconnected rings. DRI allows users to interconnect BLSR/MS-SPRings, path protection/SNCPs, or a path protection/SNCP with a BLSR/MS-SPRing, with additional protection provided at the transition nodes. In a DRI topology, ring interconnections occur at two or four nodes.

### DRI Features

The following list provides supported BLSR/MS-SPRing DRI features at a glance.

- BLSR/MS-SPRing two fiber and four fiber configurations
- BLSR/MS-SPRing with path protection/SNCP supported at the STS level (VT level not supported)
- Traditional DRI and integrated (IDRI)
- Traditional four node interconnect
- Integrated two node interconnect
- BLSR/MS-SPRing path level protection
- Drop and continue included
- Circuit routing, both manual and automatic
- Same side, or opposite side interconnect
- Ring interconnect on protect (RIP)
- Interconnection with mixed OCn/STMn
- Open ended DRI (supported for multi-vendor)



#### Note

Interconnection links do not support 1+1, 1:1, or 1:n.



#### Note

Dual transmit is not supported for Release 5.0.x BLSR/MS-SPRing DRI.

### BLSR/MS-SPRing DRI

Unlike BLSR/MS-SPRing automatic protection switching (APS) protocol, BLSR/MS-SPRing DRI is a path-level protection protocol at the circuit level. Drop-and-continue BLSR-DRI requires a service selector in the primary node for each circuit routing to the other ring. Service selectors monitor signal conditions from dual feed sources and select the one that has the best signal quality. Same-side routing drops the traffic at primary nodes set up on the same side of the connected rings, and opposite-side routing drops the traffic at primary nodes set up on the opposite sides of the connected rings. For BLSR/MS-SPRing DRI, primary and secondary nodes cannot be the circuit source or destination.

A DRI circuit cannot be created if an intermediate node exists on the interconnecting link. However, an intermediate node can be added on the interconnecting link after the DRI circuit is created.

DRI protection circuits act as protection channel access (PCA) circuits. In CTC, you set up DRI protection circuits by selecting the PCA option when setting up primary and secondary nodes during DRI circuit creation.

## Path Protection/SNCP to BLSR/MS-SPRing DRI Handoff Configurations

Path protection/SNCPs and BLSR/MS-SPRings can also be interconnected. In path protection/SNCP to BLSR/MS-SPRing DRI handoff configurations, primary and secondary nodes can be the circuit source or destination, which is useful when non-DCC optical interconnecting links are present.

## SL-Series Fibre Channel Card Enhancements

With Release 5.0.x the FC\_MR-4 card features a new enhanced mode. The FC\_MR-4 card can now operate in two different modes:

- Line Rate mode. This mode is backward compatible with the 4.6 release Line Rate mode.
- Enhanced mode. This mode supports subrate transport mapping, distance extension, and other enhancements.



### Note

The FC\_MR-4 card reboots when changing card modes (a traffic hit will result). The FPGA running on the card will be upgraded to the required image. However, the FPGA image in the card's flash will not be modified.

## Enhanced Card Mode

The following features are available in enhanced card mode.

### Mapping

1 Gbps Fibre Channel/FICON is mapped into:

- SONET CCAT: STS1c, STS3c, STS6c, STS9c, STS12c, STS18c, STS24c, STS48c
- SONET VCAT: STS3c-Nv (N is 1 to 8), STS1c-Nv (N is 1 to 24)
- SDH CCAT: VC4-1c, VC4-2c, VC4-3c, VC4-4c, VC4-6c, VC4-8c, VC4-16c
- SDH VCAT: VC4-Nv (N is 1 to 8)

2 Gbps Fibre Channel/FICON is mapped into:

- SONET CCAT: STS1c, STS3c, STS6c, STS9c, STS12c, STS18c, STS24c, STS36c, STS48c
- SONET VCAT: STS3c-Nv (N is 1 to 16), STS1c-Nv (N is 1 to 48)
- SDH CCAT: VC4-1c, VC4-2c, VC4-3c, VC4-4c, VC4-6c, VC4-8c, VC4-12c, VC4-16c
- SDH VCAT: VC4-16v (N is 1 to 16)
- SW -LCAS

Virtual Concatenation Group (VCG) is reconfigurable with the software link capacity adjustment scheme (SW-LCAS) enabled, as follows.

- Out of service and out of group members can be removed from VCG.
- Members with deleted cross connect can be removed from VCG.
- Errored members can be autonomously removed from VCG.
- Degraded bandwidth VCGs are supported.

VCG is flexible with SW-LCAS enabled (VCG can run traffic as soon as the first cross-connect is provisioned on both sides of the transport).

### Distance Extension

FC\_MR-4 card enhanced mode distance extension enables the following features and support.

- SAN extension over long distances through buffer-to-buffer (B2B) credit spoofing
- 2300 Km for 1G ports (longer distances supported with lesser throughput)
- 1150 Km for 2G ports (longer distances supported with lesser throughput)
- A negotiation mechanism to identify if the far end FC-over-SONET card supports the Cisco proprietary B2B mechanism
- Auto detection of FC switch B2B credits from FC-SW standards based ELP frames
- Support for manual provisioning of credits based on FC switch credits
- Automatic GFP buffer adjustment based on round trip latency between two SL ports
- Automatic credit recovery during SONET switchovers or failures
- Insulation for FC switches from any SONET switchovers (No FC fabric reconvergences will occur for SONET failures of less than or equal to 60 ms.)

### Interoperability Features

FC\_MR-4 card enhanced mode interoperability features a Maximum Frame Size setting to prevent accumulation of oversized PMs for VSAN frames, as well as an Ingress Filtering Disable feature for attachment to third party GFP over SONET/SDH equipment.

For other details on enhancements to FC\_MR-4 card functionality, consult the user documentation.

## Open GNE

Release 5.0.x supports open GNE configurations, through which the ONS 15454 can communicate with non-ONS nodes that do not support point-to-point protocol (PPP) vendor extensions or OSPF type 10 opaque link-state advertisements (LSA), both of which are necessary for automatic node and link discovery. An open GNE configuration allows the DCC-based network to function as an IP network for non-ONS nodes. To support open GNE Release 5.0.x provides provisionable foreign DCC terminations, provisionable proxy server tunnels, and provisionable firewall tunnels.

### Foreign DCC termination

To configure an open GNE network, you can provision SDCC, LDCC, and GCC terminations to include a far-end, non-ONS node using either the default IP address of 0.0.0.0 or a specified IP address. You provision a far-end, non-ONS node by checking the “Far End is Foreign” check box during SDCC, LDCC, and GCC creation. The default 0.0.0.0 IP address allows the far-end, non-ONS node to provide the IP address; if you set an IP address other than 0.0.0.0, a link is established only if the far-end node identifies itself with that IP address, providing an extra level of security.

### Proxy Server Tunnels and Firewall Tunnels

By default, the SOCKS proxy server only allows connections to discovered ONS peers, and the firewall blocks all IP traffic between the DCC network and LAN. You can, however, provision proxy tunnels to allow up to 12 additional destinations for SOCKS version 5 connections to non-ONS nodes. You can also provision firewall tunnels to allow up to 12 additional destinations for direct IP connectivity between the DCC network and LAN. Proxy and firewall tunnels include both a source and destination subnet. The connection must originate within the source subnet and terminate within the destination subnet before either the SOCKS connection or IP packet flow is allowed.

To set up proxy and firewall subnets in CTC, use the Provisioning > Network > Proxy and Firewalls subtabs. The availability of proxy and/or firewall tunnels depends on the network access settings of the node. See the user documentation for further details.

## 1+1 VT Protection Support

With Release 5.0.x support for VT 1+1 protection increases from 224 to 336 VTs. The CTC Resource Usage screen is updated to display the working and protect allocation.

## Provisionable Patchcord

Release 5.0.x introduces provisionable patchcord functionality. A provisionable patchcord is a user-provisioned link that is advertised by OSPF throughout the network. Provisionable patchcords, also called virtual links, are needed in the following situations:

- An optical port is connected to a transponder or muxponder client port provisioned in transparent mode.
- An optical ITU port is connected to a DWDM optical channel card.
- Two transponder or muxponder trunk ports are connected to a DWDM optical channel card and the generic control channel (GCC) is carried transparently through the ring.
- Transponder or muxponder client and trunk ports are in a regenerator group, the cards are in transparent mode, and DCC/GCC termination is not available.

Provisionable patchcords are required on both ends of a physical link. The provisioning at each end includes a local patchcord ID, slot/port information, remote IP address, and remote patchcord ID. Patchcords appear as dashed lines in CTC network view. Patchcords can be provisioned through CTC, or through TL1. For provisioning details and application specifics consult the user documentation.

## State Verification Scan Before Activation

Before allowing a software activation or reversion to proceed, Release 5.0.x nodes verify that their current state meets required activation criteria. Activation criteria must be met in order to avoid traffic hits. For ONS 15454, ONS 15454 SDH, ONS 15327, and ONS 15310 nodes, all BLSR/MS-SPRing spans on the node must be locked-out, and no 1:1, 1:N, 1+1 or Y-Cable protection switches can be in progress. For ONS 15600 nodes, all BLSR spans on the node must be locked-out.

## Admin SSM

Synchronization status messaging (SSM) is a protocol that communicates information about the quality of the timing source. SSM messages enable nodes to automatically select the highest quality timing reference and to avoid timing loops. With Release 5.0.x you can configure an SSM value for a timing source (either BITS-IN or Optical Line) by selecting from the "ADMIN. SSM" selection box in the BITS Facilities subtab of the node view, Provisioning > Timing tabs. This feature is useful when the selected external timing source has no SSM information. When you select the Admin SSM value, all switching decisions are subsequently made based on your selection. The same SSM value is transmitted out of the interface configured for BITS Out, and in transmit Optical S1. The DS1 BITS type with framing type SF(D4) only supports Admin SSM. The 64KHz+8KHz clock (ONS 15454 SONET only) also only supports Admin SSM. ESF Framing must have Sync Messaging turned off (uncheck the check box) in order to enable Admin SSM selection. SONET nodes use the SSM Generation II message set, as defined in Table 4 of ANSI T1.101-1999. SDH nodes support SDH generation 1 SSM and STU. SONET nodes support only SONET SSM (GR-253).

## Linear Port-Mapped Ethernet Mode (8-port 10/100 Ethernet Linear Mapper)

Port-mapped mode, also referred to as linear mapper, configures the E-Series card to map a specific E-Series Ethernet port to one of the card's specific STS/VC circuits. Port-mapped mode ensures that Layer 1 transport has low latency for unicast, multicast, and mixed traffic. Ethernet and Fast Ethernet on the E100T-G or E10/100-4 card operate at line-rate speed. Gigabit Ethernet transport is limited to a maximum of 600 Mbps because the E1000-2-G card has a maximum bandwidth of STS-12c/VC4-4c. Ethernet frame sizes up to 1522 bytes are also supported, which allow transport of IEEE 802.1Q tagged frames. The larger maximum frame size of Q-in-Q frames (IEEE 802.1Q in IEEE 802.1Q wrapped frames) is not supported.

### E-Series Mapping Ethernet Ports to STS/VC Circuits

Port-mapped mode disables Layer 2 functions supported by the E-Series in single-card and multicard mode, including STP, VLANs, and MAC address learning. It significantly reduces the service-affecting time for cross-connect and TCC2/TCC2P card switches.

Port-mapped mode does not support VLANs in the same manner as multicard and single-card mode. The ports of E-Series cards in multicard and single-card mode can join specific VLANs. E-Series cards in port-mapped mode do not have this Layer 2 capability and only transparently transport external VLANs over the mapped connection between ports. An E-Series card in port-mapped mode does not inspect the tag of the transported VLAN, so a VLAN range of 1 through 4096 can be transported in port-mapped mode.

Port-mapped mode does not perform any inspection or validation of the Ethernet frame header. The Ethernet CRC is validated, and any frame with an invalid Ethernet CRC is discarded.

Port-mapped mode also allows the creation of STS/VC circuits between any two E-Series cards, including the E100T-G, E1000-2-G, and the E10/100-4 (the ONS 15327 E-Series card). Port-mapped mode does not allow ONS 15454 E-Series cards to connect to the ML-Series or G-Series cards, but does allow an ONS 15327 E10/100-4 card provisioned with LEX encapsulation to connect to the ML-Series or G-Series cards.

## GFP-F Framing

Generic Framing Procedure (GFP) defines a standard-based mapping for different types of services onto SONET/SDH. With Release 5.0.x the ML-Series and CE-Series cards support frame-mapped GFP (GFP-F), the PDU-oriented client signal adaptation mode for GFP. GFP-F maps one variable length data packet onto one GFP packet. GFP defines common functions and payload specific functions. Common functions are those shared by all payloads. Payload-specific functions differ depending on the payload type. The GFP standard is detailed in ITU recommendation G.7041.

### Provisionable Framing Mode

Release 5.0.x provides a method to provision framing mode in the card view, Provisioning > Card tab, which displays the framing mode selections for the card in a drop-down list, and allows you to change the framing mechanism to either HDLC or GFP-F. You can also preprovision the framing mode prior to installing the card, and the card will boot up in the pre-provisioned mode. For details on framing mode provisioning consult to user documentation.

## Cisco IOS Version Support

Cisco IOS Version 12.2(18)SO comes preloaded on the ONS 15454 SONET/SDH TCC2/TCC2P card. Cisco IOS software controls the data functions of the ML-Series cards (ML1000-2 or ML100T-12). The ML-series cards download the IOS software from the TCC2/TCC2P when they first reset. The Cisco IOS image is also included on the standard ONS 15454 SONET/SDH System Software CD under the package file name M\_I.bin and full file name ons15454m-i7-mz. The image is not available for download or shipped separately.



### Note

You cannot update the ML-Series Cisco IOS image in the same manner as the Cisco IOS system image on a Cisco Catalyst Series. An ML-Series Cisco IOS image upgrade is accomplished only through the ONS 15454 SONET/SDH CTC, and Cisco IOS images for the ML-Series cards are available only as part of an ONS 15454 SONET or SDH software release.

## VCAT Member Routing Enhancements

Release 5.0.x supports two types of automatic and manual routing for VCAT members: common fiber routing (previously supported) and split routing. CE-100T-8, FC\_MR-4 (both line rate and enhanced mode), and ML-Series cards support common fiber routing. CE-100T-8 cards also support split fiber routing, which allows the individual members to be routed on different fibers, or each member to have different routing constraints. This mode offers both the greatest bandwidth efficiency and the possibility of differential delay (handled by buffers on the terminating cards). Both common fiber and split fiber routing support Fully Protected, PCA, and Unprotected protection schemes. Split fiber routing also supports DRI protection. In both common fiber and split fiber routing, each member can use a different protection scheme; however, for common fiber routing, CTC checks the combination to make sure a valid route exists. If it does not, the user must modify the protection type. In both common fiber and split fiber routing, intermediate nodes treat the VCAT members as normal circuits that are independently routed and protected by the SONET network. At the terminating nodes, these member circuits are multiplexed into a contiguous stream of data. For more information on VCAT member routing consult the user documentation.

## Link Capacity Adjustment

The CE-100T-8 card supports Link Capacity Adjustment Scheme (LCAS), which is a signaling protocol that allows dynamic bandwidth adjustment of VCAT circuits. When a member fails, a brief traffic hit occurs. LCAS temporarily removes the failed member from the VCAT circuit for the duration of the failure, leaving the remaining members to carry the traffic. When the failure clears, the member circuit is automatically added back into the VCAT circuit without affecting traffic. You can select LCAS during VCAT circuit creation.

Although LCAS operations are errorless, a SONET error can affect one or more VCAT members. If this occurs, the VCAT Group Degraded (VCG-DEG) alarm is raised. For information on clearing this alarm, refer to the Cisco ONS 15454 Troubleshooting Guide.

## Software–Link Capacity Adjustment

Instead of LCAS, the FC\_MR-4 (enhanced mode) and ML-Series cards support Software–Link Capacity Adjustment Scheme (Sw-LCAS). Sw-LCAS is a limited form of LCAS that allows the VCAT circuit to adapt to member failures and keep traffic flowing at a reduced bandwidth. Sw-LCAS uses legacy SONET failure indicators like AIS-P and RDI-P to detect member failure. Sw-LCAS removes the failed member from the VCAT circuit, leaving the remaining members to carry the traffic. When the failure clears, the

member circuit is automatically added back into the VCAT circuit. For ML-Series cards, Sw-LCAS allows circuit pairing over two-fiber BLSRs. With circuit pairing, a VCAT circuit is set up between two ML-Series cards; one is a protected circuit (line protection) and the other is PCA. For four-fiber BLSR, member protection cannot be mixed. You select Sw-LCAS during VCAT circuit creation. The FC\_MR-4 (line rate mode) does not support Sw-LCAS.

### Additional VCAT Support

Also, you can create non-LCAS VCAT circuits, which do not use LCAS or Sw-LCAS. While LCAS and Sw-LCAS member cross-connects can be in different service states, all In Group non-LCAS members must have cross-connects in the same service state. A non-LCAS circuit can mix Out of Group and In Group members, as long as the In Group members are in the same service state. Non-LCAS members do not support the OOS-MA,OOG service state; to put a non-LCAS member in the Out of Group VCAT state, use OOS-MA,DSBLD.

## SNMP

### High Capacity RMON

Remote Network Monitoring (RMON) is a feature commonly used to monitor the health of a network. The Internet Engineering Task Force (IETF) specifies a standard MIB, RFC 2819 [1], to be deployed for this purpose. Release 5.0.x adds enhancements to the SNMP agent on the ONS 15454, ONS 15454 SDH, and ONS 15327 platforms to supplement existing RMON SNMP support. This enhancement includes support for the HC-RMON-MIB. High Capacity RMON (HC-RMON) is an extension of RMON. RMON counters are 32-bit while HC-RMON counters are 32-bit and 64-bit as defined in the MIB. Release 5.0.x supports the following HC-RMON tables.

- mediaIndependentTable
- etherStatsHighCapacityTable
- etherHistoryHighCapacityTable

The MIB variable hcRMONCapabilities is supported along with these tables.

### STS Around Ring

Release 5.0.x supports manual provisioning of contiguous concatenation (CCAT) STS circuits around the ring (traffic travels around the ring, starting and ending at the same node). In previous releases, if you selected the circuit source and destination as starting and ending on different I/O ports of the same node, the result would be an intra-node circuit only. With Release 5.0.x, you can manually route this type of circuit all the way around the ring. STS around the ring is supported for an unprotected path, in an unprotected ring, unless the underlying topology is line protected, in which case the around the ring circuit will also be line protected. STS around the ring is supported for all circuit sizes, starting with STS1 (SONET), or STM1 (SDH), and for all supported management interfaces.

## CTC Enhancements

### CTC Circuits State Default

The Release 5.0.x circuit creation wizard uses the new node default value, `Node.circuits.State`, as the default circuit state when creating a circuit. This default can be set in the NE Defaults window, and will not be overridden by the “user preferences” command feature, which caused the default value to be abandoned when using the wizard in previous releases.

### Shell Login Challenge

Release 5.0.x supports the requirement of a specific shell password, set initially by the first shell user and then required of subsequent shell users at login. When this feature is enabled, the password is required of all shell users (rather than each user having a separate account) from the time it is set or changed. In the CTC node view, Provisioning > Security > Access tabs, check the “Enable Shell Password” check box to enable the shell password feature. The password can then be set or changed in a telnet or SSH shell session using the “passwd” command.



#### Note

---

The password should be 8 characters or less to avoid possible conflicts with certain FTP clients.

---

### Provisionable Patchcord Tab

Release 5.0.x features a Provisionable Patchcord subtab in CTC that displays physical links and their associated protection types, so that, when a control channel cannot be terminated on either end of a physical link, and as a result, the physical link cannot be automatically discovered by OSPF, you can still view the physical link and its protection type in the management software interface. You can view the physical links and their terminations from the CTC network view > Provisioning > Provisionable Patchcords tabs; or from the CTC node view > Provisioning > Comm Channels > Provisionable Patchcords tabs. To provision the patchcord, you select the Node Name, Slot, Port, and ID for both ends of the physical link. The ID is a unique 16-bit number used to identify a virtual link on a node. IDs are only unique for the particular node.

### Date Format Selection

Release 5.0.x adds a date format option to CTC, enabling you to choose between U.S. (MM/DD/YY) and European (DD/MM/YY) date formats. To choose the date format, click the Edit menu and choose Preferences. Select the desired date format (the default is MM/DD/YY) and click OK. The name/value pair (“ctc.dateFormat=DD/MM/YY” or “ctc.dateFormat=MM/DD/YY”) will be updated in the `ctc.ini` (Windows), or `.ctcrc` (UNIX) file, where preferences are stored. Subsequently, the date format used in all tables, dialogs, and tabs will be changed to the format you selected in the Preferences dialog.

### TL1-CTC Circuit Unification

In Release 5.0.x CTC fully supports TL1-created circuits and TL1 fully supports CTC-created circuits. Release 5.0.x circuit behavior and appearance is unified across both management interfaces, and you can easily alternate between the two. It is also no longer necessary to upgrade a TL1 circuit for CTC, or to downgrade a CTC circuit for TL1. The following circuit unification enhancements are supported with Release 5.0.x.

- Release 5.0.x cross-connects can be given names via TL1 using ENT-CRS and ED-CRS (use the “CKTID” parameter).

- CTC-created circuits can now be fully deleted if all cross-connects are deleted via TL1. (Deleting a source node cross-connect automatically deletes the CTC “circuitInfo” database object.)
- VCAT group objects (VCGs) can be given names via TL1 using ENT-VCG and ED-VCG commands (with the “CKTID” parameter).
- CTC-created VCAT circuits can now be fully deleted if both VCGs are deleted via TL1. (Deleting a source node VCG automatically deletes the CTC “circuitInfo” database object.)
- TL1 circuits now have names (like CTC circuits).
- You can use TL1 to change the name of any circuit, TL1-created or CTC-created.
- Low order (LO) tunnels and LO aggregation point circuits created via TL1 are now recognized and displayed in CTC.
- You can use TL1 to add cross-connects to a CTC-created circuit.
- You can edit TL1 circuits using CTC. (No need for upgrading the circuit first.)
- Circuit “upgrade” and “downgrade” functions have been removed.
- You can merge two or more CTC circuits into a single CTC circuit. (Circuit Merge and Circuit Reconfigure.)
- “ACTIVE” circuits are now called “DISCOVERED.”
- “INCOMPLETE” circuits are now called “PARTIAL.”
- “UPGRADABLE” circuits are now called “DISCOVERED\_TL1.”
- “INCOMPLETE\_UPGRADABLE” circuits are now called “PARTIAL\_TL1.”

## New Software Features and Functionality as of Release 4.7

### Enhanced State Model

Releases 4.7 and 5.0.x introduce new administrative and service states for Cisco ONS 15454 SDH cards, ports, and cross-connects. Administrative and service states are based on the generic state model defined in Telcordia GR-1093 Core, Issue 2 and ITU-T X.731 and are available for all support management interfaces. The following state types and state transition types are defined for Release 5.0.x. Consult the Cisco ONS 15454 SDH Reference Manual for specific states and their applications.

#### Service States

Service states include a Primary State (PST), a Primary State Qualifier (PSTQ), and one or more Secondary States (SST).

#### Administrative States

Administrative states are used to manage service states. Administrative states consist of a PST and an SST. A change in the administrative state of an entity does not change the service state of supporting or supported entities.

#### Service State Transitions

The possible transitions from one service state to the next state for cards, ports, and cross-connects. A service state transition is based on the action performed on the entity and any autonomous activity.

### Card Service State Transitions

The service state transitions for cards.

### Port and Cross-Connect Service State Transitions

Port states do not impact cross-connect states with one exception. A cross-connect in the Unlocked-disabled,automaticInService service state cannot transition autonomously into the Unlocked-enabled service state until the parent port is Unlocked-enabled.

The following ports do not support all of the service states:

- E-Series Ethernet ports do not support service states; these ports are either enabled or disabled.
- FC\_MR-4 ports support the Unlocked-enabled; Locked-enabled,disabled; and Locked-enabled,maintenance service states; they do not support the Unlocked-disabled,automaticInService service state.

## Circuit State Model

Releases 4.7 and 5.0.x add support for circuit service and administrative states in CTC. For more information consult the user documentation.

## ROADM

ROADM allows you to add and drop wavelengths without changing the physical fiber connections. ROADM technology is useful in network applications that require the ability to optically pass DWDM wavelengths without a physical fiber jumper. Release 4.7/5.0.x ROADM also provides channel equalization allowing all 32 wavelengths to be optically balanced. Release 4.7/5.0.x ROADM offers significant insertion loss reduction over previous back-to-back multiplexing or demultiplexing solutions. Configurations using ROADM support up to 16 node rings.

ROADM technology in Release 4.7/5.0.x also supports any-to-any connection capability, spans from 1 dB to 15 dB, and SONET, data, or video multirate traffic.

### Any-to-Any Rings

The any-to-any ring topology contains only ROADM nodes. Optical service channel (OSC) regeneration or amplifier nodes can be installed between ROADM nodes, if required. This topology potentially allows you to route every wavelength from any source to any destination node inside the network.

For optical performance information for ROADM rings and linear networks refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## New Node Types

Releases 4.7 and 5.0.x provide support for the following new node types.

### ROADM Node

ROADM nodes are equipped with at least one 32-Channel Wavelength Selective Switch (32WSS). A 32DMX or 32DMX-O demultiplexer can be installed, but is not required. For ROADM node installation options, management, and turnup, consult the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### ROADM Power Equalization Monitoring

Reconfigurable OADM (ROADM) nodes allow you to monitor the 32WSS card equalization functions on the **Maintenance > DWDM > Power Monitoring** subtab. The tab compares the input channel power Add (Padd) and express or pass-through (Ppt) with the power level at output (Pout).

### OSC Regeneration Line Site

A Release 4.7/5.0.x OSC Regeneration line site can be built using two OSC-CSMs for the single purpose of providing an electrical regeneration of the OSC channel.

MetroPlanner plans an OSC regeneration site every time there is a link longer than 37 db on which payload amplification or add and drop capabilities are not required.

NDT splits this link into n sublinks of maximum length 31 dB, then places an OSC regeneration site between each sublink and the next, as needed.

Although it is not commonly the case (due to the span length), in a limited set of cases the OSC Regeneration site can be crossed by pass through traffic (for example single channel 2.5 Gbs).

The OSC Regeneration Site feature also supports hybrid configurations.

### HUB or Terminal Nodes with 32WSS and 32DMX

The 32WSS and 32DMX are normally installed in ROADM nodes, but they can be installed in hub and terminal nodes, as well. If the cards are installed in a hub node, the 32WSS express (EXP RX and EXP TX) ports are not cabled.

### Provisioning Parameters for Terminal and HUB Sites

On Hub and Terminal sites, ANS algorithms require setting a value for VOA Target Channel Power (TPVOACh(i)) on all demultiplex and multiplex paths. Specifically, Hub and Terminal Site setup requires the use of the following parameters.

- West/East Side Add and Drop Stage Output Power [WestPoutad; EastPoutad]
- West/East Side Add and Drop Stage Input Power [WestPinad; EastPinad]
- West/East Side Add and Drop Stage By-Pass Power [WestPby-passad; EastPby-passad]
- West/East Side Add and Drop Stage Channel (i) Drop Power (for i = 1..32) [WestPDropCh(i); EastPDropCh(i)]
- West/East Side Add and Drop Stage Drop Power [WestPDrop; EastPDrop]

WestPdrop and EastPdrop are used when the 32-DMX West or East is equipped. WestPDropCh(i) and EastPDropCh(i) are used when the 32DMX-O West or East is equipped.

For a terminal site only one set (East or West) of these parameters is used according to the node line direction:

- East side parameters in the case of terminal site West
- West side parameters in the case of terminal site East

For further details on these and other Hub and Terminal site parameters, consult the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Y-Cable Protection

Y-cable protection is available for the following ONS 15454 transponder and muxponder cards:

- TXP\_MR\_10G
- TXP\_MR\_2.5G
- MXP\_MR\_2.5G
- MXP\_2.5G\_10G

In Y-cable protection, the client ports of the two cards are joined by Y-cables. A single receive client signal is injected into the receive Y-cable and is split between the working and protect cards in the protection group. The transmit client signals from the two protection group cards are connected via the transmit Y-cable with only the active card signal passing through as the single transmit client signal. The other card must have its laser turned off to avoid signal degradation where the Y-cable joins. To create Y-cable protection, first create a Y-cable protection group for two TXP or MXP cards using CTC, then connect the client ports of the two cards physically with a Y-cable. The single client signal is then sent into the receive Y-cable and is split between the two TXP or MXP cards.

## Automatic Laser Shutdown

With Release 4.7/5.0.x Automatic Laser Shutdown (ALS) is supported on both the client and trunk interfaces. On the client interface, ALS is compliant with ITU-T G.664 (6/99). On the data application and trunk interface, the switch on and off pulse duration is greater than 60 seconds. The “on” and “off” pulse duration is user-configurable.

## MSTP Fiber Support

Release 4.7/5.0.x provides qualification of MSTP over the following fibers in addition to SMF-28.

- FiberSupported ConfigurationsNode typology
- SMF-28RingHub
- E-LeafLinearActive OADM
- TW-RSLinear w/o OADMPassive OADM

For further information on use of these fibers with Release 5.0.x consult the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## OC3/STM1 Performance Monitoring for OSCM and OSC-CSM Cards

The following new PMs are supported in Releases 4.7 and 5.0.x for OC3/STM1 facility equipped on OSCM and OSC-CSM cards.

### SONET

Number of Coding violations (CV).

- CV-S: section
- CV-L-NE: line near end
- CV-L-FE: line far end

Number of Error seconds (ES).

- ES-S: section
- ES-L-NE: line near end
- ES-L-FE: line far end

Number of Severely Error Seconds (SES).

- SES-S: section
- SES-L-NE: line near end
- SES-L-FE: line far end

Number of Severely Error Framing Seconds (SEF).

- SEF-S: section

Unavailable Seconds (UAS).

- UAS-L-NE: line near end
- UAS-L-FE: line far end

Failure Counts (FC).

- UAS-L-NE: line near end
- UAS-L-FE: line far end

## SDH

Error Blocks (EB). A block in which one or more bits are in error.

- EB-RS: regeneration section
- EB-MS-NE: multiplex section, near end
- EB-MS-FE: multiplex section, far end

Background Block Errors (BBE). An error block not occurring as part of an SES.

- BBE-RS: regeneration section
- BBE-MS-NE: multiplex section, near end
- BBE-MS-FE: multiplex section, far end

Errored Seconds (ES). A one second period with one or more errored blocks or at least one defect.

- ES-RS: regeneration section
- ES-MS-NE: multiplex section, near end
- ES-MS-FE: multiplex section, far end

Number of Severely Error Seconds (SES).

- SES-RS: regeneration section
- SES-MS-NE: multiplex section, near end
- SES-MS-FE: multiplex section, far end

Unavailable Seconds (UAS).

- UAS-MS-NE: multiplex section, near end
- UAS-MS-FE: multiplex section, far end

## System Type Removal

Release 4.7 and forward removes the System Type parameters, System Type West and System Type East. These parameters are replaced in Releases 4.7 and forward with the following four pairs of parameters:

- West Side Tx Amplifier Working Mode ([dwdm.tx.amp.WkgModeW]) and West Side Tx Amplifier Ch Power ([dwdm.tx.amp.ChPwrW]), applicable for all OPT-BST facing west.
- West Side Rx Amplifier Working Mode ([dwdm.rx.amp.WkgModeW]) and West Side Rx Amplifier Ch Power ([dwdm.rx.amp.ChPwrW]), applicable for all OPT-PRE facing west.
- East Side Tx Amplifier Working Mode ([dwdm.tx.amp.WkgModeE]) and East Side Tx Amplifier Ch Power ([dwdm.tx.amp.ChPwrE]), applicable for all OPT-BST facing east.
- East Side Rx Amplifier Working Mode ([dwdm.rx.amp.WkgModeE]) and East Side Rx Amplifier Ch Power ([dwdm.rx.amp.ChPwrE]), applicable for all OPT-PRE facing east.

For further details on these new parameters and their uses, consult the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## LOS-P Threshold Configuration on OPT-BST/OSC-CS/OPT-PRE COM-RX Port

Release 4.7/5.0.x LOS-P Threshold configuration provides the following ANS provisioning parameters:

- West Side Fiber Stage Input Threshold [WestFSInTh]
- East Side Fiber Stage Input Threshold [EastFSInTh]
- West Side Rx Amplifier Input Power Fail Threshold [WestRxAmpInPwrFailTh]
- East Side Rx Amplifier Input Power Fail Threshold [EastRxAmpInPwrFailTh]
- Release 4.7/5.0.x ANS sets:
  - LOS-P Threshold on West OPT-BST LINE-1-RX port, or West OSC-CSM LINE-1-RX to WestFSInTh
  - LOS-P Threshold on East OPT-BST LINE-1-RX port, or East OSC-CSM LINE-1-RX port to EastFSInTh
  - LOS-P Threshold on West OPT-PRE LINE-1-RX port to WestRxAmpInPwrFailTh
  - LOS-P Threshold on East OPT-PRE LINE-1-RX port to EastRxAmpInPwrFailTh

## Circuit Size Label Removed from OCHNC Circuits

The circuit size specification or modification option is no longer supported for any of the interfaces, as follows.

- CTC Circuit Creation wizard
- CTC Edit Circuit function
- TL1 commands for OCHNC x-connection creation
- TL1 commands for OCHNC x-connection editing

## Wavelength Path Provisioning Changes

The following changes have been made for Wavelength Path Provisioning (WPP). Consult the *Cisco ONS 15454 DWDM Installation and Operations Guide* for details.

- Warning message for last OSC deletion
- Conditions when last OSC cannot be deleted are listed

## Calibration Value by Port Service State

As of Release 4.7 you can modify calibration values independently by port service state, with the exception of amplifier Offset (former power calibration), when the OPT-BST LINE-3-TX LINE-1-RX or OPT-PRE LINE-1-TX is in IS-NR service state.

The following table summarizes the calibration functions that can be performed in the different service states.

**Table 5 Calibration Functions**

Function	IS-NR	OOS-AU,AINS	OOS-MA,DSLBD	OOS-MA,MT
Offset	No	Yes	Yes	Yes
VOA Attenuation Calib	Yes	Yes	Yes	Yes
VOA Power Calib	Yes	Yes	Yes	Yes

## New Alarms and Conditions

The following alarms and conditions are new for Release 4.7/5.0.x. For details consult the *Cisco ONS 15454 SONET and DWDM Troubleshooting Guide*.

- New LOS-P, LOS-O alarms
- New PARAM\_MISM condition
- OSRI ON raises conditions in specific instances
- ALS standing condition is revised

## New CTC Functionality

### ANS Provisioning Tab

In Release 4.7/5.0.x CTC, ANS NE Update and Provisioning tabs have been removed and merged in a new pane having a tree format. Parameters in tree view are organized according to four main layout sectors: West RX, West TX, East RX and West TX. In each sector parameters are grouped according to their type category: amplifier, thresholds, power.



#### Note

The System type has been removed. See the [“System Type Removal” section on page 63](#).

Only parameters applicable for the node type are presented in the tree view. By using the Import button can load a MetroPlanner provisioning file. Provisioning information can be exported in two formats: for a future import (by Export button), for node commissioning (csv/tsv/html) by selecting from the **File > Export** menu. All settings will become effective only after having launched the ANS application.

### ANS Results Report

For every MSTP port for which a regulation is required, ANS provides details about parameters set or unset.

Possible results values are:

- “Success - Changed” when a calculated set-point differs from the old one

- “Success - Unchanged” when a calculated set-point is equal to the old one
- “Fail - Out of Range” when a calculated set-point is outside of the acceptable range
- “Fail - Port in IS state” when the set-point cannot be applied because port is in service
- “Not Applicable” when the set-point is not calculable for that particular node layout

## OCHNC Bidirectional Circuits

In release 4.6.x OCHNC bidirectional circuit support existed in the creation wizard only. Creation of a bidirectional circuit in the wizard resulted in the actual creation of two unidirectional circuits with no link between them. Releases 4.7 and forward add full support for bidirectional circuits both in CTC and in the TL1 interface. OCHNC bidirectional circuit forward and reverse components always use the same wavelength and always cross the same optical path. Support for unidirectional circuits remains unchanged.

## Changes to Automatic Power Control

### APC Interface

Release 4.7/5.0.x enables you to manually launch, enable, or disable APC. These functions can be performed upon any network node, by CTC or TL1.



#### Note

---

The APC interface is a maintenance function for use by maintenance personnel. Improper use of this function can have undesirable effects at the network level.

---

### APC States

An “APC State” flag indicates the APC working condition for all nodes in a given network. The APC state flag can be any of the following values.

- “Disable - Internal”—Displayed when APC has been automatically disabled for an internal cause.
- “Disable - User”—Displayed when APC has been disabled by the user.
- “Not Applicable - Network Type”—Displayed when the Network Type is set to “Not DWDM” or “Metro Access,” types that do not support the APC application.
- “Enable”—Displayed when APC is enabled.

### APC Outputs

CTC and TL1 users can retrieve “Last monitored time” and “Last modified time” for every parameter whose set point is monitored by APC. APC updates the last check time value every time it checks a parameter set point for correctness. APC updates the last modification time value every time it modifies the parameter set point. Last check time and Last modification time will then be displayed on the CTC and TL1 interfaces only for those parameters effectively checked by APC. This implies that parameters associated to ports that are not in IS-NR service state will not be reported (since they are not carrying traffic).

## Span Loss Check

The Release 4.7/5.0.x Network Design Tool guarantees optical performance on a given span if its length is included between two values:

- Start of Life (SoL)—A span loss value provided by the user
- End of Life (EoL)—A span loss value given by the SoL plus aging margins

Release 4.7/5.0.x also provides a measurement of actual span loss in field, comparing the far end OSC power with the near end OSC power. This measurement can be performed in every MSTP node because for each such node OSC channel is regenerated.

From a network management point of view, span loss measurement can be useful when equipment is installed, or anytime a fiber is repaired after a cut. The NE will raise the Span Loss Out of Range Transient Condition on CTC, TL1 and SNMP interfaces when the measured span loss is higher than the maximum expected span loss, or when it is lower than the minimum expected span loss, and the difference between the MaxExpSpanLoss and MinExpSpanLoss is greater than 1 dB. The condition is not raised in case of a software release upgrade. The maximum and minimum expected span loss data is provided by MetroPlanner and provisioned via the CTC or TL1 interface. Expected and Measured span loss are displayed in the tool-tip associated with the particular link in the Network View.

### Optical Channel Graphical Equalizer

In an ROADM node you can monitor the 32-WSS equalization functions comparing channel power level at the input ports (ADD(i) and EXP-RX) with channel power level at the output port (COM-TX). You can access this feature every time a 32-WSS is equipped or provisioned; however, the feature's use in Hub and Terminal site configurations is not warranted, since these nodes do not allow provisioning of pass-through traffic.

Line direction is identified by a double notation:

- Functional (W->E and E->W)
- Physical (slot/port on which both incoming and outgoing signals are associated)

### New Provisioning Interface for Amplifiers

The CTC interface for the OPT-PRE and OPT-BST amplified port in the card view > **Provisioning** tab is modified for Releases 4.7 and forward for thoroughness and readability as follows.

- Working Mode—Control Power or Control Gain. This is set by ANS.
- Signal Output Power—ASE compensated power value.
- Total Output Power—Sum of ASE and signal power.
- Total Output Power Set-Point—Power set point, applicable only if the working mode is control power.
- Gain—Applicable only when the working mode is control gain.
- Gain Set Point—Gain set-point calculated by APC or user-provided via the ANS interface.
- Offset—This is the former “Power Calibration,” applicable for both amplifier working modes.
- Per Channel Power Reference—Set by ANS.
- Tilt Reference—Set by ANS.
- Tilt Calibration—Read and write parameter used to modify the amplifier tilt.

### Pluggable Port Module Support

Release 4.7/5.0.x CTC provides a new “PPM” subtab in the Provisioning tab of the card view for the transponder, and muxponder cards. This tab enables you to provision the pluggable port modules (PPMs) for SFPs (with a muxponder) and XFPs (with a transponder). When you create a PPM you can choose the slot number for the SFP or XFP, and then choose the appropriate PPM type for that card, selecting as many ports as you wish within the range of supported ports for the card. For specific instructions on provisioning PPMs, consult the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## Buffer-to-Buffer in CTC

Release 4.7/5.0.x CTC supports the following features related to buffer-to-buffer technology.

- CTC enables distance extension (B2B).
- CTC allows Autodetect, or manual setting of the client buffer credit.

## MetroPlanner 2.5



### Note

---

DWDM operation requires that you have a network plan calculated for your DWDM network with Cisco MetroPlanner, Release 2.5. Cisco MetroPlanner is a DWDM planning tool that is available from your Cisco account representative. Cisco MetroPlanner prepares a shelf plan for each network node and calculates the power and attenuation levels for the DWDM cards installed in the node. For information about Cisco MetroPlanner, contact your Cisco account representative. For more information about MetroPlanner, refer to the Cisco MetroPlanner DWDM Installation and Operations Guide, Release 2.5.

---

Release 4.7/5.0.x integrates the ability to use Cisco MetroPlanner 2.5. The primary purpose of MetroPlanner is to assist sales engineers (SEs) in the design and validation of optical networking deployment using Cisco Optical Networking System (ONS) platforms. MetroPlanner provides a means to construct and test optical networks in a modelled graphical environment, enabling you to efficiently model multiple network design options for customers across a wide range of Cisco optical network products. You can enter specific configurations, or site distances alone, and from them build the desired network type. You can enter topology and service requirement specifications, then choose the type of platform or equipment for the network design. Several solutions can correspond to one type of equipment or platform. The MetroPlanner graphical user interface (GUI) models general specifications and produces detailed BOMs to provision optimized networks. Using MetroPlanner you can verify multiple constraints such as optical budget limitations and platform architecture. MetroPlanner automatically models and tests both simple and complex optical network designs. Optical networks designed using MetroPlanner can take advantage of the availability of dark fiber to build a common infrastructure that supports data, storage area network (SAN), and time-division multiplexing (TDM) traffic.

## Topology Support

MetroPlanner supports the following network topologies.

- Bus (single span, point-to-point, and linear)
- Open (or hubbed) ring
- Closed (or meshed) ring

## Protection Scheme Support

MetroPlanner designs support the following protection schemes.

- Client-based 1+1 protection
- Fiber switched protection
- Y-cable protection
- Unprotected

## Service Support

Depending on the platform selected, MetroPlanner can support any subset of the following services.

- 2R Any Rate
- Gigabit Ethernet
- 10 Gigabit Ethernet
- Enterprise System Connection (ESCON)
- Fibre Channel
- Fibre Channel 2G
- Fast Ethernet
- FDDI
- STM-1
- STM-4
- STM-16
- STM-64
- OC-3
- OC-12
- OC-48
- OC-192
- Inter-System Channel (ISC)
- Sysplex Control Link Oscillator (CLO)
- Sysplex External Throughput Rate (ETR)
- D1 Video
- Serial Data Input (SDI)
- Fiber Connection (FICON)
- FICON 2G
- HDTV
- Reserved

## TL1

In Releases 4.5 and 4.6.x only TL1 test access was available for the ONS 15454 SDH platform. As of Releases 4.7 and 5.0 the full range of TL1 commands is available. For specific commands, syntax, and their uses, consult the *Cisco ONS SDH TL1 Command Guide*.

# Related Documentation

## Release-Specific Documents

- *Release Notes for the Cisco ONS 15454 SDH, Release 5.0.2*
- *Release Notes for the Cisco ONS 15454, Release 5.0.4*
- *Release Notes for the Cisco ONS 15327, Release 5.0.4*
- *Release Notes for the Cisco ONS 15600, Release 5.0.4*
- *Release Notes for the Cisco ONS 15310-CL, Release 5.0.4*
- *Cisco ONS 15454 SDH Software Upgrade Guide, Release 5.0.2*

## Platform-Specific Documents

- *Cisco ONS 15454 SDH Procedure Guide*  
Provides installation, turn up, test, and maintenance procedures
- *Cisco ONS 15454 SDH Reference Manual*  
Provides technical reference information for SONET/SDH cards, nodes, and networks
- *Cisco ONS 15454 DWDM Installation and Operations Guide*  
Provides technical reference information for DWDM cards, nodes, and networks
- *Cisco ONS 15454 SDH Troubleshooting Guide*  
Provides a list of SONET alarms and troubleshooting procedures, general troubleshooting information, and hardware replacement procedures
- *Cisco ONS SDH TL1 Command Guide*  
Provides a comprehensive list of TL1 commands

# Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

## World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

## Documentation CD-ROM

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

## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

## Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

### Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/en/US/support/index.html>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

### Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

---

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2005, Cisco Systems, Inc.  
All rights reserved.