



# Release Notes for Cisco ONS 15454 SDH Release 6.0.3

---



## Note

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

---

## August 2007

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15454 SDH multiplexer. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to the “Release 6.0” version of the *Cisco ONS 15454 DWDM Installation and Operations Guide*; and the “Release 6.0” 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 6.0.3*, visit the following URL:

[http://www.cisco.com/en/US/products/hw/optical/ps2006/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/hw/optical/ps2006/prod_release_notes_list.html)

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

<http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs>

## Contents

- [Changes to the Release Notes, page 2](#)
- [Caveats, page 2](#)
- [Resolved Caveats for Release 6.0.x, page 25](#)
- [New Features and Functionality, page 30](#)
- [Related Documentation, page 67](#)



---

### Corporate Headquarters:

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

Copyright © 2007 Cisco Systems, Inc. All rights reserved.

[Obtaining Documentation and Submitting a Service Request, page 67](#)

## Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15454 SDH Release 6.0.3* since the production of the Cisco ONS 15454 SDH System Software CD for Release 6.0.3.

No changes have been added to the release notes for Release 6.0.3.

## 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.

### 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.

### 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.

## 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.

## 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.

---

## 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 not be resolved.

## 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

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



Caution

---

Before you upgrade to Release 6.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, 5.x or 6.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 6.x, 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 6.x. Current settings are displayed in CTC (whether they were inherited from an upgrade, or they were set using the current GUI).

## CSCei67897

Rarely, autoprovisioned audits (those with the unique ID of 0) can become stranded after a bulk roll of VC LO circuits prior to deletion of those circuits. If an attempt was made previously to delete all such circuits, you can use subtractive logic to discover which circuits have become stranded. That is, matrices indicating usage in the node view, Maintenance > Cross-connect > Resource Usage window will indicate stranded circuits.

Once you have identified that there are stuck STSs, go to the card view for each affected trunk card and view the Maintenance > Loopback > SDH STS tabs. From here you can view all used STSs, including any stuck STSs. Determine which STSs in your network have no circuit associated with them, then create and subsequently delete a LO circuit on each affected STS. This will clean up the stuck STSs. This issue is resolved in Release 7.0.

## CSCeh84908

A CTC client session can disconnect from an ONS node during simultaneous deletion of large numbers of VT level circuits (3000+). Connectivity to the node will recover without any user action. If the condition persists, restart the CTC session to reconnect. This issue is under investigation.

## CSCin92246

When one of the underlying connections of a circuit moves to the Unlocked-disabled, failed state, CTC treats the Unlocked-disabled, failed state as out of service and interprets part of the circuit to be out of service, or Locked. However, this is incorrect, as none of the underlying connections is in a Locked state. The result is that the circuit state is displayed as Locked[Partial], even though all of the underlying connections are technically Unlocked. This issue is resolved in Release 8.0.

## CSCin90057

A signal degrade or signal failure is not reported when you inject bit errors into the line for an E3 card. To see the SD or SF, inject a code violation error instead. This issue will not be resolved.

## CSCeh92201

When you create a bidirectional MS-SPRing-SNCP IDRI circuit using autorouting and select the PCA option for secondary spans, the circuit is created over working MS-SPRing spans and does not use PCA spans. To enforce the use of the PCA option, provision the circuit using manual routing. This issue will not be resolved.

## 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 is resolved Release 7.0.

## 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 not be resolved.

## 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.

## 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 is resolved in Release 7.0.

## 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.

## 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.

## 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.

## 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. This issue will not be resolved.

## 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 will not be resolved.

## CSCeb39359

When changing NE timing from External or Mixed to Line timing, a Transient IEF alarm might be reported against the standby XC10G. This issue will be resolved in a future hardware release.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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

## 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.

## 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

### 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 not be resolved; however, this does not occur when the newer optical line cards, TCC2P cards, and XC-VXC cards are used.

## 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

### 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 not be resolved.

### 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. This issue will not 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).

## Electrical IO Cards

### 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 cannot be resolved.

### 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.

### CSCeg19255

Rarely, DS3I VC3 traffic takes a hit greater than 60 ms during a cross connect card soft reset. This issue will not be resolved; however, a node configured with the latest line cards, XC-VXC cards, and TCC2P cards, and with Release 6.0.x will not exhibit this behavior.

### 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.

### 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 a future release.

## 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

### CSCei37691

The trunk port service state for the TXPP and TXP cards does not transition to unlocked-disabled,failed in the presence of an LOS-P alarm. This can occur when the payload signal for LOS-P is missing for the particular port type. This issue will be resolved in a future release.

### CSCuk57046

An unexpected Mismatch Equipment Attributes (MEA) transient alarm can occur on rapidly inserting and removing a PPM. This issue can occur with a TXP\_MR\_10E-L for which you preprovision an OC-192 PPM. The transient alarm is raised on the PPM. This issue is resolved in Release 7.0.

### CSCeh94567

Setting a Terminal loopback on an MXP-2.5G-10G trunk port causes OTUK alarms.

This can occur under the following conditions.

1. Two MXP-2.5G-10G cards are connected via the trunk ports.
2. The client ports are connected to respective STM16 line cards.
3. SDCC is enabled on the client ports and the line cards' STM16 port.
4. A terminal loopback is set on the MXP-2.5G-10G trunk port.

This terminal loopback causes OTUK-LOF and OTUK-IA alarms to be reported on both MXP-2.5G-10G trunk ports. This issue will not be resolved.

### 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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. This issue will not be resolved.

## 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.

## CSCuk51185

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

## 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.

## 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 not be resolved.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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. This issue will not be resolved.

## 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 Tspd cards have G709 and FEC on. If the cards have G709 and FEC off, only the near end counts will increment, as expected.

## 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.

## 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.

## 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.

## 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.

## 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.

## CSCea87290

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

## 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.

## 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

### 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
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
CE-100T-8	8 port 10/100FE Ethernet Module
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

**Table 3** SONET Data Cards that are SDH Compatible (Continued)

Product Name	Description
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

## CSCsb40206

In Asymmetric configuration, with autonegotiation enabled and flow control selected, an ML-series card might fail to synchronize with, or to recognize the asymmetric flow control. This issue is under investigation.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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.

## CSCea01675

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

## 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 not be resolved.

## 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. This issue will not be resolved.

## 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.

## 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

### 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 not be resolved.

### 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 not be resolved.

## 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

### CSCee65471

Rarely, during a software upgrade of a passthrough node in an MS-SPRing, the VC3 traffic on a DS31 card might incur a traffic hit. This issue will be resolved in a future release.

### 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.

### CSCdw53481

Two MS-SPRings 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.

### 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.

### 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.

## 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

### 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 not be resolved.

### 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 not be resolved.

## Active XCVXL or TCC2/TCC2P Card Removal

As in MS-SPRing, 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

### 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.

## Bridge and Roll

### CSCei37364

When a rollTo leg is not receiving a good signal, and because of this the rollPending alarm is not cleared, there is no alarm indicating the reason that the RollPending alarm fails to clear. This issue is resolved in Release 7.0.

## Resolved Caveats for Release 6.0.x

This section highlights resolved caveats for Release 6.0.x.

## Hardware

### CSCsb77209

Split route circuits on some FC\_MR-4 cards will take some errors at -5C to +10C ambient temperatures. This issue is resolved in Releases 6.0.1, 6.1, and 7.0.

### CSCsi29405

Some fan trays exhibit high electrical noise which causes communication loss between the fan tray and the controller card. Eventually, this causes the controller card to reboot. The noise is proportional to the voltage level of the shelf and inversely proportional to the speed of the fans.

Workaround: Allow the fan trays to run at high speeds. There is considerable reduction in the noise. This issue is resolved in 6.03, 7.05, and 7.23.

## Maintenance and Administration

### CSCsb70881

In a DWDM node the alarm correlation at node level does not work. This issue can be seen in the presence of an upstream alarm. This issue is resolved in Release 6.0.1.

### CSCsb80734

It is not possible to create a second circuit in a metro access network. This issue is resolved in Release 6.0.1.

### CSCsb80699

In a metro access network the amplifiers don't switch to constant gain. This issue can be seen when recreating a circuit previously deleted without re-executing ANS. Relaunching ANS manually every time avoids this issue. This issue is resolved in Release 6.0.1.

### 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.

### CSCei60452, CSCei43450

Occasionally you might be unable to launch CTC or connect to the NE via http or https if you have not first deleted the CTC cache and closed all open web browser sessions prior to opening a new CTC version. If you experience this issue, in the browser window where CTC was loaded, click Delete CTC Cache, then close all instances of that browser. Ensure that no browser processes remain active (you can check this in the Windows Task Manager) before launching a new browser session and subsequent CTC session. This issue is resolved in Release 6.0.

### 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 is resolved in Release 6.0.

**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 support low order VT thresholds.

**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 is resolved in Release 6.0.

**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 is resolved in Release 6.0.

**Common Control and Cross Connect Cards****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. This issue is resolved in Release 6.0 with the XCVXC card.

**DWDM Cards****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 is resolved in Release 6.0.

**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 is resolved in Release 6.0.

## 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 is resolved in Release 6.0.

## Electrical IO Cards

### 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 is resolved in Release 6.0.

### 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 is resolved in Release 6.0.

## Data IO Cards

### 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 is resolved in Release 6.0.

## 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040827-telnet>

This issue is resolved in Release 6.0.

## 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 is resolved in Release 6.0.

## 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 6.0.

## 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 is resolved in Release 6.0.

## 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 is resolved in Release 6.0.

## CSCeg30605

The diagnostics information provided for ML cards in the diagnostic file is incomplete. This issue is resolved in Release 6.0.

## MS-SPRing Functionality

### CSCeh08553

A two-fiber MS-SPRing protection switch generates an AU-LOP alarm on a one way VC12 circuit. This issue is resolved in Release 6.0.

## 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 is resolved in Release 6.0.

## SNCP Functionality

### CSCsh77496

If path protection/SNCP circuits are created while path defects are present on path protection/SNCP trunks, then sometimes path protection/SNCP circuits may not switch and traffic outage is observed

Workaround: Avoid creating path protection circuits while faults are present on either of the path protection trunks ports. This issue is resolved in 6.03, 7.05 and 7.2.3

### 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 is resolved in Release 6.0.

### 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 is resolved in Release 6.0.

## Online Help

### 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 is provided in Release 6.0.

## 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

### XC-VXC-10G Card

Release 6.0.x introduces the XC-VXC-10G card. You can upgrade to the XC-VXC-10G from XC-VXL-10G or XC10G cards (as described in the user documentation). Upgrading a system to XC-VXC-10G from an earlier cross-connect module type is performed in-service, with hitless operation (less than 50-ms impact to any traffic).

The XC-VXC-10G card establishes connections at the VC-4, VC-3, VC-12, and VC-11 levels. The XC-VXC-10G cards provides STM-64 capacity to Slots 5, 6, 12, and 13, and STM-16 capacity to Slots 1 to 4 and 14 to 17. VC-4 cross-connections are nonblocking, so any VC-4 on any port can be connected to any other port.

The XC-VXC-10G card can be configured to support either full VC-12 or VC-11 grooming, or mixed (VC-12 and VC-11) grooming.

The XC-VXC-10G card is supported in redundant configuration only.

### XC-VXC-10G Functionality

The XC-VXC-10G card manages up to 192 bidirectional VC-4 cross-connects, 192 VC-3 bidirectional cross-connects, 1008 VC-12 bidirectional cross-connects, or 1344 VC-11 bidirectional cross-connects. The TCC2/TCC2P card assigns bandwidth to each slot on a per-STM-1 basis.

The XC-VXC-10G card provides the following:

- 384 VC-4 bidirectional ports
- 192 VC-4 bidirectional cross-connects
- 384 VC-3 bidirectional ports
- 192 VC-3 bidirectional cross-connects
- 2016 VC-12 ports by means of 96 logical VC-3 ports
- 1008 VC-12 bidirectional cross-connects
- 2688 VC-11 ports by means of 96 logical VC-3 ports
- 1344 VC-11 bidirectional cross-connects
- Nonblocking operation at the VC-11 level
- VC-11, VC-12, VC-4/-4c/-8c/-16c/-64c cross-connects

### XC-VXC-10G Compatibility

The XC-VXC-10G card supports the same features as the XC-VXL-10G and XC-VXL-2.5G cards. The XC-VXC-10G card supports STM-64 operation.

If you are using Ethernet cards, the E1000-2-G or the E100T-G must be used when the XC-VXC-10G cross-connect card is in use.

### 15454\_MRC-12 Multirate Card

Release 6.0.x introduces the 15454\_MRC-12 multirate card. You can upgrade to a 15454\_MRC-12 card from the one port OC12/STM-4 or OC48/STM-16 card. The 15454\_MRC-12 card provides up to twelve OC-3/STM-1 ports, twelve OC-12/STM-4 ports, or four OC-48/STM-16 ports using Small Form-factor

Pluggables (SFPs), in any combination of line rates. All ports are Telcordia GR-253 compliant. The SFP optics can use SR, IR, LR, coarse wavelength division multiplexing (CWDM), and DWDM SFPs to support unrepeated spans. Refer to the user documentation for more information about SFPs.

The ports operate at up to 2488.320 Mbps over a single-mode fiber. The 15454\_MRC-12 card has twelve physical connector adapters with two fibers per connector adapter (Tx and Rx). The card supports VT payloads, STS-1 payloads, and concatenated payloads at STS-3c, STS-6c, STS-9c, STS-12c, STS-18c, STS-24c, STS-36c, or STS-48c signal levels. It is fully interoperable with the ONS 15454 SDH G-Series Ethernet cards.

The 15454\_MRC-12 port contains a transmit and receive connector (labeled) on the card faceplate. The card supports unidirectional and bidirectional facility protection. You can provision this card as part of an MS-SPRing, SNCP, or linear configuration.

### Slot Compatibility

You can install 15454\_MRC-12 cards in Slots 1 through 6 and 12 through 17 with dual XC-VXL-2.5G, XC-VXL-10G, or XC-VXC-10G cards.

The maximum bandwidth of the 15454\_MRC-12 card is determined by the cross-connect card.

For further information, ports, and line rates refer to the user documentation.

### Errorless Switching

The 15454\_MRC-12 card supports an errorless software-initiated cross-connect card switch for high order traffic (VC4) when used in a shelf equipped with XC-VXC-10G and TCC2/TCC2P cards.

## OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach Card

Release 6.0.x introduces the OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach card (also referred to as the “OC192-XFP” card). The OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach card provides a single OC-192/STM-64 interface, as follows.

- OC192SR1/STM64IO Short Reach (SR-1)
- OC192/STM-64 Any Reach (SR-1, IR-2, or LR-2)

The interface operates at 9.952 Gbps over single-mode fiber spans and can be provisioned for both concatenated and nonconcatenated payloads on a per VC-4/STS-1 basis. Specification references can be found for the OC-192/STM-64 interface in ITU-T G.691, ITU-T G.693, and ITU-T G.959.1, and Telcordia GR-253.

The optical interface for this card uses a 10-Gbps Form-factor Pluggable (XFP) optical transceiver that plugs into a receptacle on the front of the card. OC192SR1/STM64IO Short Reach is used only with an SR-1 XFP, while OC192/STM-64 Any Reach can be provisioned for use with an SR-1, IR-2, or LR-2 XFP module. The XFP SR, IR, and LR interfaces each provide one bidirectional OC192/STM64 interface compliant with the recommendations defined by ITU-T G.91. SR-1 is compliant with ITU-T I-64.1, IR-2 is compliant with ITU G.691 S-64.2b, and LR-2 is compliant with ITU G.959.1 P1L1-2D2.

### Slot Compatibility

The cards are used only in the high-speed backplane slot (slots 5, 6, 12, and 13) and only with 10 Gbps cross-connect cards, such as the XC-VXL-10G and XC-VXC-10G. The cards also must be supported with the TCC2 or TCC2P timing and control cards.

For OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach span limitations and port-level indicators consult the user documentation.

## Errorless Switching

The OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach card supports an errorless software-initiated cross-connect card switch for high order traffic (VC4) when used in a shelf equipped with XC-VXC-10G and TCC2/TCC2P cards.

## ML100X-8 Card

Release 6.0.x introduces the ML100X-8 data card. The ML100X-8 card provides eight ports with 100 base FX interfaces. The FX interfaces support one of two connectors, an LX SFP or an FX SFP. The LX SFP is a 100 Mbps 802.3-compliant SFP that operates over a pair of single-mode optical fibers and includes LC connectors. The FX SFP is a 100 Mbps 802.3-compliant SFP that operates over a pair of multimode optical fibers and includes LC connectors. For more information on the Single and Multi mode SFPs supported for the ML100X-8 consult the user documentation.

Each interface supports full-duplex operation for autonegotiation and a maximum bandwidth of 200 Mbps per port and 2.488 Gbps per card.

The card features two SDH virtual ports with a maximum combined bandwidth of VC4-16c. Each port carries an STM concatenated circuit (CCAT) with a size of VC3, VC4, VC4-2c, VC4-3c, VC4-4c, and VC4-8c. To configure an ML-Series card STM circuit, refer to the user documentation.

The ML-Series packet-over-SDH (POS) ports supports virtual concatenation (VCAT) of SDH circuits and a software link capacity adjustment scheme (SW-LCAS). The ML-Series card supports a maximum of two VCAT groups with each group corresponding to one of the POS ports. Each VCAT group must be provisioned with two circuit members. An ML-Series card supports VC-3-2v, VC-4-2v and VC-4-4c-2v. To configure an ML-Series-card VCAT circuit, refer to the user documentation.

## CE-100T-8 Card

Release 6.0.x supports the CE-100T-8 card for the ONS 15454 SDH. The CE-100T-8 card provides eight RJ-45 10/100 Mbps Ethernet ports accessible on the faceplate. The ports are numbered 1 through 8. The 10/100 Mbps Ethernet traffic on these ports map into SDH payloads for transport over the SDH infrastructure.

The CE-100T-8 card supports Generic Framing Procedure (GFP-F) and point-to-point protocol/high-level data link control (PPP/HDLC) framing protocols.

The CE-100T8 card also supports the link capacity adjustment scheme (LCAS), which allows hitless dynamic adjustment of SONET link bandwidth. The CE-100T-8 card's LCAS is hardware-based, but the CE-100T-8 also supports SW-LCAS, making it compatible with the ONS 15454 SDH ML-Series card, which supports only SW-LCAS and does not support the standard hardware-based LCAS. SW-LCAS is supported when a circuit from the CE-100T-8 terminates on the ONS 15454 SDH ML-Series card.

The CE-100T-8 supports the following SDH circuit sizes and types.

- CCAT sizes of VC-3 and VC-4
- Low order (LO) VCAT VC-3 circuit sizes of up to three members: VC-3-1v, VC-3-2v, or VC-3-3v
- Low order (LO) VCAT VC-12 circuit sizes of up to 63 members: VC-12-Nv (where N=1 to 63)

VC-3 VCAT circuits map administrative unit 4 (AU-4), and VC-12 VCAT circuits map tributary unit 12 (TU-12).

For further details about the CE-100T-8 card consult the user documentation.

## Cross-Connect and Slot Compatibility

The ML100X-8 card is compatible in Slots 1 to 6 or 12 to 17. The ML100X-8 card operates with the XC-VXL-2.5G, XC-VXL-10G, or XC-VXC-10G cross-connect cards.

For ML-Series card and circuit configuration details consult the user documentation.

## Small Form-Factor Pluggables

Release 6.0.x introduces two new SFPs that work with the new ML100X-8 data card:

- ONS-SE-100-FX
- ONS-SE-100-LX10

SFPs are integrated fiber optic transceivers that provide high speed serial links from a port or slot to the network. For more information about these SFPs refer to the user documentation.

## New Software Features and Functionality

### XC-VXC-10G Errorless Side Switching

Release 6.0.x supports errorless side switching (switching from one card on one side of the shelf to the other card on the other side of the shelf) for XC-VXC-10G cross connect cards in combination with TCC2/TCC2P control cards for high order traffic (VC4). Specifically, the following switch types and configurations are supported as errorless for high order traffic.

#### XC-VXC-10G Errorless Switch Types

- XC-VXC-10G side switch initiated through CTC or TL1
- TCC2/TCC2P side switch initiated through CTC or TL1
- Soft reboot of XC-VXC-10G or TCC2/TCC2P cards initiated through CTC or TL1



#### Note

---

Active XC-VXC-10G or TCC2/TCC2P removals are hitless but not errorless.

---

#### XC-VXC-10G Errorless Configuration

High order (VC4) traffic is errorless on the ONS 15454 SDH platform.



#### Note

---

Low order traffic is not supported for errorless side switches on the ONS 15454 SDH.

---

The following cards support errorless side switching for high order traffic when used in a shelf equipped with XC-VXC-10G and TCC2/TCC2P cards.

- The 15454\_MRC-12 card

- The OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach cards (also called OC192/STM64-XFP cards)

## 64+8kHz Clock Support

Release 6.0.x supports a new 64+8kHz clock type for the ONS 15454 SDH, per Telcordia G.703 Table II.1. The 64+8kHz clock features AMI with 8 kHz bipolar violation, and works with dual TCC2P cards. The TCC2P card supports 64K composite clock BITS in, with corresponding support for 6.312 MHz BITS out.

With Release 6.0.x you can select the 64+8kHz clock from the Facility Type selection box in the BITS Facilities subtab of the node view, Provisioning > Timing tabs.



### Note

You must have TCC2P cards installed to select the 64+8kHz clock in CTC.

The 64+8kHz clock only supports the Admin SSM. The ESF Framing “Sync. Messaging” check box will be grayed-out with only Admin SSM selection available in CTC when you select the 64K clock for BITS in. SDH nodes use the SSM Generation II message set, as follows, where STU is the default.

- STU
- G811
- G812T
- G812L
- SETS
- DUS

## 64K Clock Specific Alarms

The following alarms are supported with the 64k clock.

- LOS—Loss of Signal
- HI-CCVOLT—Composite Clock High Line Voltage
- BPV—Bipolar Violation

## FC\_MR-4 Enhanced Card Mode Differential Delay

Release 6.0.x features FC\_MR-4 differential delay support for VCAT circuits in enhanced card mode.

### Differential Delay Features

The combination of VCAT, SW-LCAS, and GFP specifies how to process information for data and storage clients. The resulting operations introduce delays. Their impact depends on the type of service being delivered. For example, storage requirements call for very low latency, as opposed to traffic such as e-mail where latency variations are not critical.

With VCAT, SDH paths are grouped to aggregate bandwidth to form VCGs. Because each VCG member can follow a unique physical route through a network, there are differences in propagation delay, and possibly processing delays between members. The overall VCG propagation delay corresponds to that

of the slowest member. The VCAT differential delay is the relative arrival time measurement between members of a VCG. The FC\_MR-4 card supports VCAT differential delay with the following associated features.

- A maximum of 122 ms of delay difference between the shortest and longest paths
- Diverse fiber routing for VCAT circuits
- All protection schemes are supported (SNCP [CCAT circuits only], MS-SPRing, protection channel access [PCA]).
- Supports routing of VCAT group members through different nodes in the SDH cloud.
- Differential delay compensation is automatically enabled on VCAT circuits that are diversely (split-fiber) routed, and disabled on VCAT circuits that are common-fiber routed.

For further information on FC\_MR-4 differential delay, consult the user documentation.

## Bridge and Roll

Release 6.0.x introduces bridge and roll for the ONS 15454 SDH. You can use the bridge and roll feature for maintenance functions such as card or facility replacement, or for load balancing. As of Release 6.0 you can perform bridge and roll operations using CTC or TL1 on all of the following ONS platforms: ONS 15454, ONS 15454 SDH, ONS 15600, ONS 15327, and ONS 15310-CL.

The CTC Bridge and Roll wizard reroutes live traffic without interrupting service. The bridge process takes traffic from a designated “roll from” facility and establishes a cross-connect to the designated “roll to” facility. When the bridged signal at the receiving end point is verified, the roll process creates a new cross-connect to receive the new signal. When the roll completes, the original cross-connects are released.

### CTC Rolls Window

The CTC Rolls window provides access to information about a rolled circuit before the roll process is complete. To view the Rolls window, click the Circuits > Rolls tabs in either network or node view.

The Rolls window provides information on the following roll states and options. For descriptions of each state or option, consult the user documentation.

- Roll From Circuit
- Roll To Circuit
- Roll State
- Roll Valid Signal
- Roll Mode (automatic or manual)
- Roll Path
- Roll From Circuit
- Roll From Path
- Roll To Path
- Complete
- Force Valid Signal

- Finish
- Cancel
- Types of Rolls

## TL1 Bulk Roll

Release 6.0.x TL1 bridge and roll features support for bulk rolling. Bulk rolling enables you to roll a subset of cross-connections from one port/facility to another port/facility.

The following TL1 commands specifically support bulk rolls. These commands support line-level rolling/bulk rolling and cannot be used for path-level rolling. For a complete list of TL1 commands supporting bridge and roll, as well as examples for each of the supported features, including bulk roll, consult the user documentation.

### **DLT-BULKROLL-<OCN\_TYPE>**

This command deletes an attempted rolling operation or completes an attempted rolling operation. The rolls that are created using the ENT-BULKROLL-<OCN\_TYPE> command can be deleted using the DLT-BULKROLL-<OCN\_TYPE> command.

### **ED-BULKROLL-<OCN\_TYPE>**

This command edits information about rolling traffic from one end point to another without interrupting service. This command can use the CMDMDE option to force a valid signal. The only parameter that can be edited is CMDMDE. The time slots cannot be edited.

### **ENT-BULKROLL-<OCN\_TYPE>**

This command enters information about rolling traffic from one end-point to another without interrupting service.

### **RTRV-BULKROLL-<OCN\_TYPE>**

This command retrieves roll data parameters.

## Single and Dual Rolls

CTC supports two roll types. In a single roll operation you select only one roll point. This allows you to move either the source or destination of a circuit to a new end-point on the same node (similar to a TL1 single roll), or on a different node (rolling the original circuit onto another circuit).

In a dual roll, you select two roll points. This allows you to reroute a segment between the two roll points of a circuit. The new route for a dual roll can be a new link (no circuit is required), or it can be another circuit (created before or during the bridge and roll process).

For dual roll constraints, consult the user documentation.

## Protected Circuits

CTC allows you to roll the working or protect path regardless of which path is active. You can upgrade an unprotected circuit to a fully protected circuit or downgrade a fully protected circuit to an unprotected circuit with the exception of a SNCP circuit. When using bridge and roll on SNCP circuits, you can roll the source or destination, or both path selectors in a dual roll, but not a single path selector.

## Enhanced Security Features

### Security Policy Enhancements

With Release 6.0.x the range of days over which you can enforce disabling of inactive users has increased. The previous range was 45 to 90 days. The new range is 1 to 99 days.

With Release 6.0.x enforced single concurrent user session applies to EMS, TL1, telnet, SSH, sftp, and ftp. This support applied only to EMS and TL1 in previous releases.

In Release 6.0.x you can set how many characters difference must exist between a user's old password and the next new password in a range of one to five characters.

### Secure Shell Encryption and Node Access Security

In previous releases the ONS platforms supported SSH version 2 (SSHv2) as an alternative to the ability to telnet into a node (shell access). In Release 6.0.x SSH encrypts all traffic (including passwords) to effectively eliminate unwanted monitoring of node activity. SSHv2 also supports access to the line card shell via shelf controller (that is, via relay), and access to line cards via IOS CLI (for cards in L2/L3 mode).

In Release 6.0.x all HTTP access to a node (for example, database backup, bulk PM retrieval, or software download) allows the use of HTTPS.

In previous releases any service type supported by ONS software could access ONS nodes. In Release 6.0.x node access can be controlled by service type. Each service type from which you can access a node in Release 6.0.x is configurable to support a choice of access states. The available states are non-secure (the default), secure (via SSHv2), and disabled (deny access from this service type). The SSHv2 secure state is supported for shell and ftp (using sftp), TL1, and EMS access types. Only nonsecure and disabled modes are supported for SNMP access.

### RADIUS Security

As of Release 6.0 users with Superuser security privileges can configure nodes to use Remote Authentication Dial In User Service (RADIUS) authentication. Cisco Systems uses a strategy known as authentication, authorization, and accounting (AAA) for verifying the identity of, granting access to, and tracking the actions of remote users.

#### RADIUS Authentication

RADIUS is a system of distributed security that secures remote access to networks and network services against unauthorized access. RADIUS comprises three components:

- A protocol with a frame format that makes use of User Datagram Protocol (UDP)/IP
- A server
- Clients

The server runs on a central computer, while clients reside in the dial-up access servers and can be distributed throughout the network.

An ONS node operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and returning all configuration information necessary for the client to deliver service to the user. RADIUS servers can act as proxy clients to other kinds of authentication servers. Transactions between the client and RADIUS

server are authenticated through the use of a shared secret, which is never sent over the network. User passwords are sent encrypted between the client and RADIUS server. This eliminates the possibility that someone illicitly monitoring an unsecured network might detect a user's password.

An ONS node acting as a RADIUS client can request authentication from up to ten hierarchically arranged RADIUS servers. RADIUS security provisioning features are located in the Provisioning > Security > RADIUS tabs. For further details and operation of RADIUS security features consult the user documentation.

### **RADIUS Session Time Limits**

Release 6.0.x RADIUS supports RADIUS session time limits. This feature applies only when a RADIUS server is used for authentication. When RADIUS indicates that a session is to have a time limit, that session is terminated immediately after the time expires. There is no local database support for session time limits. Rather, when EMS users are forcibly logged out by the RADIUS server, they are presented with a notification dialog box indicating that they have been forcibly logged out due to session time expiration. Similarly, when a TL1 user is logged out, an autonomous REPT\_EVT\_SESSION is sent. After a TL1 user is logged out, the next command the user enters receives a DENY response with a reason code of PLNA (Login Not Active).

### **AAA Server Enable/Disable**

In Release 6.0.x RADIUS a Superuser can turn AAA server authentication on or off. When AAA server authentication is turned off, the local security policy and settings are employed for user authentication. When AAA server authentication is enabled, it applies to all NE management services, overriding local settings where the two conflict.



#### **Note**

The following security policy features are not available when AAA server authentication is used:

- Idle user timeout (RADIUS user session timeouts are employed instead)
- Single session per user
- Forced password change at first login (global policy)
- Forced password change at next login (individual user)
- Password change prevention
- Excess failed login attempt lockout
- Password reuse prevention
- Inactive account disable
- Password expiration

AAA server authentication can be set in the node view > Provisioning > Defaults tabs. The default for AAA server authentication is OFF.

## **Audit Trail Enhancements**

The following features enhance your ability to monitor node and network activity through use of the audit trail in Release 6.0.x.

- Archival of the audit trail in TL1, with a supporting archival failure transient alarm, AUD-ARCHIVE-FAIL

- Audit trail initiation support for IOS-based data cards in the L2/L3 mode (available over the Syslog/IOS CLI)
- Tracking of all Release 6.0.x supported failed login types (incorrect password, disabled account, locked account, single login per user per node denial)
- Shell session login, logout, and activity trail
- Tracking of FTP/sftp logins and logouts
- Sustained audit trail for all logins and logouts whether or not an AAA server is used for user authentication
- Tracking of all user attempts to log in to the node
- When a login is denied, the audit trail records the reason (type of login failure)

## CTC Enhanced Security Support



### Note

---

All of the security options and settings described in this section are available to Superuser level users. For specific security levels for any given feature, consult the user documentation.

---

CTC provides several user-configurable security features in the following subtabs under the The CTC node view Security tab.

- Users
- Active Logins
- Policy
- Data Comm (displayed only for nodes equipped with TCC2P cards)
- Access
- RADIUS

The Active Logins, Policy, Access, and RADIUS tabs support new features for Release 6.0.x, as described below.

### Active Logins

The Active logins tab supports session management for Release 6.0.x. The Active Logins tab displays current login status information for the network. In previous releases the Active Logins tab displayed only which users were logged in, and the IP address from which each user was logged in. As of Release 6.0.x, in addition to user names and IP addresses, the Active Logins tab displays the specific node to which the user is logged in, the type of session used to log in, the date and time each user logged in, and the last date/time each user was active during the login. You can refresh the Last Activity Time by clicking the Retrieve Last Activity Time button. You also have the option to log out selected sessions. This feature logs out any selected sessions immediately, and interrupts any activities associated with those sessions. When you log out an active user session you have the option to lock the user out (from future sessions) prior to the logout.

In Release 6.0.x the following services are monitored in the Active Logins tab.

- TL1
- EMS
- FTP

- sftp
- telnet shell sessions (via serial port only; not the debug port)
- SSH shell sessions

## Policy

The Policy tab supports user security policy options. The Policy tab provides security policy settings and options. In previous releases the Policy tab provided the following functionality, in five display areas, in which settings could be applied:

- Idle User Timeout—Sets the hours and minutes a user can remain idly logged in before a timeout will occur; settings are provided for each user level.
- User Lockout—Sets the number of times a user can fail an attempt to log in before a lockout will occur, with an option to enforce manual unlocking of the user name by a Superuser, or alternatively, to set the lockout duration in minutes and seconds. Login failure types include:
  - Incorrect password
  - Disabled account
  - Locked account
  - Single login per user per node denial
- Password Change—Sets the number of unique passwords that must be used before a single password can be reused. Sets the option to disable changing of passwords for a fixed, user-configurable number of days. Sets the option to require a password change on first login to a new account.
- Password Aging—Enables you to optionally set a fixed number of days for each user security level (after which time a warning will be issued to create a new password), and to set a fixed number of days after which the password will actually expire and the user will no longer be able to log in.
- Other—Sets the option to enforce a single concurrent session per user (EMS and TL1 only). Also sets the option to enforce disabling of inactive users for users inactive a specified number of days; for example, if this feature is checked, with 90 days selected, a user ID that has not logged in for 90 days or more will be unable to log in again.

With Release 6.0.x, in the “Other” area, enforced single concurrent user session applies to EMS, TL1, telnet, SSH, HTTP, sftp, and ftp, and also, the range of days over which you can enforce disabling of inactive users has increased. The new range is 1 to 99 days.

Release 6.0.x also adds a new Password Change configuration that sets how many characters difference must exist between the old password and the new password in a range of one to five characters.

## Node Access

The Access tab supports node access options, including enhanced SSH secure connection support for Release 6.0.x. The Access tab provides settings and options for each type of access that can be used to reach the node. In previous releases, the Access tab included the following three areas for applying node access settings and options.

- LAN Access—Sets the option of None, Front only, Backplane only, or Front and Backplane. Also includes a “Restore Timeout” setting, configurable in minutes.
- Shell Access—Sets a choice between Telnet, with a configurable port number, and SSH, with a fixed port number.
- Other—Sets the PM clearing privilege as Provisioning or Superuser.

With Release 6.0.x the Access tab provides four new areas, plus functional changes to the Shell Access area, for a total of seven areas in which settings can be applied as follows.

- LAN Access—(Same as in previous releases.) Sets the option of None, Front only, Backplane only, or Front and Backplane. Also includes a “Restore Timeout” setting, configurable in minutes.
- Serial Craft Access—Sets the option to enable or disable the shelf controller serial craft port.
- Shell Access—Sets the Access security state for shell logins as Disable, Nonsecure, or Secure. Sets the configurable Telnet Port. Sets the option to Enable Shell Password.
- EMS Access—Sets the Access security state for EMS logins as Nonsecure or Secure. Sets the TCC Corba IIOP Listener Port.
- TL1 Access—Sets the Access security state for TL1 logins as Disable, Nonsecure, or Secure.
- SNMP Access—Sets the Access security state for SNMP logins as Disable or Nonsecure.
- Other—(Same as in previous releases.) Sets the PM clearing privilege as Provisioning or Superuser.

## RADIUS

The RADIUS tab is new for Release 6.0.x, and supports the new RADIUS security features, including RADIUS server management, authentication, accounting, and management of shared secrets. The RADIUS tab provides an area for setting the options to:

- Enable RADIUS Authentication
- Enable RADIUS Accounting
- Enable the given node as the final Authentication when no RADIUS server is reachable

The RADIUS tab also provides a display area for RADIUS servers, in order of authentication preference. This area displays the IP Address, Shared Secret, Authentication Port, and Accounting Port for each RADIUS server.

In the RADIUS tab you can create a RADIUS server by clicking the Create button. The RADIUS tab also provides the following additional actions, which can be performed upon selected server(s).

- Edit
- Delete
- Move up (in order of Authentication)
- Move down (in order of Authentication)

For information on using and configuring RADIUS features in Release 6.0.x consult the user documentation.

## IOS Security Enhancements

With Release 6.0.x the ML-Series card includes several security features. Some of these features can operate independent of the ONS node where the ML-Series card is installed. Others are configured using CTC or TL1.

Security features configured with Cisco IOS include:

- Cisco IOS login enhancements
- Secure Shell connection
- AAA/RADIUS stand alone mode
- Cisco IOS basic password

Security features configured with CTC or TL1 include:

- Disabled console port
- AAA/RADIUS relay mode

### Disabling the Console Port on the ML-Series Card

There are several ways to access the Cisco IOS running on the ML-Series card, including a direct connection to the console port, which is the RJ-11 serial port on the front of the card. As of Release 6.0, you can increase security by disabling this direct connection, which is enabled by default. This prevents console port input without preventing any console port output, such as Cisco IOS error messages.

You can disable console port access through CTC or TL1.

### Secure Login on the ML-Series Card

The ML-Series card supports the Cisco IOS login enhancements integrated into Cisco IOS Release 12.2(25)S and introduced in Cisco IOS Release 12.3(4)T. The enhancements allow users to better secure the ML-Series card when creating a virtual connection, such as Telnet, Secure Shell (SSH), or HTTP. The secure login feature records successful and failed login attempts for vty sessions on the ML-Series card. These features are configured using the Cisco IOS command-line interface (CLI).

### Secure Shell on the ML-Series Card

In previous releases the ML-Series card supported SSH version 1 (SSHv1) only. With Release 6.0.x the ML-Series card also supports SSH version 2 (SSHv2). SSHv2 offers security improvements over SSHv1 and is the default choice on the ML-Series card.

SSH has two applications, an SSH server and SSH client. The ML-Series card only supports the SSH server and does not support the SSH client. The SSH server in Cisco IOS software works with publicly and commercially available SSH clients.

The SSH server enables a connection into the ML-Series card, similar to an inbound Telnet connection, but with stronger security. Before SSH, security was limited to the native security in Telnet. SSH improves on this by allowing the use of Cisco IOS software authentication.

The ONS node also supports SSH. When SSH is enabled on the ONS node, the user must use SSH to connect to the ML-Series card for Cisco IOS CLI sessions. Telnet access to the ML-Series card is prevented when SSH is enabled on the ONS node except for connections through the console port of the ML-Series card. Disabling the console port on the ML-Series card will prevent this Telnet access.

### RADIUS on the ML-Series Card

RADIUS is a distributed client/server system that secures networks against unauthorized access. Clients send authentication requests to a central RADIUS server, which contains all user authentication and network service access information. The RADIUS host is normally a multiuser system running RADIUS server software from Cisco or another software provider.

Many Cisco products offer RADIUS support, including the ONS 15454, ONS 15454 SDH, ONS 15327, ONS 15310-CL, and ONS 15600. The ML-Series card also supports RADIUS.

The ML-Series card can operate either in RADIUS relay mode or in RADIUS stand alone mode (default). In either mode, the RADIUS messages from the ML-Series card are passed to a RADIUS server that is on the data communications network (DCN) used to manage the ONS node. For more information about RADIUS modes and operation on the ML-Series card consult the user documentation.

## IP and OSI on DCC

As of Release 6.0, IP and OSI can coexist on DCC on a Cisco ONS network, addressing legacy OSI via NSIF Mediation, and allowing migration into IP via G.7712. IP on DCC provides security through strong encryption, SSH, SSL, and HTTPS; centralized control and strong authentication (AAA); RADIUS; communication to Layer 2 and Layer 3 devices (IP + Optical); and pseudo wire, in support of the interworking function between IP and OSI. The ability to address IP/OSI issues gives you flexibility for the future, while working within existing DCN/DCC/OSS infrastructure.

Release 6.0.x uses PPP, a Layer 2 encapsulation protocol, with high-level data link control (HDLC) datagram encapsulation to transport IP and OSI data, and link control protocol (LCP) to establish, configure, and test the point-to-point connections. CTC automatically enables IP over PPP whenever you create an SDCC or LDCC. The SDCC or LDCC can also be provisioned to support OSI over PPP. Link access protocol on the D channel (LAP-D), a data link protocol used in the OSI protocol stack, provides provisionable parameters when you elect to provision an ONS SDCC as OSI only.

Release 6.0.x TCP/IP and OSI networking employs the following additional features, described in detail in the user documentation.

### OSI Connectionless Network Service

OSI connectionless network service is implemented by using the Connectionless Network Protocol (CLNP) and Connectionless Network Service (CLNS). CLNP and CLNS are described in the ISO 8473 standard.

### OSI Routing

OSI routing uses a set of routing protocols that allow end system and intermediate system information collection and distribution; a routing information base; and a routing algorithm (shortest path first).

### TARP

TID Address Resolution Protocol (TARP) is used when TL1 target identifiers (TIDs) must be translated to network service access point (NSAP) addresses.

### TCP/IP and OSI Mediation

Two mediation processes, T-TD and FT-TD, facilitate TL1 networking and file transfers between NEs and ONS client computers running TCP/IP and OSI protocol suites.

### OSI Virtual Routers

Release 6.0.x supports three OSI virtual routers, provisionable on the Provisioning > OSI > Routers tab.

### IP-over-CLNS Tunnels

IP-over-CLNS tunnels are used to encapsulate IP for transport across OSI NEs. Release 6.0.x supports two tunnel types, Generic Routing Encapsulation (GRE) and Cisco IP.

### OSI Provisioning in CTC

The following OSI features are provisionable in the CTC node view, Provisioning tab. For full explanations of CTC provisioning for OSI, consult the user documentation.

- OSI setup

- TARP configuration, static TDC, and MAT
- Router setup and subnets
- Tunnels
- Communication channels

## 64-Bit RMON Monitoring Over DCC

The ONS 15454 SDH DCC is implemented over the IP protocol, which is not compatible with Ethernet. The system builds Ethernet equipment History and Statistics tables using HDLC statistics that are gathered over the DCC (running point-to-point protocol, or PPP). Release 6.0.x adds RMON DCC monitoring (for both IP and Ethernet) to monitor the health of remote DCC connections.

In Release 6.0.x RMON monitoring over DCC is accomplished by the following two MIBs for DCC interfaces.

- `cMediaIndependentTable`—Standard, rfc3273; the proprietary extension of the HC-RMON MIB used for reporting statistics
- `cMediaIndependentHistoryTable`—The proprietary MIB used to support history

Monitoring using the two MIBs is accomplished by the creation of rows of data. For more information on creating rows using the two MIBs, consult the user documentation.

## New Secondary State: failed

Release 6.0.x introduces a new secondary service state (SST), failed. The failed secondary state is defined as follows:

- `failed`—The entity has a raised alarm or condition.

The failed SST is an extension to the existing ONS State Model. It identifies that the affected entity is disabled because it is faulty. The failed secondary state affects the service state only. The administrative state (the state you manage the entity into) is not affected. The failed SST is the result of autonomous action; you cannot manage an entity into the failed SST. The failed SST is for retrieval purposes only. An entity's service state will transition into an autonomously disabled service state if alarms or conditions are present. The failed SST is appended to the existing secondary state for the entity when an alarm or condition exists.

Some equipment alarms will not generate a failed SST transition. If a state already exists to represent the equipment condition, failed will not be added to the secondary state list. For further information about the failed SST consult the user documentation.

## Manage Pluggable Port Modules

Release 6.0.x adds pluggable-port module (PPM) management for the 15454\_MRC-12 and OC192-XFP cards. For the 15454\_MRC-12 card you can provision or delete a PPM, and you can provision or change optical line rates. OC-192XFPs are single-rate PPMs, and therefore can only be deleted.

## Change Pluggable Port Module Service States

On the OC192-XFP and 15454\_MRC-12 cards, the PPM port is equivalent to an optical port. To change a PPM port's service state you can follow the same procedure as in changing any port's service state (refer to the user documentation for this procedure).

## Cisco Service Assurance Agent ML-Series Support

The Cisco Service Assurance Agent (SAA) is an application-aware synthetic operation agent that monitors network performance, especially IP SLAs. Performance can be measured between any Cisco device that supports this feature and any remote IP host (server), Cisco routing device, or mainframe host. Performance measurement statistics provided by this feature can be used for troubleshooting, for problem analysis, and for designing network topologies.

The Cisco SAA can be especially useful for enterprise and service provider networks, because it provides expanded measurement and management capabilities. In particular, the Cisco SAA is a reliable mechanism for accurately monitoring the metrics in SLAs.

Because Cisco SAA is accessible using SNMP, it also can be used in performance monitoring applications for network management systems (NMSs) such as CiscoWorks2000 (CiscoWorks Blue) and the Internetwork Performance Monitor (IPM). SAA notifications also can be enabled through Systems Network Architecture (SNA) network management vector transport (NMVT) for applications such as NetView.

For information on configuring the Cisco SAA to provide advanced network service monitoring information, see the “Network Monitoring Using Cisco Service Assurance Agent” chapter of the Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2.

### Cisco Service Assurance Agent on the ML-Series

As of Release 6.0, the ML-Series card has a complete IP SLA Cisco IOS subsystem and offers all the normal features and functions available in Cisco IOS Release 12.2S. It uses the standard IP SLA Cisco IOS CLI commands. SNMP support is equivalent to the support provided in the IP SLA subsystem 12.2(S), which is the rttMon MIB.

The following restrictions apply for ML-Series card operation with Cisco SAA.

The ML-Series card supports only features in the Cisco IOS 12.2S branch. It does not support functions available in future Cisco IOS versions, such as the IP SLA accuracy feature or the enhanced Cisco IOS CLI support with updated IP SLA nomenclature.

Setting the CoS bits is supported, but set CoS bits are not honored when leaving or entering the CPU when the sender or responder is an ONS 15454, ONS 15454 SDH or ONS 15310-CL platform. Set CoS bits are honored in intermediate ONS nodes.

On RPR, the direction of the data flow for the IP SLA packet might differ from the direction of customer traffic.

The system clock on the ML-Series card synchronizes with the clock on the TCC2/TCC2P card. Any NTP server synchronization is done with the TCC2/TCC2P card's clock and not with the ML-Series card's clock.

## CTC Launcher

Release 6.0.x introduces the CTC Launcher utility, CtcLauncher.jar. The CTC Launcher utility can be used to launch CTC and manage an ONS node running Release 6.0.x or higher.

CTC Launcher provides two connection options. First, it can be used to access ONS NEs that have IP connectivity to the CTC computer. Second, CTC Launcher can establish connectivity to ONS NEs that reside behind a third party, OSI-based GNE. To create a connection through the OSI-based GNE, CTC Launcher creates a TL1 tunnel. This tunnel is similar to the static IP-over-CLNS tunnels that are available in CTC Release 6.0.x. (For information about IP-over-CLNS tunnels, refer to the Release 6.0

ONS product documentation.) However, unlike the static IP-over-CLNS tunnels, the TL1 tunnel does not require provisioning on the third party GNE, the DCN routers, or the ONS NEs. The tunnel connection is created using the CTC Launcher. It can then be managed using CTC.

**Note**

To establish a TL1 tunnel, the ONS node behind the GNE must be running Release 6.0.x or higher.

Prior to using the CTC Launcher utility, the CTC jar files must be precached, either from the installation CD, using the LDCACHE utility, or from the node, by launching CTC from a web browser. For installation instructions for the CTC Launcher utility, consult the readme file. The CtcLauncher.jar utility and the CtcLauncher-README.txt file are located in the CtcLauncher directory on the R6.0.x software CD. For additional information about CTC Launcher, refer to the CTC Launcher Application Guide. To access the application guide:

- 
- Step 1** Go to <http://www.cisco.com>.
  - Step 2** Choose Technical Support & Documentation.
  - Step 3** Choose Optical Networking.
  - Step 4** Choose the ONS 15300, ONS 15400, or ONS 15600 product category.
  - Step 5** Choose the Configuration Guides category.
  - Step 6** Click the CTC Launcher Application Guide link under the appropriate product.
- 

## TL1

### TL1 Open GNE

TL1 supports the ability to act as a GNE or ENE to an OEM IP DCN (foreign) connected node that also uses TL1. To accomplish TL1 GNE-ENE interoperability, the DCN communication path between the GNE and ENE employs PPP and OSPF in a non-proprietary manner, while ensuring that these connections remain secure. Open GNE TL1 functionality enables you to configure DCC terminations to interoperate with a system on the far end that does not support proprietary PPP vendor extensions or OSPF types.

#### Open GNE Commands

The following commands support TL1 open GNE. For input and output formats and parameters, plus examples of how to use each command, consult the user documentation.

##### **RTRV-TADRMAP**

- RETRIEVE-TID\_ADDRESS\_MAP

This command is used to instruct a Gateway NE to return the entries of the TADRMAP. One row is used for each displayed TID name.

##### **DLT-TADRMAP**

- DELETE-TID\_ADDRESS\_MAP

This command is used to instruct a Gateway NE to delete an entry in the table which maps the TIDs of the subtending NEs to their addresses. The OSs will address the subtending NEs using the TID in TL1 messages and a Gateway NE will address these NEs using IP Addresses or NSAPs. This table, which resides in a Gateway NE, correlates a TID and an address.

#### **ENT-TADRMAP**

- ENTER-TID\_ADDRESS\_MAP

This command is used to instruct a Gateway NE to create an entry in the table which maps the TIDs of the subtending NEs to their addresses. The OSs will address the subtending NEs using the TID in TL1 messages and a Gateway NE will address these NEs using IP Addresses or NSAPs. This table, which resides in a Gateway NE, correlates a TID and an address. This command requires that at least one of (IPADDR or NSAP) be specified.

#### **ENT-TUNNEL-PROXY**

- ENTER-TUNNEL\_PROXY

This command is used to create a proxy tunnel.

#### **DLT-TUNNEL-PROXY**

- DELETE-TUNNEL\_PROXY

This command is used to delete a proxy tunnel.

#### **RTRV-TUNNEL-PROXY**

- RETRIEVE-TUNNEL\_PROXY

This command is used to view the proxy tunnels contained in the NE proxy table.

#### **ENT-TUNNEL-FIREWALL**

- ENTER-TUNNEL\_FIREWALL

This command is used to create a firewall tunnel.

#### **DLT-TUNNEL-FIREWALL**

- DELETE-TUNNEL\_FIREWALL

This command is used to delete a firewall tunnel.

#### **RTRV-TUNNEL-FIREWALL**

- RETRIEVE-TUNNEL\_FIREWALL

This command is used to view the firewall tunnels contained in the NE proxy table.

### **Changed Commands for Open GNE**

The following previously-existing TL1 commands support new parameters for open GNE.

#### **ED-<OCN\_TYPE>**

- foreignFarEnd—Input parameter used to indicate that the far end NE on the DCC is a foreign NE.
- foreignIPAddress—Input parameter specifying the IP Address of the far end Node on the DCC. Used only if foreignFarEnd is 'Y'.

**RTRV-<OCN\_TYPE>**

- foreignFarEnd—Output parameter used to indicate that the far end NE on the DCC is a foreign NE.
- foreignIPAddress—Output parameter specifying the IP Address of the far end Node on the DCC. Used only if foreignFarEnd is ‘Y’.

The following command has been modified to support open GNE as described.

**REPT^DBCHG**

Generate an update after an addition to or deletion from the TADRMAP or an addition or deletion of a firewall or proxy tunnel. The ENT-TADRMAP, DLT-TADRMAP, ENT-TUNNEL-PROXY, DLT-TUNNEL-PROXY, ENT-TUNNEL-FIREWALL, and DLT-TUNNEL-FIREWALL commands each generate an appropriate REPT^DBCHG message.

## New Card Support

The following new cards are supported by TL1 in Release 6.0.x.

- STM64-XFP
- MRC-12
- XCVXC
- Filler card
- ML100X-8
- OPT-BST-E

## TL1 Command Changes

### New Commands

The following new TL1 commands are added for Release 6.0.x.

- CHG-EQPT
- ALW-CONSOLE-PORT
- DLT-BULKROLL
- DLT-ROLL
- DLT-ROUTE-GRE
- DLT-TADRMAP
- DLT-TUNNEL-FIREWALL
- DLT-TUNNEL-PROXY
- ED-BULKROLL
- ED-PROTOCOL
- ED-ROLL
- ENT-BULKROLL
- ENT-ROUTE-GRE
- ENT-TADRMAP
- ENT-TUNNEL-FIREWALL

- ENT-TUNNEL-PROXY
- INH-CONSOLE-PORT
- RTRV-AUDIT-LOG
- RTRV-BULKROLL
- RTRV-TUNNEL-FIREWALL
- RTRV-TUNNEL-PROXY
- RTRV-FFP
- RTRV-ROLL
- RTRV-ROUTE-GRE
- RTRV-TADRMAP

## Command Syntax Changes

The syntax of the following commands is changed in Release 6.0.x.



### Note

These changes apply to all ONS platforms.

#### **COPY-IOSCFG** syntax:

```
COPY-IOSCFG[:<TID>]:<aid>:<CTAG>::SRC=<src>,DEST=<dest>;
```

Is changed to:

```
COPY-IOSCFG[:<TID>]:<aid>:<CTAG>::SRC=<src>,DEST=<dest>[,FTTD=<fttd>];
```

#### **COPY-RFILE** syntax:

```
COPY-RFILE[:<TID>]:<src>:<CTAG>::TYPE=<xfertype>,[SRC=<srcurl>],[DEST=<desturl>],[OVRT=<ovwrt>],[FTTD=<fttd>];
```

Is changed to:

```
COPY-RFILE[:<TID>][:<src>]:<CTAG>::TYPE=<xfertype>,[SRC=<srcurl>],[DEST=<desturl>],[OVRT=<ovwrt>],[FTTD=<fttd>];
```

#### **DLT-ROUTE** syntax:

```
DLT-ROUTE[:<TID>]:<CTAG>::<DESTIP>,<IPMASK>;
```

Is changed to:

```
DLT-ROUTE[:<TID>]:<CTAG>::<DESTIP>;
```

#### **ED-10GIGE** syntax:

```
ED-10GIGE[:<TID>]:<aid>:<CTAG>[::NAME=<portname>],[MACADDR=<macaddr>],[MFS=<mfs>],[CMDMDE=<cmdmde>][:<pst>[,<sst>]];
```

Is changed to:

```
ED-10GIGE[:<TID>]:<aid>:<CTAG>[::NAME=<portname>],[MACADDR=<macaddr>],[MFS=<mfs>],[CMDMDE=<cmdmde>],[FREQ=<freq>],[LOSSB=<lossb>][:<pst>[,<sst>]];
```

#### **ED-BITS** syntax:

```
ED-BITS[:<TID>]:<aid>:<CTAG>[::LINECDE=<linecde>],[FMT=<fmt>],[SABIT=<sabit>],[IMPEDANCE=<impedance>],[LBO=<lbo>],[SYNCSMSG=<synmsg>],[AISTHRSHLD=<aistrshld>],[BITSFAC=<bitsfac>],[ADMSSM=<admssm>][:<pst>];
```

Is changed to:

```
ED-BITS[:<TID>]:<aid>:<CTAG>[::LINECDE=<linecde>],[FMT=<fmt>],[SABIT=<sabit>],
[[LBO=<lbo>],[SYNCSMSG=<syncmsg>],[AISTHRSHLD=<aisthrshld>],[BITSFAC=<bitsfac>],
[[ADMSSM=<admssm>][:<pst>];
```

**ED-CRS-STP-PATH** syntax:

```
ED-CRS-STP-PATH:<src>,<dst>:<CTAG>[::ADD=<add>],[REMOVE=<remove>],[CKTID
=<ctid>],[CMDMDE=<cmdmde>][:<pst>[,<sst>]]
```

Is changed to:

```
ED-CRS-STP-PATH:<src>,<dst>:<CTAG>[::<cct>][:ADD=<add>],[REMOVE=<remove>],[
CKTID=<ctid>],[CMDMDE=<cmdmde>][:<pst>[,<sst>]]
```

**ED-E1** syntax:

```
ED-E1[:<TID>]:<aid>:<CTAG>[::LINECDE=<linecde>],[FMT=<fmt>],[TACC=<tacc>],[T
APTYPE=<tatype>],[SFBER=<sfber>],[SDBER=<sdber>],[SOAK=<soak>],[NAME=<nam
e>],[CMDMDE=<cmdmde>][:<pst>[,<sst>]];
```

Is changed to:

```
ED-E1[:<TID>]:<aid>:<CTAG>[::LINECDE=<linecde>],[FMT=<fmt>],[TACC=<tacc>],[T
APTYPE=<tatype>],[SFBER=<sfber>],[SDBER=<sdber>],[SOAK=<soak>],[NAME=<nam
e>],[CMDMDE=<cmdmde>],[SYNCSMSG=<syncmsg>],[SENDUS=<sendus>],[ADMSSM
=<admssm>],[SABIT=<sabit>][:<pst>[,<sst>]];
```

**ED-EC1** syntax:

```
ED-EC1[:<TID>]:<aid>:<CTAG>[::PJMON=<pjmon>],[LBO=<lbo>],[SOAK=<soak>],[SF
BER=<sfber>],[SDBER=<sdber>],[NAME=<name>],[CMDMDE=<cmdmde>][:<pst>[,<sst>
]];
```

Is changed to:

```
ED-EC1[:<TID>]:<aid>:<CTAG>[::PJMON=<pjmon>],[LBO=<lbo>],[SOAK=<soak>],[SF
BER=<sfber>],[SDBER=<sdber>],[NAME=<name>],[AISONLPBK=<aisonlpbk>],[CMDM
DE=<cmdmde>],[EXPTRC=<exptrc>],[TRC=<trc>],[TRCMODE=<trcmode>],[TRCFORM
AT=<trcformat>][:<pst>[,<sst>]];
```

**ED-FFP-MOD2** syntax:

```
ED-FFP-MOD2:<aid>:<CTAG>[::PROTID=<protid>],[RVRTV=<rvrtv>],[RVTM=<rvtm>],[
PSDIRN=<psdirn>][:]
```

Is changed to:

```
ED-FFP-MOD2:<aid>:<CTAG>[::PROTID=<protid>],[RVRTV=<rvrtv>],
```

**ED-G1000** syntax:

```
ED-G1000[:<TID>]:<aid>:<CTAG>[::MFS=<mfs>],[FLOW=<flow>],[LOWMRK=<int>],[
HIWMRK=<int>],[NAME=<name>],[CMDMDE=<cmdmde>],[SOAK=<soak>][:<pst>[,<sst>
]];
```

Is changed to:

```
ED-G1000[:<TID>]:<aid>:<CTAG>[::MFS=<mfs>],[FLOW=<flow>],[LOWMRK=<int>],[
HIWMRK=<int>],[AUTONEG=<autoneg>],[NAME=<name>],[CMDMDE=<cmdmde>],[SO
AK=<soak>][:<pst>[,<sst>]];
```

**ED-GIGE** syntax:

```
ED-GIGE[:<TID>]:<aid>:<CTAG>[:::ADMINSTATE=<adminstate>],[LINKSTATE=<linkstate>],[MTU=<mtu>],[FLOWCTRL=<flowctrl>],[OPTICS=<optics>],[DUPLEX=<duplex>],[SPEED=<speed>],[NAME=<name>],[CMDMDE=<cmdmde>][:<pst>[,<sst>]];
```

Is changed to:

```
ED-GIGE[:<TID>]:<aid>:<CTAG>[:::ADMINSTATE=<adminstate>],[LINKSTATE=<linkstate>],[FLOWCTRL=<flowctrl>],[OPTICS=<optics>],[DUPLEX=<duplex>],[SPEED=<speed>],[NAME=<name>],[CMDMDE=<cmdmde>],[FREQ=<freq>],[LOSSB=<lossb>][:<pst>[,<sst>]];
```

**ED-NE-GEN** syntax:

```
ED-NE-GEN[:<TID>]:<CTAG>[:::NAME=<name>],[IPADDR=<ipaddr>],[IPMASK=<ipmask>],[DEFRTR=<defrtr>],[IIOPORT=<iioport>],[NTP=<ntp>];
```

Is changed to:

```
ED-NE-GEN[:<TID>]:<CTAG>[:::NAME=<name>],[IPADDR=<ipaddr>],[IPMASK=<ipmask>],[DEFRTR=<defrtr>],[IIOPORT=<iioport>],[NTP=<ntp>],[SUPPRESSIP=<mode>];
```

**ED-POS** syntax:

```
ED-POS[:<TID>]:<src>:<CTAG>[:::ENCAP=<encap>],[NAME=<name>],[CMDMDE=<cmdmde>],[SOAK=<soak>][:<pst>[,<sst>]];
```

Is changed to:

```
ED-POS[:<TID>]:<aid>:<CTAG>;
```

**ED-T1** syntax:

```
ED-T1[:<TID>]:<aid>:<CTAG>[:::LINECDE=<linecde>],[FMT=<fmt>],[LBO=<lbo>],[TACC=<tacc>],[TAPTYPE=<tatype>],[SOAK=<soak>],[SFBER=<sfber>],[SDBER=<sdber>],[NAME=<name>],[CMDMDE=<cmdmde>][:<pst>[,<sst>]];
```

Is changed to:

```
ED-T1[:<TID>]:<aid>:<CTAG>[:::LINECDE=<linecde>],[FMT=<fmt>],[LBO=<lbo>],[TACC=<tacc>],[TAPTYPE=<tatype>],[SOAK=<soak>],[SFBER=<sfber>],[SDBER=<sdber>],[SYNMSG=<synmsg>],[SENDDUS=<senddus>],[NAME=<name>],[CMDMDE=<cmdmde>],[AISONLPBK=<aisonlpbk>],[MODE=<mode>],[SYNMAP=<syncmap>],[ADMSSM=<admssm>],[VTMAP=<vtmap>],[AISONAIS=<aisvonais>],[AISONLOF=<aisionlof>],[INHFELPBK=<inhfelpbk>][:<pst>[,<sst>]];
```

**ED-T3** syntax:

```
ED-T3[:<TID>]:<aid>:<CTAG>[:::FMT=<fmt>],[LINECDE=<linecde>],[LBO=<lbo>],[INHFELPBK=<inhfelpbk>],[TACC=<tacc>],[TAPTYPE=<tatype>],[SOAK=<soak>],[SFBER=<sfber>],[SDBER=<sdber>],[NAME=<name>],[CMDMDE=<cmdmde>][:<pst>[,<sst>]];
```

Is changed to:

```
ED-T3[:<TID>]:<aid>:<CTAG>[:::FMT=<fmt>],[LINECDE=<linecde>],[LBO=<lbo>],[INHFELPBK=<inhfelpbk>],[TACC=<tacc>],[TAPTYPE=<tatype>],[SOAK=<soak>],[SFBER=<sfber>],[SDBER=<sdber>],[NAME=<name>],[AISONLPBK=<aisonlpbk>],[CMDMDE=<cmdmde>][:<pst>[,<sst>]];
```

**ED-VC3** syntax:

```
ED-VC3[:<TID>]:<src>:<CTAG>[:::RVRTV=<rvrtv>],[RVTM=<rvtm>],[HOLDOFFTIMER=<holdofftimer>],[TACC=<tacc>],[TAPTYPE=<tatype>],[CMDMDE=<cmdmde>],[EXPTRC=<exptrc>],[TRC=<trc>],[TRCMODE=<trcmode>][:<pst>[,<sst>]];
```

Is changed to:

```
ED-VC3[:<TID>]:<src>:<CTAG>[::RVRTV=<rvrtv>],[RVTM=<rvtm>],[HOLDOFFTIMER=<holdofftimer>],[TACC=<tacc>],[TAPTYPE=<tatype>],[CMDMDE=<cmdmde>],[EXPTRC=<exptrc>],[TRC=<trc>],[TRCMODE=<trcmode>],[TRCFORMAT=<trcformat>][:<pst>[,<sst>]]];
```

**ED-VT1** syntax:

```
ED-VT1[:<TID>]:<aid>:<CTAG>[::RVRTV=<rvrtv>],[RVTM=<rvtm>],[HOLDOFFTIMER=<holdofftimer>],[TACC=<tacc>],[TAPTYPE=<tatype>],[CMDMDE=<cmdmde>],[EXPTRC=<exptrc>],[TRC=<trc>],[TRCMODE=<trcmode>][:<pst>[,<sst>]]];
```

Is changed to:

```
ED-VT1[:<TID>]:<aid>:<CTAG>[::SFBER=<sfber>],[SDBER=<sdber>],[RVRTV=<rvrtv>],[RVTM=<rvtm>],[HOLDOFFTIMER=<holdofftimer>],[TACC=<tacc>],[TAPTYPE=<tatype>],[CMDMDE=<cmdmde>],[EXPTRC=<exptrc>],[TRC=<trc>],[TRCMODE=<trcmode>],[TRCFORMAT=<trcformat>][:<pst>[,<sst>]]];
```

**ED-VT2** syntax:

```
ED-VT2[:<TID>]:<src>:<CTAG>[::RVRTV=<rvrtv>],[RVTM=<rvtm>],[HOLDOFFTIMER=<holdofftimer>],[TACC=<tacc>],[TAPTYPE=<tatype>],[CMDMDE=<cmdmde>],[EXPTRC=<exptrc>],[TRC=<trc>],[TRCMODE=<trcmode>][:<pst>[,<sst>]]];
```

Is changed to:

```
ED-VT2[:<TID>]:<src>:<CTAG>[::SFBER=<sfber>],[SDBER=<sdber>],[RVRTV=<rvrtv>],[RVTM=<rvtm>],[HOLDOFFTIMER=<holdofftimer>],[TACC=<tacc>],[TAPTYPE=<tatype>],[CMDMDE=<cmdmde>],[EXPTRC=<exptrc>],[TRC=<trc>],[TRCMODE=<trcmode>],[TRCFORMAT=<trcformat>][:<pst>[,<sst>]]];
```

**ENT-EQPT** syntax:

```
ENT-EQPT[:<TID>]:<aid>:<CTAG>::<aidtype>[:PROTID=<protid>],[PRTYPE=<prtype>],[RVRTV=<rvrtv>],[RVTM=<rvtm>],[CARDMODE=<cardmode>],[PEERID=<protid>],[REGENNAME=<regenname>],[PWL=<pwl>],[CMDMDE=<cmdmde>][:];
```

Is changed to:

```
ENT-EQPT[:<TID>]:<aid>:<CTAG>::<aidtype>[:PROTID=<protid>],[PRTYPE=<prtype>],[RVRTV=<rvrtv>],[RVTM=<rvtm>],[CARDMODE=<cardmode>],[PEERID=<protid>],[REGENNAME=<regenname>],[PWL=<pwl>],[CMDMDE=<cmdmde>],[RETIME=<retime>][:];
```

**ENT-ROLL** syntax:

```
ENT-ROLL-<MOD_PATH>[:<TID>]:<src>,<dst>:<CTAG>::RFROM=<rfrom>,RTO=<rto>,RMODE=<rmode>,[FORCE=<force>];
```

Is changed to:

```
ENT-ROLL-<MOD_PATH>[:<TID>]:<from>,<to>:<CTAG>::RFROM=<rfrom>,RTO=<rto>,RMODE=<rmode>,[CMDMDE=<cmdmde>];
```

**SET-ATTR-SECUDFLT** syntax:

```
SET-ATTR-SECUDFLT[:<TID>]:<CTAG>[:PAGE=<page>],[PCND=<pcnd>],[MXINV=<mxinv>],[DURAL=<dural>],[TMOUT=<tmout>],[UOUT=<uout>],[PFRCD=<pfrcd>],[POL D=<pold>],[PINT=<pint>],[LOGIN=<login>],[PRIVLVL=<uap>];
```

Is changed to:

```
SET-ATTR-SECUDFLT[:<TID>]:<CTAG>[:PAGE=<page>],[PCND=<pcnd>],[MXINV=<mxinv>],[DURAL=<dural>],[TMOUT=<tmout>],[UOUT=<uout>],[PFRCD=<pfrcd>],[POL D=<pold>],[PINT=<pint>],[LOGIN=<login>],[PRIVLVL=<uap>],[PDIF=<pdif>];
```

Miscellaneous syntax changes:

Syntax:

```
[:<TID>]:<aid>:<CTAG>;
```

Is changed to:

```
[:<TID>>::<CTAG>;
```

Response:

```
<aid>:<sc>,<switchtype>
```

Is changed to:

```
[<vendor>],<netype>
```

## Command Response Changes

The following TL1 responses have changed in Release 6.0.x.



**Note**

---

These changes apply to all ONS platforms.

---

**RTRV-10GIGE** response:

```
<aid>:,<role>,<status>:[<portname>],[<macaddr>],[<lbc1>],[<opt>],[<opr>],[<mfs>]:<ps
t>,<sst>
```

Is changed to:

```
<aid>:,<role>,<status>:[<portname>],[<macaddr>],[<lbc1>],[<opt>],[<opr>],[<mfs>],[<fr
eq>],[<lossb>]:<pst>,<sst>
```

**RTRV-DS3I** response:

```
<aid>::<fmt>,<linecde>,<lbo>,<tacc>,<tatype>,<sfber>,<sdber>,<soak>,<name>]:
<pst>,<sst>
```

Is changed to:

```
<aid>::<fmt>,<linecde>,<lbo>,<tacc>,<tatype>,<sfber>,<sdber>,<soak>,<soakleft
>,<name>,<inhfelpbk>]:<pst>,<sst>
```

**RTRV-E1** response:

```
<aid>::<linecde>,<fmt>,<tacc>,<tatype>,<sfber>,<sdber>,<soak>,<name>]:<pst>
,<sst>
```

Is changed to:

```
<aid>::<linecde>,<fmt>,<tacc>,<tatype>,<sfber>,<sdber>,<soak>,<soakleft>,<na
me>,<syncmsg>,<senddus>,<retime>,<admssm>,<providesync>,<aisionlpbk>,<sa
Bit>]:<pst>,<sst>
```

**RTRV-E3** response:

```
<aid>::<tacc>,<tatype>,<sfber>,<sdber>,<soak>,<name>]:<pst>,<sst>
```

Is changed to:

```
<aid>::<tacc>,<tatype>,<sfber>,<sdber>,<soak>,<soakleft>,<name>]:<pst>,<sst>
```

**RTRV-E4** response:

<aid>::[<payload>],[<sfber>],[<sdber>],[<soak>],[<name>]:<pst>,<sst>

Is changed to:

<aid>::[<payload>],[<sfber>],[<sdber>],[<soak>],[<soakleft>],[<name>]:<pst>,<sst>

**RTRV-EC1** response:

<aid>::[<pjmon>],[<lbo>],[<rxequal>],[<soak>],[<soakleft>],[<sfber>],[<sdber>],[<name>],[<aisonlpbk>]:<pst>,<sst>

Is changed to:

<aid>::[<pjmon>],[<lbo>],[<rxequal>],[<soak>],[<soakleft>],[<sfber>],[<sdber>],[<name>],[<aisonlpbk>],[<exptrc>],[<trc>],[<inctrc>],[<trcmode>],[<trcformat>]:<pst>,<sst>

**RTRV-EQPT** response:

<aid>:<aidtype>,<equip>,[<role>],[<status>]:[<protid>],[<prtype>],[<rvrtv>],[<rvtm>],[<cardname>],[<ioscfg>],[<cardmode>],[<peerid>],[<regenname>],[<pwl>]:<pst>,<sst>

Is changed to:

<aid>:<aidtype>,<equip>,[<role>],[<status>]:[<protid>],[<prtype>],[<rvrtv>],[<rvtm>],[<cardname>],[<ioscfg>],[<cardmode>],[<peerid>],[<regenname>],[<pwl>],[<transmode>],[<retime>]:<pst>,<sst>

**RTRV-FSTE** response:

<aid>::[<adminstate>],[<linkstate>],[<mtu>],[<flowctrl>],[<duplex>],[<speed>],[<flow>],[<expduplex>],[<expspeed>],[<vlancosthreshold>],[<iptosthreshold>],[<name>],[<soak>],[<soakleft>]:<pst>,<sst>

Is changed to:

<aid>::[<adminstate>],[<linkstate>],[<mtu>],[<flowctrl>],[<optics>],[<duplex>],[<speed>],[<flow>],[<expduplex>],[<expspeed>],[<vlancosthreshold>],[<iptosthreshold>],[<name>],[<soak>],[<soakleft>]:<pst>,<sst>

**RTRV-GIGE** response:

<aid>::[<adminstate>],[<linkstate>],[<mtu>],[<flowctrl>],[<optics>],[<duplex>],[<speed>],[<name>]:<pst>,<sst>

Is changed to:

<aid>:,[<role>],[<status>]:[<adminstate>],[<linkstate>],[<mtu>],[<flowctrl>],[<optics>],[<duplex>],[<speed>],[<name>],[<freq>],[<lossb>]:<pst>,<sst>

**RTRV-INV** response:

<aid>,<aidtype>::[<plugtype>],[<pn>],[<hwrev>],[<fwrev>],[<sn>],[<clei>],[<twl1=nwl in code>],[<twl2= w11 in code>],[<twl3=w12 in code>],[<twl4=w13 in code>],[<pluginvendorid>],[<pluginpn>],[<pluginhwrev>],[<pluginfwrev>],[<pluginsn>],[<ilossref>],[<productId>],[<versionId>],[<fpgaVersion>]

Is changed to:

<aid>,<aidtype>::[<pn>],[<hwrev>],[<fwrev>],[<sn>],[<clei>],[<twl1=nwl in code>],[<pluginvendorid>],[<pluginpn>],[<pluginhwrev>],[<pluginfwrev>],[<pluginsn>],[<ilossref>],[<productId>],[<versionId>],[<fpgaVersion>]

**RTRV-STM1E** response:

<aid>::[<payload>],[<syncmsg>],[<senddus>],[<sfber>],[<sdber>],[<soak>],[<name>]:<pst>,<sst>

Is changed to:

<aid>::[<payload>],[<syncmsg>],[<senddus>],[<sfber>],[<sdber>],[<soak>],[<soakleft>],[<name>]:<pst>,[<sst>]

**RTRV-T1** response:

<aid>::[<linecde>],[<fmt>],[<lbo>],[<tacc>],[<tatype>],[<soak>],[<soakleft>],[<sfber>],[<sdber>],[<name>],[<syncmsg>],[<senddus>],[<retime>],[<aisonlypbk>]:<pst>,[<sst>]

Is changed to:

<aid>::[<linecde>],[<fmt>],[<lbo>],[<tacc>],[<tatype>],[<soak>],[<soakleft>],[<sfber>],[<sdber>],[<name>],[<syncmsg>],[<senddus>],[<retime>],[<aisonlypbk>],[<aisvonais>],[<aisonlyof>],[<mode>],[<syncmap>],[<admssm>],[<providesync>],[<vtmap>],[<inhfelpbk>]:<pst>,[<sst>]

**RTRV-VT2** response:

<aid>::[<sfber>],[<sdber>],[<rvrtv>],[<rvtm>],[<holdofftimer>],[<exptrc>],[<trc>],[<inctrc>],[<trcmode>],[<tacc>],[<tatype>],[<upsrpthstate>]:<pst>,[<sst>]

Is changed to:

<aid>::[<sfber>],[<sdber>],[<rvrtv>],[<rvtm>],[<holdofftimer>],[<exptrc>],[<trc>],[<inctrc>],[<trcmode>],[<trcformat>],[<tacc>],[<tatype>],[<upsrpthstate>]:<pst>,[<sst>]

**SET-TOD** response:

<year>,<month>,<day>,<hour>,<minute>,<second>,<tmtime>

Is changed to:

<year>,<month>,<day>,<hour>,<minute>,<second>,<difference>:<tmtime>

## TL1 ENUM Changes



**Note**

These changes apply to all ONS platforms.

### TL1 ENUM Types Changed

The following enum types have been merged into the EQUIPMENT\_TYPE enum type.

- EQUIPMENT\_TYPE\_15310
- EQUIPMENT\_TYPE\_15327
- EQUIPMENT\_TYPE\_15454

### TL1 ENUM Items Added or Removed

The following section, including [Table 5](#) through [Table 33](#), highlights ENUM items changed (added or removed) for Release 6.0.x, by ENUM type.

**Table 5** *ADDRTYPE enum items added to Release 6.0.x*

ENUM Name	ENUM Value
ADDRTYPE_ENUM_IP	“IP”
ADDRTYPE_ENUM_IPANDNSAP	“IP-AND-NSAP”
ADDRTYPE_ENUM_NSAP	“NSAP”

ADDRTYPE is used in the following commands:

- DLT-TADRMAP

**Table 6** *CARDMODE enum items added to Release 6.0.x*

ENUM Name	ENUM Value
CARDMODE_DS1E1_DS1ONLY	“DS1E1-DS1ONLY”
CARDMODE_DS1E1_E1ONLY	“DS1E1-E1ONLY”

CARDMODE is used in the following commands:

- ED-EQPT
- ENT-EQPT
- RTRV-EQPT

**Table 7** *DL\_TYPE enum items added to Release 6.0.x*

ENUM Name	ENUM Value
DL_TYPE_ACCEPT	“ACPT”
DL_TYPE_CANC	“CANC”

DL\_TYPE is used in the following commands:

- APPLY

**Table 8** *ENCODING enum items added to Release 6.0.x*

ENUM Name	ENUM Value
ENCODING_ENUM_LV	“LV”
ENCODING_ENUM_RAWCISCO	“RAW-CISCO”
ENCODING_ENUM_RAWSTD	“RAW-STD”

ENCODING is used in the following commands:

- ENT-TADRMAP

**Table 9** *ENV\_ALM enum items added to Release 6.0.x*

ENUM Name	ENUM Value
ENV_ALM_ENV_ALM_ENGTRANS	“ENGTRANS”
ENV_ALM_ENV_ALM_FUELLEAK	“FUELLEAK”
ENV_ALM_ENV_ALM_GASALARM	“GASALARM”
ENV_ALM_ENV_ALM_HATCH	“HATCH”
ENV_ALM_ENV_ALM_LEVELCON	“LEVELCON”
ENV_ALM_ENV_ALM_LVDADSL	“LVDADSL”
ENV_ALM_ENV_ALM_LVDBYPAS	“LVDBYPAS”

**Table 9** ENV\_ALM enum items added to Release 6.0.x (Continued)

ENUM Name	ENUM Value
ENV_ALM_ENV_ALM_PWRMJ	“PWRMJ”
ENV_ALM_ENV_ALM_PWRMN	“PWRMN”
ENV_ALM_ENV_ALM_PWR_139	“PWR-139”
ENV_ALM_ENV_ALM_PWR_190	“PWR-190”
ENV_ALM_ENV_ALM_RINGENMN	“RINGENMN”
ENV_ALM_ENV_ALM_RINGGENMJ	“RINGGENMJ”
ENV_ALM_ENV_ALM_RTACADSL	“RTACADSL”
ENV_ALM_ENV_ALM_RTACCRIT	“RTACCRIT”
ENV_ALM_ENV_ALM_RTACPWR	“RTACPWR”
ENV_ALM_ENV_ALM_RTACPWRENG	“RTACPWRENG”
ENV_ALM_ENV_ALM_RTBAYPWR	“RTBAYPWR”
ENV_ALM_ENV_ALM_RTRVENG	“RTRVENG”
ENV_ALM_ENV_ALM_TEMP	“TEMP”
ENV_ALM_ENV_ALM_TREPEATER	“TREPEATER”

ENV\_ALM is used in the following commands:

- RTRV-ALM-ENV
- RTRV-ATTR-ENV
- RTRV-COND-ENV
- SET-ATTR-ENV

**Table 10** EQUIPMENT\_TYPE enum items added to Release 6.0.x

ENUM Name	ENUM Value
EQUIPMENT_TYPE_ET_DS1_E1_56	“DS1-E1-56”
EQUIPMENT_TYPE_ET_FILLER	“FILLER”
EQUIPMENT_TYPE_ET_ML100FX	“ML100X-8”
EQUIPMENT_TYPE_ET_MRC_12	“MRC-12”
EQUIPMENT_TYPE_ET_OC192_XFP	“OC192-XFP”
EQUIPMENT_TYPE_ET_STM64_XFP	“STM64-XFP” (SDH Nomenclature of OC192-XFP)
EQUIPMENT_TYPE_ET_XCVXC10G	“XCVXC-10G”
EQUIPMENT_TYPE_ET_OPT_BST_E	“OPT-BST-E”

EQUIPMENT\_TYPE is used in the following commands:

- CHG-EQPT
- ENT-EQPT

**Table 11** *EQPT\_TYPE enum items added to Release 6.0.x*

ENUM Name	ENUM Value
EQPT_TYPE_EQPT_ID_DS1_E1_56	“DS1-E1-56”
EQPT_TYPE_EQPT_ID_FILLER_CARD	“FILLER”
EQPT_TYPE_EQPT_ID_ML100FX	“ML100X-8”
EQPT_TYPE_EQPT_ID_MRC_12	“MRC-12”
EQPT_TYPE_EQPT_ID_OC192_XFP	“OC192-XFP”
EQPT_TYPE_EQPT_ID_STM64_XFP	“STM64-XFP” (SDH Nomenclature of OC192-XFP)
EQPT_TYPE_EQPT_ID_XCVXC10G	“XCVXC-10G”
EQPT_TYPE_EQPT_ID_OPT_BST_E	“OPT-BST-E”

EQPT\_TYPE is used in the following command response:

- REPT\_EVT

**Table 12** *FC\_LINKRATE enum items dropped from Release 5.0.x*

ENUM Name	ENUM Value
FC_LINKRATE_1GFC	“1GFC”
FC_LINKRATE_2GFC	“2GFC”

FC\_LINKRATE is used in the following commands:

- RTRV-FC

**Table 13** *FC\_LINKRATE enum items added to Release 6.0.x*

ENUM Name	ENUM Value
FC_LINKRATE_1GBPS	“1GBPS”
FC_LINKRATE_2GBPS	“2GBPS”

FC\_LINKRATE is used in the following commands:

- RTRV-FC

**Table 14** *FRAME\_FORMAT enum items added to Release 6.0.x*

ENUM Name	ENUM Value
FRAME_FORMAT_LT_JESF	“JESF”

FRAME\_FORMAT is used in the following commands:

- ED-BITS
- ED-DS1
- ED-E1
- ED-T1

- RTRV-BITS
- RTRV-DS1
- RTRV-E1
- RTRV-T1

**Table 15** *LO\_XC\_MODE enum items added to Release 6.0.x*

ENUM Name	ENUM Value
LO_XC_MODE_MIXED	“MIXED”
LO_XC_MODE_VC11	“VC11”
LO_XC_MODE_VC12	“VC12”
LO_XC_MODE_VT1	“VT1”
LO_XC_MODE_VT2	“VT2”

LO\_XC\_MODE is used in the following commands:

- ED-NE-PATH
- RTRV-NE-PATH

**Table 16** *LPBK\_TYPE enum items dropped from Release 5.0.x*

ENUM Name	ENUM Value
LPBK_TYPE_FE_CMD_ESF_PAYLD_LPBK	“PAYLOAD”

FC\_LINKRATE is used in the following commands:

- RTRV-FC

**Table 17** *LPBK\_TYPE enum items added to Release 6.0.x*

ENUM Name	ENUM Value
LPBK_TYPE_FE_CMD_ESF_PAYLD_LPBK	“FE-CMD-ESF-PAYLOAD”
LPBK_TYPE_PAYLOAD_LPBK	“PAYLOAD”

LPBK\_TYPE is used in the following commands:

- OPR-LPBK-MOD2
- RLS-LPBK-MOD2

**Table 18** *MOD2 enum items added to Release 6.0.x*

ENUM Name	ENUM Value
MOD2_M2_VC11	“VC11”

MOD2 is used in the following commands:

- RTRV-FFP-MOD2
- RTRV-LNK-MOD2LNK

- RTRV-NE-APC
- RTRV-NE-WDMANS
- RTRV-TRC-OCH
- SCHED-PMREPT-MOD2

**Table 19** *MOD2ALM enum items added to Release 6.0.x*

ENUM Name	ENUM Value
MOD2ALM_M2_VC11	“VC11”

MOD2ALM is used in the following commands:

- RTRV-ALM-MOD2ALM
- RTRV-COND-MOD2ALM

**Table 20** *MOD2B enum items added to Release 6.0.x*

ENUM Name	ENUM Value
MOD2B_M2_TSC	“TSC”
MOD2B_M2_VC11	“VC11”

MOD2B is used in the following commands:

- ALS
- RTRV-ALM-ALL
- RTRV-ALM-BITS
- RTRV-ALM-EQPT
- RTRV-ALM-SYNCN
- RTRV-COND-ALL
- RTRV-COND-BITS
- RTRV-COND-EQPT
- RTRV-COND-SYNCN
- RTRV-PM-MOD2
- RTRV-TH-ALL
- RTRV-TH-MOD2

**Table 21** *MOD\_PATH enum items added to Release 6.0.x*

ENUM Name	ENUM Value
MOD_PATH_M2_VC11	“VC11”

MOD\_PATH is used in the following commands:

- ENT-VCG
- RTRV-CRS

- RTRV-PATH
- RTRV-TRC-OC48
- RTRV-VCG

**Table 22** *OPTICAL\_WLEN enum items added to Release 6.0.x*

ENUM Name	ENUM Value
OPTICAL_WLEN_WL_1310	"1310"
OPTICAL_WLEN_WL_1470	"1470"
OPTICAL_WLEN_WL_1490	"1490"
OPTICAL_WLEN_WL_1510	"1510"
OPTICAL_WLEN_WL_1530	"1530"
OPTICAL_WLEN_WL_1550	"1550"
OPTICAL_WLEN_WL_1570	"1570"
OPTICAL_WLEN_WL_1590	"1590"
OPTICAL_WLEN_WL_1610	"1610"

OPTICAL\_WLEN is used in the following commands:

- ED-10GIGE
- ED-DWDM-CLNT
- ED-EQPT
- ED-FC
- ED-GIGE
- ED-OCH
- ED-OCN-TYPE
- ENT-EQPT
- RTRV-10GIGE
- RTRV-DWDM-CLNT
- RTRV-EQPT
- RTRV-FC
- RTRV-GIGE
- RTRV-LNK-MOD2LNK
- RTRV-OCH
- RTRV-OCN-TYPE

**Table 23** *OPTICS enum items added to Release 6.0.x*

ENUM Name	ENUM Value
OPTICS_OP_100_BASE_FX	"100_BASE_FX"
OPTICS_OP_100_BASE_LX	"100_BASE_LX"

OPTICS is used in the following commands:

- ED-GIGE
- RTRV-FSTE
- RTRV-G1000
- RTRV-GIGE

**Table 24** *PROTOCOLAID enum items added to Release 6.0.x*

ENUM Name	ENUM Value
PROTOCOLAID_EMS	“EMS”
PROTOCOLAID_SHELL	“SHELL”
PROTOCOLAID_SNMP	“SNMP”
PROTOCOLAID_TL1	“TL1”

PROTOCOLAID is used in the following commands:

- ED-CMD-SECU

**Table 25** *PROTOCOLSTAT enum items added to Release 6.0.x*

ENUM Name	ENUM Value
PROTOCOLSTAT_DISABLED	“DISABLED”
PROTOCOLSTAT_SECURE	“SECURE”
PROTOCOLSTAT_UNSECURE	“UNSECURE”

PROTOCOLSTAT is used in the following commands:

- ED-PROTOCOL

**Table 26** *REACH enum items added to Release 6.0.x*

ENUM Name	ENUM Value
REACH_AUTOPROV	“AUTOPROV”
REACH_CX	“CX”
REACH_DX	“DX”
REACH_ER	“ER”
REACH_EW	“EW”
REACH_HX	“HX”
REACH_I1	“I1”
REACH_I2	“I2”
REACH_I3	“I3”
REACH_I5	“I5”
REACH_IR_1	“IR-1”
REACH_IR_2	“IR-2”

**Table 26 REACH enum items added to Release 6.0.x (Continued)**

<b>ENUM Name</b>	<b>ENUM Value</b>
REACH_IR_3	"IR-3"
REACH_IR_5	"IR-5"
REACH_L1	"L1"
REACH_L2	"L2"
REACH_L3	"L3"
REACH_L5	"L5"
REACH_LR	"LR"
REACH_LRM	"LRM"
REACH_LR_1	"LR-1"
REACH_LR_2	"LR-2"
REACH_LR_3	"LR-3"
REACH_LR_5	"LR-5"
REACH_LW	"LW"
REACH_LX	"LX"
REACH_MM	"MM"
REACH_MX	"MX"
REACH_PIL1	"PIL1"
REACH_S1	"S1"
REACH_S2	"S2"
REACH_S3	"S3"
REACH_S5	"S5"
REACH_SM	"SM"
REACH_SR	"SR"
REACH_SR_1	"SR-1"
REACH_SR_2	"SR-2"
REACH_SR_3	"SR-3"
REACH_SR_5	"SR-5"
REACH_SW	"SW"
REACH_SX	"SX"
REACH_T	"T"
REACH_V2	"V2"
REACH_V3	"V3"
REACH_VX	"VX"
REACH_ZX	"ZX"

REACH is used in the following commands:

- ED-10GIGE
- ED-DWDM-CLNT
- ED-FC
- ED-GIGE
- ED-OCN-TYPE
- RTRV-10GIGE
- RTRV-DWDM-CLNT
- RTRV-FC
- RTRV-GIGE
- RTRV-OCN-TYPE

**Table 27** REQTYPE enum items added to Release 6.0.x

ENUM Name	ENUM Value
REQTYPE_ENH_24HR_BES	“ENH-24HR-BES”
REQTYPE_ENH_24HR_CSS_AND_LOFC	“ENH-24HR-CSS-AND-LOFC”
REQTYPE_ENH_24HR_ES	“ENH-24HR-ES”
REQTYPE_ENH_24HR_SES	“ENH-24HR-SES”
REQTYPE_ENH_24HR_UAS	“ENH-24HR-UAS”

REQTYPE is used in the following commands:

- RTRV-BFDLPM-MOD2

**Table 28** RFILE enum items added to Release 6.0.x

ENUM Name	ENUM Value
RFILE_LOG	“RFILE-LOG”

RFILE is used in the following commands:

- COPY-IOSCFG
- COPY-RFILE

**Table 29** SYNCMAP enum items added to Release 6.0.x

ENUM Name	ENUM Value
SYNCMAP_ASYNC	“ASYNC”
SYNCMAP_BYTE	“BYTE”

SYNCMAP is used in the following commands:

- ED-T1
- RTRV-T1

**Table 30** *SYNC\_CLOCK\_REF\_QUALITY\_LEVEL enum items dropped from Release 5.0.x*

ENUM Name	ENUM Value
SYNC_CLOCK_REF_QUALITY_LEVEL_QREF_RES_SDH	“RES-SDH”

SYNC\_CLOCK\_REF\_QUALITY\_LEVEL is used in the following commands:

- ED-BITS
- ED-E1
- ED-OCN-TYPE
- ED-T1
- RTRV-BITS
- RTRV-E1
- RTRV-OCN-TYPE
- RTRV-SYCN
- RTRV-T1

**Table 31** *TIDADRMODE enum items added to Release 6.0.x*

ENUM Name	ENUM Value
TIDADRMODE_ENUM_ALL	“ALL”
TIDADRMODE_ENUM_DISC	“DISC”
TIDADRMODE_ENUM_IP	“IP”
TIDADRMODE_ENUM_NSAP	“NSAP”
TIDADRMODE_ENUM_PROV	“PROV”

TIDADRMODE is used in the following commands:

- RTRV-TADRM

**Table 32** *TRANSMODE enum items added to Release 6.0.x*

ENUM Name	ENUM Value
TRANSMODE_AU3	“AU3”
TRANSMODE_AU4	“AU4”
TRANSMODE_SONET	“SONET”

TRANSMODE is used in the following commands:

- ED-EQPT
- ENT-EQPT
- RTRV-EQPT

**Table 33** VTMAP enum items added to Release 6.0.x

ENUM Name	ENUM Value
VTMAP_GR253	“GR253”
VTMAP_INDUSTRY	“INDUSTRY”

VTMAP is used in the following commands:

- ED-T1
- RTRV-T1

## Related Documentation

### Release-Specific Documents

- *Release Notes for the Cisco ONS 15454 SDH, Release 6.0*
- *Cisco ONS 15454 SDH Software Upgrade Guide, Release 6.0*

### 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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned 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. (1110R)

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

© 2007 Cisco Systems, Inc. All rights reserved.