



Release Notes for Cisco ONS 15454 Release 7.0.1

June 2008

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15454 ANSI MSTP. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to the “Release 7.0.1” version of the *Cisco ONS 15454 DWDM Reference Manual*, *Cisco ONS 15454 DWDM Troubleshooting Guide*, *Cisco ONS 15454 DWDM Procedure Guide*, *Cisco ONS SONET TL1 Command Guide*, and *Cisco ONS SONET TL1 Command Quick Reference Guide*; and the “Release 7.0” version of the *Cisco ONS 15454 Procedure Guide*; *Cisco ONS 15454 Reference Manual*; and *Cisco ONS 15454 Troubleshooting Guide*. For the most current version of the *Release Notes for Cisco ONS 15454 Release 7.0.1*, visit the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/454relnt/index.htm>

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

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl



Note

ONS 15454 Release 7.0.1 is intended for DWDM deployment only. For SONET deployment use the most current maintenance release of Release 7.0.x. For caveats and resolved items pertaining to non-DWDM specific aspects of Release 7.0.x refer to the Release Notes for ONS 15454 Release 7.0.

Contents

- [Changes to the Release Notes, page 2](#)
- [Caveats, page 2](#)
- [Resolved Caveats for Release 7.0.1, page 13](#)
- [New Features and Functionality, page 15](#)
- [Related Documentation, page 17](#)
- [Obtaining Documentation, page 18](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

[Documentation Feedback, page 19](#)

[Cisco Product Security Overview, page 19](#)

[Obtaining Technical Assistance, page 20](#)

[Obtaining Additional Publications and Information, page 21](#)

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15454 Release 7.0.1* since the production of the Cisco ONS 15454 System Software CD for Release 7.0.1.

The following changes have been added to the release notes for Release 7.0.1.

Changes to Caveats

The following caveats have been added to the release notes:

[CSCse07471](#)

[CSCsd55460](#)

[CSCsl22337](#)

Caveats

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

Alarms

CSCsj26750

When the card type in CTC is changed from DS1_14 to DS1_E1_56 with DS1-14 physical card in the slot, the LED in DS1_14 card will show Act (Green) LED, instead of Fail (RED) LED. This issue will be resolved in a future release.

Hardware

CSCuk48503

Under specific conditions the 4x2.5G FEC Muxponder unit 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 textbox 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 not be resolved.

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.

CSCsd49163

In a Y cable protection group using TXP_MR_10E or TXT_MR_10DME cards the switch time when you remove a trunk fibre is sometimes longer than 50 ms. This issue will be resolved in a future release.

CSCsd21294

If you disconnect a subtended shelf from a multi-shelf node controller, the Communication failure is not correctly characterized by the LCD and Fan Tray LEDs of the multi-shelf node. You can use CTC or TL1 to get the status of the nodes correctly, however. This issue will be resolved in a future release.

CSCsd22880

The APC regulations when a channel is dropped from an AD4C are not correctly managed. Consider a channel dropped from the first CHAN-TX port of an AD4C card. In the CTC > Maintenance > DWDM tab the APC Last modification date is never changed; it remains N/A. In any case of span aging conditions, the object is always incorrectly referred to the fourth channel of the add/drop card, even if that channel is not active. This issue will be resolved in a future release.

CSCsd32197

Four channel Mux/Demux PM counters on CHAN ports (both TX and RX) fail to update after midnight in both CTM and TL1. This issue will be resolved in a future release.

CSCsd33369

ALS mode can be set to Auto Restart on a TXP_MR_10G trunk port via TL1 when the TXP_MR_10G card is configured for an Ethernet 10G LAN payload. This issue will be resolved in a future release.

CSCed23484

A user might remain in the logged-in state after rebooting the PC while logged into a node running CTC. The user login will time out once the "Idle User Timeout" limit is up. Alternatively, you can log in as a superuser and force the user off. This issue will not be resolved.

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.

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.

CSCef29516

The ALS pulse recovery minimum 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 LOS-P 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.

Common Control Cards

CSCsd32113

The link status of the front Ethernet port is always reported as “up” by diagnostics. This is true whether or not there is an Ethernet connection to the front panel. This issue applies to TCC2P cards in secure mode. The link status LEDs on the front panel are not affected; they reflect the true state of the link. When examining diagnostics disregard the front-panel link status of TCC2P cards in secure mode. It is not known when or if this issue will be resolved.

DWDM Cards

CSCse07471

An MXP-MR-10DME card in GE mode might not recover from a synchronization loss fault condition. Near end and far end PM Ethernet counters exhibit truncated and errored packets in this case. This has been seen with a particular type of test set sending an invalid order set and truncated packet sequence while in LOS condition. Place the affected client port in OOS-IS state to recover. This issue will be resolved in a future release.

CSCsd47767

TXP_MR_10E transponders can take slightly longer than 50 ms to switch when you place the active trunk port OOS. This issue will be resolved in a future release.

CSCsd00491

On TXP_MR_10G transponders provisioned as terminal loopback on the trunk facility or on a client, the GCC channel is disabled. This issue will be resolved in Release 8.0.

CSCsd14754

After an LOS clears the on trunk port of a transponder, the alarms, ODUk-SD and OTUk-SD, are sometimes raised at the same time; the OTUk-SD should mask the ODUk-SD, but fails to do so. This issue will be resolved in Release 8.0.

CSCsd40399

On a TXP-MR-10E transponder provisioned as Line, Section or Transparent terminated, with OTN ON, FEC set to STD,ENH or disable, and a valid signal (OC192) on the client port, if OTUk-LOF is injected two alarms are raised: PTIM and OTU-LOF. The OTUk-LOF should mask the PTIM, but fails to do so. This issue will be resolved in Release 8.0.

CSCsd33382

A configured default of Ethernet 10G LAN for the TXP_MR_10G port assignment might be ignored. This can be seen when you provision the following default values for a TXP_MR_10G card:

- TXP-MR-10G.config.AlsMode = Auto Restart
- TXP-MR-10G.config.client.mrPortAssignment = 10G Ethernet LAN Phy

This provisioning is invalid as “Auto Restart” ALS (Automatic Laser Shutdown) mode is not valid for Ethernet payloads. However it is accepted by the NE. Now if you provision a TXP-MR-10G card, the configured default payload type of “Ethernet 10G LAN” is ignored, since it is inconsistent with the ALS value. It is not known if or when this issue will be resolved.

CSCeh22604

When an MXP_MR_2.5G card is in MIXED or ESCON mode, TCA and alarm optical thresholds of Tx power for laser bias are configurable for ESCON payload, though not supported. This issue will be resolved in the future release.

CSCei19148

When a port is placed in-service while the conditions necessary to squelch the port are present, as in when the trunk port on a DWDM card is OOS,DSBLD and a client port is placed in-service, the client will momentarily enable, emitting light, before squelching due to the trunk OOS,DSBLD condition. The pulse is approximately 500 ms. This issue will not be resolved.

CSCei87554

When using a 1GE payload over the TXP_MR_2.5G the IfInErrors counter does not report oversized, undersized, or CRC errored frames, but rather, reports frame coding only. This issue will not be resolved.

CSCsb47323

For MXP_MR_10DME-C and MXP_MR_10DME-L cards, an unexpected RFI condition might be raised along with an OTUk-BDI. When there is an LOS downstream, the node receives OTUk-BDI. Because of the placement of dual OTN and SONET wrappers, it can also receive an RFI. This issue will not be resolved.

CSCsb79548

A long traffic hit can occur when an active TCC2/TCC2P resets while an MXP_MR_10DME-C or MXP_MR_10DME-L card is rebooting.

This issue can be reproduced as follows:

-
- Step 1** Set up two MXP_MR_10DME-C or MXP_MR_10DME-L cards, connected back-to-back in two different nodes, A and B.
 - Step 2** Ensure that Node A has two TCC2 cards; one is active, and the other is standby.
 - Step 3** Set up any kind of traffic between the two MXP_MR_10DME-C or MXP_MR_10DME-L cards.
 - Step 4** Soft reset the MXP_MR_10DME card in Node A, then soft reset the active TCC2/TCC2P.
-

OTUk/ODUk-SD, FEC Uncorrected word alarms are raised on the trunk port. Traffic goes down and does not recover until the MXP_MR_10DME card is able to come up. This issue will be resolved in a future release.

CSCsb94736

After a fault condition (trunk LOS or Y-cable switch) an MXP_MR_10DME card might fail to detect the login message and traffic might not start for some minutes (after multiple login trials). This can occur in an N-F configuration with MDS switch and MXP_MR_10DME distance extension on, where test

equipment traffic is set to 2G Fibre channel (FC) full bandwidth occupancy and started. Stop traffic or keep bandwidth occupancy below 80% during the login phase to work around this issue. This issue will not be resolved.

CSCsb95918

All GFP related alarms are raised with their active severities on the standby card after a Y-Cable protection switch. When a DWDM card (with GFP support) in a Y-Cable protection group becomes standby as a result of a Y-Cable protection switch, the GFP alarms raised when the card was active retain their severities instead of assuming standby severities. The alarms can be seen in the alarm pane if not suppressed, or in the condition pane if suppressed. This issue will be resolved in a future release.

CSCsc36494

Manual Y cable switches with squelching turned off can cause a Fibre channel link with Brocade switches to go down.

This issue can be reproduced as follows:

-
- Step 1** Set up MXP_MR_10DME cards so that they are Y cable protected. Squelching is provisioned to be off. Distance extension is turned on.
 - Step 2** The path between the working pair of Y cable protected cards, has no distance introduced. But the protect path has a delay of 800 km introduced.
 - Step 3** Start Fibre channel traffic with brocade switches.
 - Step 4** Perform user-initiated manual Y cable switches from CTC.
-

After a few switchovers, the FC link will go down. SIGLOSS and GFP-CSF alarms are seen on the CTC. Cisco recommends you provision squelching to be on when interworking with brocade switches. If for some reason, squelching must be off with brocade switches, Cisco recommends you use a FORCE command to perform Y cable switches. It is not known when or if this issue will be resolved.

CSCsc55771

When two MXP_MR_10DME cards are interconnected through OC-192/STM-64 cross connects and traffic is up, if you hard reset one of the MXP_MR_10DME cards, the traffic might fail to recover. To recover traffic flow, place the client port in OOS,DSBLD state, delete the PPM then recreate it, and re-provision the port. This issue will be resolved in a future release.

CSCsc60472

CTC is not able to discover a TL1 OCHCC circuit provisioned over an ITU-T line card (ITU-T OC48/STM16 and ITU-T OC192/STM64). This issue can occur when, using the TL1 client interface, you create the OCHNC layer that will be used by the OCHCC circuit, then create the OCHCC connections that involve the ITU-T line cards. The result is an OCHNC and two OCHCC partial circuits, instead of an OCHNC and a single OCHCC complete circuit. This issue will not be resolved.

CSCsc62581

A T-TX-PWR-MIN TCA is raised and a wrong receive optical power value (of -40 dB) is displayed after a card is reset. The alert and incorrect Rx value both clear in the next 15 min. sample period. This issue will be resolved in a future release.

CSCsc54518

The OPT-BST amplifier card is in a LASER OFF state, even if input power is provided to all input ports. This issue only occurs with Release 7.0 and can be reproduced on a card with the amplifier turned on, in operating conditions (with lasers on) as follows.

-
- Step 1** From the card-level **Maintenance** tab set ALS Mode to **Manual Restart** and click **Apply**.
 - Step 2** Set **OSRI** to **ON** and click **Apply**. The amplifier turns off.
 - Step 3** Set **OSRI** to **OFF** and click **Apply**. The amplifier stays turned off (this is expected, since in Manual Restart the lasers are turned back on by means of a Request Laser Restart command issued in CTC).
 - Step 4** Select the **Request Laser Restart** check box in the **Maintenance** tab and click **Apply**.
-

The amplifier goes into APR for 9 seconds (correct), but after this it turns off; it should go into LASER ON state (State 4 at module level). If this issue occurs, change the card from manual restart to auto restart, then toggle OSRI ON and OFF. This issue will be resolved in a future release.

CSCsc14290

LOW communication between two nodes equipped with TXP-MR-10E and AIC-I cards does not work with TXP-MR-10E cards in line termination mode, G.709 enabled, GCC present on the trunk port, and LOW circuits created between the transponders and AIC-I; Cisco recommends that you use EOW instead. This issue will be resolved in a future release.

CSCsc58941

Trunk ports of the TXPP_MR_2.5G and MXPP_MR_2.5G can be in facility and terminal loopback at the same time. This can occur if you provision terminal loopback on the protected trunk port after putting the trunk ports in facility loopback. You can clear this condition by removing loopback provisioning on the trunk ports. This issue will be resolved in a future release.

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.

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.

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 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, using TXP-MR-2.5G cards, 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 do not support any 8B/10B Payload PM monitoring. This is as designed.

CSCea78210

The TXP_MR_2.5G and TXPP_MR_2.5G cards do not support TX Optical power performance monitoring on the trunk port. This is as designed.

CSCeb32065

Once engaged, 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.

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.

CSCeb12609

For the TXPP, attenuating Port 2 Rx signal, SD, and SF alarms are not declared before LOS-P 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.

Interoperability

CSCsl22337

When a DWDM ring or network has to be managed through a Telcordia operations support system (OSS), every node in the network must be set up as multi-shelf. OLA sites and nodes with one shelf must be set up as "multi-shelf stand-alone" to avoid the use of LAN switches.

Resolved Caveats for Release 7.0.1

This section documents caveats resolved in Release 7.0 and 7.0.1.

Maintenance and Administration

CSCsd55460

When upgrading a network to Release 6.0.1, 6.1, or 7.0, where LOS-P exists on a pass-through port of a WSS for a ROADM node, if you change the circuit state to OOS,DSBLD and then again to IS-AINS, the circuit fails to go up. There are two possible work-arounds:

1. Change the calibration value on the pass-through port of the WSS.
2. When the circuit is in OOS state, relaunch ANS.

This issue is resolved in Releases 6.2 and 7.0.1.

CSCsd31753

After card pre-provisioning, if you launch an ANS default patchcord using CTC or TL1, the TCC resets and internal patchcords are not created. This can occur in an OADM or Flexible terminal MSTP node configured with any possible combination of AD-xC card, but containing wavelength 1560.61 (that is AD-1C-60.6, AD-2C-59.7 and AD-4C-58.1). Any Fiber stage configuration will display this issue. This issue is resolved in Release 7.0.1.

CSCsc61572

Traffic incurs a hit when a Y-cable protection group is created with an IS working facility and OOS,DSBLD protect facility. If a Y-cable protection group is created, and traffic is flowing cleanly over the working facility, and the protect facility is OOS,DSBLD, the working facility will momentarily shutdown and then restart. This behavior is generally not seen when a deleted protection group is

recreated, provided that the Y-cable cards and the shelf controller have not been reset since the protection group was deleted. Therefore, to reproduce this issue it is necessary to soft reset the Y-cable cards and the shelf controller before creating the protection group. This issue is resolved in Release 7.0.1.

CSCsd32106

Traffic is lost briefly when a Y-cable group is created and the working facility is preprovisioned. The traffic hit occurs when traffic is flowing over the planned protect path, and the planned working path is only preprovisioned. When the Y-cable group is created, the group selects the working path, interrupting traffic. Within one second the group selects the protect path, restoring traffic. This issue is resolved in Release 7.0.1.

CSCsd18450

A node with TCC2P cards in “Data Comm Secure Mode” and the SOCKS Proxy in ENE mode cannot be reached via its LAN connection. This occurs when the TCC2P cards are placed in Data Comm Secure Mode and the SOCKS Proxy is configured for ENE operation. Under most IP address configurations, the node will become unreachable by its backplane connection. Also, if the front panel Ethernet and the backplane Ethernet are on the same LAN, the node might be unreachable via either interface. When both interfaces are on the same LAN, the ARP cache can become corrupted and will contain incorrect data until the ARP entries expire. To work around this issue you can configure the node as a SOCKS Proxy GNE. This is always permissible, even if the node is not connected to the DCN. Also, avoid making an Ethernet connection to the backplane Ethernet of an ENE in secure mode. This issue is resolved in Release 7.0.1.

DWDM Cards

CSCsd33492

Rarely, pre-amplifiers and booster amplifiers (15454-OPT-BST, 15454-OPT-PRE) might raise an equipment failure alarm for an internal communication issue, even though operating conditions remain unaffected. This alarm will disabled APC control in the network and prevent circuit creation. If this occurs, perform a non-traffic affecting reset using the CTC craft terminal on the line card to clear the alarm. This issue occurs only when the line cards have a component mounted with component vendor ID 1025. This issue is resolved in Releases 6.2 and 7.0.1.

CSCsc56015

Extracting an MSTP card and inserting a different type of card in the same slot will result in an MEA alarm and APC DISABLE condition being raised. The APC DISABLE condition will not clear even if you insert the correct card. The workaround is to send a software reset to the active TCC. This issue is resolved in Release 7.0.1.

CSCei37691

The trunk port service state for the TXPP and TXP cards does not transition to OOS-AU,FLT 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 is resolved in Release 7.0.

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.

Electrical IO Cards

CSCsd59042

When upgrading the software from Release 6.x.x to Release 7.x.x, the DS3 and EC1-12 cards fail to load if the node name begins with the letters FL. Changing the node name resolves this issue.

TL1

CSCsc62784

The Calibration Tilt is not properly changed using the TL1 interface. The reference tilt is changed instead. This issue can be seen when you try to change the CALTILT parameter on amplifier cards using the ED-OTS command. To avoid this issue, use CTC. This issue is resolved in Release 7.0.1.

New Features and Functionality

This section highlights new features and functionality for Release 7.0.1. For detailed documentation of each of these features, consult the user documentation.

New Software Features and Functionality

Secure Mode on Multishelf

In Release 7.0.1 both single-shelf and multishelf configurations support the use of secure mode and locked secure mode. The procedures for using secure mode in multishelf configurations do not differ from the procedures used in single shelf configurations. The default setting for secure mode is “off.” Consult the user documentation prior to using secure mode in any configuration.

NLAC Trunk TCA Suppression

With Release 7.0.1 OTN Based Network Level alarm correlation adds the ability to automatically demote Threshold Crossing Alerts (TCAs), throttling spontaneous multiple notifications of management interfaces when a server alarm is outstanding on the facility or port.

Threshold defaults are defined for near end and/or far end and at 15-minute or one-day intervals. When LOS-P, LOS, or LOF alarms occur on TXP or MXP cards, different TCAs are suppressed depending on how the trunk is configured (G.709, SONET, or SDH). See the user documentation for a table of TCAs for each type of trunk framing and alarm.

TCA suppression does not extend to optical thresholds such as OPR (optical power received). Optical threshold TCAs can effectively be suppressed by setting their thresholds to the maximum value. TCA suppression also does not extend to client ports; it only applies to TXP and MXP trunk ports when they are configured as G.709, SONET, or SDH. TCA suppression does not extend to 10GE payloads.

Because they are preempted from being raised, suppressed TCAs do not show up as Not Reported (NR) conditions in the CTC Conditions tab and they cannot be retrieved with the RTRV-COND TL1 command.

DWDM Alarm Correlation Exceptions

In multishelf correlated alarms the Payload Missing Indication (PMI) condition is raised at the far end to correlate optical multiplex section (OMS) and optical transmission section (OTS) communication failures. A single PMI condition is sent when every channel on the aggregated port is lost; that is, when all pass-through channels are lost and there are no active add channels. If there are add channels on the node, the Forward Defect Indication (FDI) condition is sent downstream to indicate that a given channel has been lost upstream.

In Release 7.0.1, two exceptions apply to DWDM alarm correlation as previously described. In ROADM configurations, if any drop traffic is lost on a WSS COM-TX port, the event does not raise a PMI condition for the COM-TX port; instead, each errored channel associated with the CHAN-(i)-TX port raises an FDI condition. Similarly, if a WSS EXP-RX port loses any pass-through traffic, an FDI condition is raised against each errored channel associated with the PT-(i) port and no PMI is raised on the EXP-RX port.

TL1 Support for OCHCC RTRV-PATH-OCH Command

Release 7.0.1 adds a TL1 command, RTRV-PATH-OCH, to retrieve all OCH terminations inside a specified node. The TL1 RTRV-PATH-OCH command lists in output all OCH Terminations belonging to a single optical connection. The command accepts in input either the wavelength or any OCH Termination. The output lists all the OCH Terminations belonging to the circuit in the TID. For a full description of the command and its application consult the *Cisco ONS SONET TL1 Command Guide* for Release 7.0.1.

OCH Optical Link Support

Release 7.0.1 add support for optical provisionable patchcords, or virtual links between OCH filter and trunk ports. For the specific situations in which a patchcord is necessary, refer to the “Management Network Connectivity” chapter in the *Cisco ONS 15454 DWDM Reference Manual*.

CTC Support for OCH Optical Links

If a provisionable patchcord is manually created using CTC, it automatically tunes the TXP or MXP trunk as an OCH filter—provided that the TXP or MXP is set to autoprovisioning at the first tunable wavelength.

TL1 Support for OCH Optical Links

In Release 7.0.1 TL1 the ENT-LNK command is enhanced to support the creation of optical links between optical channel ports of the same wavelength. When the enhanced command is used to create an optical link between two optical channel ports, where the first port belongs to an OCH filter and the second port is an OCH trunk, the second port can be automatically tuned to the same wavelength as that of the OCH filter, if it has not been set yet. The ENT-LNK command From and To Band AIDs are

replaced with new Channel AIDs in Release 7.0.1. Channel AIDs access the optical channels (OCH) layer of an optical networking unit. For specific channel values and their descriptions consult the *Cisco ONS SONET TL1 Command Guide* for Release 7.0.1.

NE Defaults Support for ALS Mode

Release 7.0.1 adds the ability to disable the ALS/APR through an NE default. The Defaults editor and defaults file add an ALS mode entry that can be set to Disabled or Auto Restart for the following cards:

- OPT-BST
- OPT-BST-L
- OSCM
- OSC-CSM

The default value for ALS mode on the OPT-BST, OPT-BST-L, OSCM, and OSC-CSM is Auto Restart (enabled). For information on how ALS card settings achieve network level optical safety consult the “Network Optical Safety—Automatic Laser Shutdown” section in the *Cisco ONS 15454 DWDM Reference Manual*.

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15454, Release 7.0*
- *Release Notes for the Cisco ONS 15454 SDH, Release 7.0.1*
- *Cisco ONS 15454 Software Upgrade Guide, Release 7.0.1*

Platform-Specific Documents

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

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco ONS 15xxx product documentation, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated periodically and may be more current than printed documentation.

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
or view the digital edition at this URL:
<http://cisoiq.texterity.com/cisoiq/sample/>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

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

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

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

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