Release Notes for Cisco ONS 15454 Release 8.6

OL-19058-01
March 2009

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15454 SONET platform. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to the Release 8.5.x version of the *Cisco ONS 15454 DWDM Installation and Operations Guide*; and the Release 8.5.x version of the *Cisco ONS 15454 Procedure Guide*; Release 8.5.x version of the *Cisco ONS 15454 Reference Manual*; Release 8.5.x version of the *Cisco ONS 15454 Troubleshooting Guide*; and Release 8.5.x version of the *Cisco ONS 15454 SONET TL1 Command Guide*. For the most current version of the Release Notes for Cisco ONS 15454 Release 8.6, see the following URL:

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, see the following URL:

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

About Release 8.6

Cisco ONS 15454 Release 8.6 does not include any new features.

Cisco ONS 15454 Release 8.6 is based on Cisco ONS 15454 Release 8.5.2 and Cisco ONS 15454 Release 8.5.3. The Release Notes for Cisco ONS 15454 Release 8.6 contain closed (maintenance) issues and caveats found in Cisco ONS 15454 Release 8.5.2 and 8.5.3. Some bug fixes made in Cisco ONS 15454 Release 8.5.2 are not available in Cisco ONS 15454 Release 8.5.3 and vice versa. For detailed information on bugs fixed refer to the respective sections in this document.

Contents

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

Changes to the Release Notes

This section documents supplemental information that has been added to the *Release Notes for Cisco ONS 15454 Release 8.6* since the production of the Cisco ONS 15454 System Software CD for Release 8.6.

- Added CSCsg42366—Traffic outage occurs when FPGA upgrade is done with manual switch on Y-cable, under Maintenance and Administration sub-section of the Caveats section.

Caveats

Review the notes listed below before deploying the Cisco 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

This section documents caveats for Alarms in Release 8.6.

CSCsm32278 —Alarms at GFP level on MXP-MR-10DME cards do not trigger FLT state on port

Alarms at generic framing procedure (GFP) level on MXP-MR-10DME cards do not trigger an FLT state on the Virtual Facility (VFAC) port. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsl18519 —One CARLOSS and TPTFAIL alarm reported with dual failure on ports of CE-MR-10 card

When dual failure occurs on the ports of the CE-MR-10 card equipped with electrical small form-factor pluggables (SFPs), only one CARLOSS and TPTFAIL alarm is reported. No workaround is available for this issue.This issue will not be resolved.

CSCsm16960 —AUTO RESET alarm cleared before activation

When upgrading software on OC-12 4-port cards from Release 7.0.7 to Release 8.6, the AUTO RESET alarm is cleared before completing activation. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsm19928 —AS-MT condition not persistent against subtended shelf TCC software reset

An AS-MT alarm on the transponder (TXP) card in a subtended shelf of a multishelf configuration is cleared when a soft reset of the TCC is performed. The workaround is to change the port status to IS-AINS and OOS-MT. This issue will be resolved in a future release.

CSCsu40460—External remote alarm relay is not set correctly

The External Alarm Relay (ERA) (A1/B1 VIS/AUD on the backplane) on a node created on the Cisco ONS 15454 platform indicates incorrectly set remote alarms when remote nodes are raised or alarms are cleared. This issue occurs under the following conditions:

1. The node is stable with no MN/MJ/CR alarms on the entire network on a Cisco ONS 15454 platform.
2. Another node on the network raises an MN/MJ/CR alarm, but it does not update the REM ALARM VIS/AUD contact pins on the backplane.
3. The issue occurs when the remote nodes clear their alarms also. (This issue has been observed since Release 7.0).

The workaround is to create and clear an alarm *or* modify the severity of the already raised alarm (if raised) on the node using the alarm profile.

This issue will be resolved in a future release.

CSCsm32308— Roll-pend(NA) and UNEQ-P(CR) alarms move to Conditions pane on soft reset of active TCC

Roll-pend(NA) and UNEQ-P(CR) alarms move to the Conditions pane when a soft reset is performed on an active TCC during the manual mode of a circuit roll. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsq68460—LCAS-RX-FAIL and LCAS-RX-DNU alarms are not reported for AIS-V and LOP-V for MLMR and CEMR cards

LCAS-RX-FAIL and LCAS-RX-DNU alarms are not reported for AIS-V and LOP-V alarms but seen for other SONET alarms (such as UNEQ) under the following condition:

- Inject AIS or LOP alarm in a HW-LCAS circuit.

No workaround is available for this issue. This issue will be resolved in a future release.

BLSR Functionality

This section documents caveats for bidirectional line switched ring (BLSR) in Release 8.6.

CSCdv53427— Protection vulnerabilities in two-ring, two-fiber MS-SP ring configuration

In a two-ring, two-fiber BLSR configuration (or in a two-ring 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 both broken.

CTC

This section documents CTC caveats in Release 8.6.

CSCsr89201—Unable to launch CTC with emsAccessState=secure after upgrade

After a release upgrade, CTC does not launch on certain 'custom packages.' This issue occurs only on the custom package and while upgrading with the EMS access state set to secure.

The workaround is to use TL1 to change the EMS access state to secure, or delete the database and reboot the node. This issue will be resolved in a future release.

CSCsr47355—Unable to cut new hybrid node into an existing hybrid MSTP ring

When cutting a new node into an existing hybrid ring, the user is unable to run the Update Circuits With New Node Wizard from CTC, and receives the following error message:

EID-2034

Network Circuits Could Not Be Added: cerent.cms.ncp.missingLinks: No Reverse Link!

This issue occurs under the following condition:

- The node being cut into the ring must be a hybrid (MSTP/MSPP) shelf with OSC-CSMs created and In-Service. The problem appears only after OSC connectivity has been established between the new node and the adjacent nodes.

The workaround for this issue is to either manually build cross-connects through a new node using CTC/TL1, or disable OSC on the new node and the adjacent nodes and then run the Update Circuits With New Node Wizard in CTC.

CSCsq73116—PPC does not work on secure mode node

PPC does not work on a secure mode node under the following condition:

- Create a PPC that terminates on a secure mode node. At this point, a new "unknown" node appears and the PPC is not shown on the network map.

No workaround is available for this issue. This issue will be resolved in a future release.

CSCsq88986—Filler card prevents enabling MSTP multishelf

MSTP multishelf cannot be enabled under the following condition:

- At least one filler card is plugged in the shelf.

The workaround is to perform the following steps:

1. Unplug all the filler cards.
2. Enable multishelf. The TCCs will reload.
3. After the TCCs finish reloading, plug in all the required filler cards.

This issue will be resolved in a future release.

CSCsv01621—It is not possible to enter in the WXC card panel

The user cannot open the card configuration panel for any WXC inserted or pre-provisioned in the system. This issue occurs under the following conditions:

1. Configure a multidegree node with WXC.
2. Some WXC cards are inserted in the system but are then “deleted.”

The workaround is to physically remove the “deleted” WXC cards from the slots.

This issue will be resolved in a future release.

Data I/O Cards

This section documents caveats for Data I/O Cards in Release 8.6.

CSCsm09512—Packet drop and VCG-DEG condition observed after hard reset of CE-MR-10 card

The VT1.5-64v or VT1.5-63v circuit moves to VCG degraded state following the hard reset of a CE-MR-10 card. The number of members that are not available for use is approximately 6 to 10. The following workarounds apply:

- To recover from the VCG-DEG condition, transition members to OOS-OOG state, delete them in OOS-OOG state, and then re add them.
- Disabling and reenabling associated ports recovers from this condition. This workaround causes a one-time traffic hit.

This issue will be resolved in a future release.

CSCso66424—LCAS VCG Member Rx side in Add State condition persists after hard reset of CE-MR-10 card

The LCAS VCG Member Rx side in Add State condition might persist after a hard reset of a CE-MR-10 card carrying a VT1.5 HW-LCAS circuit with a member count of greater than 40. The workaround is to place all the affected circuit members in the OOS,OOG state. After all the members have been placed in OOS,OOG state, place them back in IS state. This issue will be resolved in a future release.

CSCsq16464—Traffic on nodes duplicates on ML-series cards

On ML-series cards, if a priority-multicast is configured and a wrap occurs on the shared packet ring (SPR), traffic on some nodes will be duplicated, which can result in sequencing issues in the multicast stream. Multicast video may experience deterioration in clarity. The workaround is to configure the video reception device so that it does not act on the duplicate stream or, if no congestion is present on the ring, the priority-multicast configuration can be removed. This issue will be resolved in a future release.

CSCsu02307—Unable to add members with SD-P alarm present on one member

The ADD condition persists when adding more members to the LCAS circuit signal degrade-path (SD-P) is present on a member. This issue occurs under the following conditions:

1. Create an STS1-2v VCAT, HW-LCAS between a Cisco ONS 15310-MA and Cisco ONS 15454 node.
2. Put the test set in through mode (Agilent VCAT test set).
3. Inject SD-P or SF-P toward the Cisco ONS 15310-MA node. As expected, members go into out of group (OOG).
4. Add some more members (for example, 5) on the span that does not have the test set. As expected, members should be added; however, members are not added to the VCAT group, causing the ADD condition to persist.
5. Add more members when SD-P is present on one of the members and SD-P is injected through the Agilent test set.

Note This issue is seen only with the Agilent GFP test set.

The workaround is to use the OTN test set or variable attenuator to inject SD-P.

This issue will be resolved in a future release.

CSCsw64346—UNEQ raised on CEMR-10 HW LCAS circuit after XC switch

AIS-P conditions change to UNEQ-P on a trunk card that corresponds to members of a HW-LCAS circuit after the XC is switched under the following conditions:

1. Create the circuit with POS ports in IS state. Later, the POS port on one end is placed in OOS,DSBLD state.
2. Perform the XC side-switch is performed.

The workaround is to place the OOS,DSBLD port in IS state.

CSCsu02236—Members of the VT-1.5 LCAS circuits are in idle state

On an ML-MR-10 card, injecting a signal degrade (SD) or signal fail-V (SF-V) on one member and switching the cross-connect (XC) main causes a few members of the VT-1.5 LCAS circuits to become stuck in the Idle state. This issue occurs under the following conditions:

1. Configure two ML-MR-10 cards, that is, ML-MR-10 card A and ML-MR-10 card B.
2. Create a VT1.5-64V circuit between ML-MR-10 card A and ML-MR-10 card B.
3. Inject an SD/SF-P on one member and observe that traffic is reduced on the affected member.
4. Switch the XC main and observe the Stuck Idle state (with sequence number 63) on a few members.

The workaround is to recover from the Stuck Idle condition, move the affected members out of group (OOG), and then back to in group (IG).

CSCsr67830—High traffic hit seen with larger HW-LCAS circuits with fiber pull

A high traffic hit is seen on fiber pull for a HW-LCAS, split-fiber circuit on CE-MR-10, CE-MR-6, and ML-MR-10 cards under the following condition:

- For larger-member HW-LCAS, split-fiber circuits on CE-MR-10, CE-MR-6, and ML-MR-10 cards, a high traffic hit is seen when pulling a fiber on one span.

No workaround is available for this issue. This issue will be resolved in a future release.

CSCsr06085—Error message on CPU switching packets greater than 1500 bytes in length

An error message on CPU switching packets greater than 1500 bytes in length occurs under the following conditions:

- When an IP multicast packet of size > 1500 bytes is received on a BVI interface, an error message is displayed on the console/vty and packets are dropped.

No workaround is available for this issue. This issue will be resolved in a future release.

CSCsm78387—PDI-P alarm causes the Ethernet port to go down when members are deleted on open-ended HW-LCAS VCAT circuit

A path payload defect indication (PDI-P) alarm is raised and the Ethernet port goes down when members are deleted in a circuit under the following conditions:

- A VC-12-63v open-ended HW-LCAS circuit exists between two network elements (NEs).
- All members on the CE-MR-10 card are placed in the OOS,OOG state and the last 45 members are deleted.
- The remaining 18 members on the CE-MR-10 card are placed in IS.

These conditions result in an unbalanced virtual concatenation group (VCG). Traffic is lost and a PDI-P alarm is raised on the card where members were deleted.

The workaround is to place members in the OOG state on both ends. When members are being placed in IS, place them in IS state on both ends of the circuit.This issue will be resolved in a future release.

CSCsm99133 —Packet loss on CE-MR-10 cards running more than 8.5 Gbps traffic during software upgrade

Upgrading software on a Cisco ONS 15454 from Release 8.5.0 or 8.5.1 to a later version causes packet loss on CE-MR-10 cards carrying more than 8.5 Gbps of traffic. The workaround is to do a hard reset on the CE-MR-10 card, which may result in a traffic outage for a few minutes. This issue will not be resolved.

CSCso55327—TCC switch on CE-MR-10 and ML-MR-10 cards causes a traffic hit of up to 180 ms

A reset of a TCC switch on CE-MR-10 and ML-MR-10 cards causes a traffic hit of up to 180 ms on all circuits with software earlier release 9.0. No workaround is available for this issue. This issue will be resolved in a future release.

CSCso94644—LCAS VCG Member Rx side in Add State condition persists after hard reset of CE-MR-10 card or ML-MR-10 card

The LCAS VCG Member Rx side in Add State condition might persist after a hard reset of a CE-MR-10 card or an ML-MR-10 card carrying a HW-LCAS circuit with loopback on split fiber routing. The workaround is to place all the affected circuit members in the OOS,OOG state. After all the members have been placed in OOS,OOG state, place them back in IS state. This issue will be resolved in a future release.

CSCsq02815—Negative values for gfpStatsRxCRCErrors and ifInPayloadCrcErrors parameters in CTC for CE-MR-10 cards

The gfpStatsRxCRCErrors and ifInPayloadCrcErrors performance monitoring parameters in CTC for CE-MR-10 cards can contain negative values. The workaround is to either refresh the Performance > Statistics pane by clicking the Refresh button or by clearing the PM parameters by clicking the Clear button. This issue may be resolved in a future release.

CSCsq05285—Traffic hit of 180 ms on CE-MR-10 cards with VCAT LCAS circuits during software upgrade

Upgrading software on a Cisco ONS 15454 from Release 8.5.0 or 8.5.1 to Release 8.5.2, 8.6 sometimes causes a traffic hit of 180 ms on CE-MR-10 cards with VCAT LCAS circuits. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsq12616—PDI-P alarm from the far-end NE causes Ethernet port to go down

A path payload defect indication (PDI-P) alarm is raised from the far-end NE causing the Ethernet port to go down. This situation happens when all the LCAS members on the near-end NE are changed to OOS,OOG state while all the members on the far-end NE are still in service. This issue occurs while provisioning an open-ended VCAT circuit using CTC or TL1 and modifying the near- end NE of the LCAS circuit, without making modifications to the far-end NE.

The workaround is to perform provisioning steps on both ends, in sequence, rather than completing the near- end and then provisioning the far end. For example, to remove members of a VCG, perform the following steps:

1. On the near-end NE, move members to be deleted to the OOS,OOG state.
2. On the far-end NE, move members to be deleted to the OOS,OOG state.
3. Delete members on the near-end NE.
4. Delete members on the far-end NE.
5. Put other members in IS on the near-end NE, if required.
6. Put other members in IS on the far-end NE, if required.

This issue will be resolved in a future release.

CSCsq20532—Traffic hit of 25 ms occurs in a low-order LCAS circuit

A traffic hit of about 25 ms may occur in a low-order LCAS circuit if members in the OOS,OOG state are deleted in CE-MR-10, CE-MR-6, or ML-MR-10 cards. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsq24264—Traffic hit on CE100T-8 cards during an upgrade from release 8.5.0 to release 8.5.2 or 8.6

An upgrade on Cisco ONS 15454 from Release 8.5.0 to release 8.5.2 or 8.6 followed by a power cycle of the node causes a traffic hit on CE-100T-8 cards. The workaround is to change the Admin state of the CE-100T-8 card to the MT state, followed by a hard reset. This issue will be resolved in a future release.

CSCsq24423—GE port changes continuously when facility loopback is applied on the intermediate optical card

The state of the CE-MR-10 Gigabit Ethernet port changes continuously for an STS-3c HW-LCAS unprotected, split routed circuit when path trace is enabled on all the members and facility loopback is applied on the intermediate optical card. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsq24903 —First data frame sent on POS circuit is lost on CE-MR-10 card

On CE-MR-10 cards, the first data frame that is sent on a POS circuit is lost under the following conditions:

- For a new provisioned POS circuit
- If the data frame is large

No workaround is available for this issue. This issue will not be resolved.

CSCsq52786—Link Integrity does not work for HW-LCAS circuits

The far-end port does not go down when an AIS-P, AIS-V, or LOP alarm is injected into the HW-LCAS circuit on CE-MR-10 and CE-MR-6 cards. A TPTFAIL alarm is raised on the injected port and the port goes down. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsq55568—High traffic hit while upgrading from pre 9.00 load on CE-MR-10, CE-MR-6 cards

A high traffic hit occurs while upgrading from pre 9.00 load on CE-MR-10 and CE-MR-6 cards. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsq77755—UNEQ alarmed HW-LCAS member will go into In-Group when CTX or XC card is reset

Resetting the CTX/XC card while a HW-LCAS member has the UNEQ alarm raised causes the HW-LCAS member to go into In-Group state. This issue occurs under the following conditions:

1. Create a HW-LCAS circuit on a CE-MR-10/CE-MR-6/ML-MR-10 card.
2. Inject UNEQ on a HW-LCS member. Because of this defect, the member will be taken out-of-group.
3. Reset the CTX/XC card. HW-LCAS members with the UNEQ alarm raised will go into In-Group.

No workaround is available for this issue. This issue will be resolved in a future release.

CSCsr41260—RPR convergence time is more than expected (50 ms) in ML-100X

RPR convergence time is more than expected (50 ms) in ML-100X cards and is noticed under the following condition:

- RX fiber cut occurs on trunk of RPR-IEEE 802.17 ring.

No workaround is available for this issue. This issue will be resolved in a future release.

DWDM

This section documents caveats for DWDM in Release 8.6.

CSCso73947—E port is down after MXP-MR-10DME card power up

The E port is down for 2 minutes after an MXP-MR-10DME card is powered up under the following conditions:

- The card is connected to Fiber Channel (FC) switches on both ends.
- The switches are connected to 4G-FC ports.

The system does not report an alarm. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsu06528—GE_XP and 10GE_XP Trail Trace receive incorrect message

An incorrect “received string” message is displayed on the CTC card TTI panel continually when TTI is enabled even though the line card receives the correct string and correct alarm behavior. This issue occurs under the following conditions:

1. Set up a node with two GE_XP cards.
2. Connect card A on port 21 to card B on the same port, and card A on port 22 to card B on port 22 card.
3. Enable TTI on both trunks. The strings are received correctly.
4. Disable TTI on port 22. Port 21 reports an incorrect received string.

No workaround is available for this issue. This issue will be resolved in a future release.

CSCsx49926—Egress WRR scheduling does not work for frames > ~1500 on GE_XP card

Egress WRR scheduling does not work for frames more than approximately 1500 on GE_XP card. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsx55119—Ingress COS remarking not working for NNI ports on GE_XP card

Ingress COS remarking does not work for NNI ports on GE_XP cards. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsw49064—GR3 protection is not triggered by SD or SF alarms on trunk ports

GR3 protection is not triggered by SD/SF alarms on trunk ports under the following conditions:

1. Configure a GR3 protection on a ring of muxponder cards.
2. Generate an SF or an SD on a trunk. The protection is not triggered.

No workaround is available for this issue. This issue will be resolved in a future release.

CSCsu49109— Y-cable does not switch for client syncloss on TXP-MR-10E card

On TXP_MR_10E cards, the SYNCLOSS alarm on the client port does not cause the Y- cable switch under the following conditions:

1. Install a Y-cable with G709 on a 10GE/10GFC card.
2. Inject a SYNCLOSS alarm in the client receiving fiber on the far-end working card. The near-end protection does not perform a switch to protection.

No workaround is available for this issue. This issue will be resolved in a future release.

CSCsr60270—Upgrade issues in GE_XP/10GE_XP cards

The following issues are noticed:

- Electrical SFP

  If a copper SFP has a link flap (cable disconnect or autoneg restart) the link will come up but traffic will not flow.

- VLAN range issue

  After an upgrade, if the user tries to add or configure a new VLAN range, it does not work. Also, previously configured VLAN ranges will not work

- Selective configuration

  When there is a sequence of add and delete selective operations followed by a reset, new selective operations might not work after reset.

- Metering on port1

  If a VLAN range is configured, after an upgrade, metering on port 1 will not work anymore. Traffic will flow, but metering is not applied.

These issues occur when the software is upgraded from Release 8.0 to 8.5.

The workaround for each issue is as follows:

- Electrical SFP issue: IS>OOS>IS.
- VLAN range issue: Cold boot card.
- Selective configuration: Cold boot card.
- Metering on port1: Remove VLAN range entry, change metering parameters on port 1, and reapply metering.

This issue will be resolved in a future release.

CSCsr22181—IPG change for Copper SFP

Upgrading the software from a software release with CRC errors issue for traffic on a copper PPM does not automatically fix the issue. This issue occurs under the following conditions:

- In a release that includes a copper-card pair, most of the packets are dropped due to CRC errors (even in normal working condition)
- Upgrade the software to a new release to fix this issue for new copper PPMs.

Copper PPMs with CRC issues that were already installed before the software upgrade will again drop packets.

The workaround is to change the port state to OOS and IS. This issue will be resolved in a future release.

CSCsq99089—Traffic does not flow on the fast automatic protection switching (FAPS) circuit

Traffic does not flow on the fast automatic protection switching (FAPS) circuit when the master node is powered up after being powered down. This issue occurs under the following conditions:

1. Enable GR3/FAPS.
2. Remove the fiber from the working trunk (trunk_1). The card switches to the protected trunk (trunk_2) and traffic is up and running.
3. Power down the master node.
4. Power up the master node.
5. The master node is up and running, but traffic does not flow.

No workaround is available for this issue. This issue will be resolved in a future release.

CSCsq99680—Unwanted PM updates and alarms occur

While an LOS (or TRAIL-SIGNAL-FAIL) alarm is present, the following unwanted PM updates and alarms occur:

- FEC-PM continues increment.
- UNC-WORD alarm is raised.

This issue occurs under the following conditions:

1. Enable a 10GE-XP trunk port, configured with FEC on and G709 on.
2. The trunk port reports an LOS alarm due to a valid reason.
3. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsq78030—Continuous squelch asserts or clears are observed on MXP-MR-2.5G card

Continuous squelch asserts or clears are observed on an MXP-MR-2.5G card. This issue occurs under the following condition:

- SYNCLOSS alarm is present on the peer card.

No workaround is available for this issue. This issue will be resolved in a future release.

CSCsq78337—Unable to provision ONS-SE-G2F-LX= (10-2273-02) on a TXP-MR-2.5G card for ISC3

ONS-SE-G2F-LX= (10-2273-02) on a TXP-MR-2.5G card for ISC3 cannot be provisioned while using the Release 8.5.x software version.

The workaround for this issue is to either:

- Use 10-1832-03 --> 15454-SFP-GE+-LX= on the TXP-MR-2.5G card.
- Use 10-2273-01 --> ONS-SE-G2F-LX= on the ADM-10G card.

This issue will be resolved in a future release.

CSCsg10008—Y-cable protection switch time higher than 50 ms in GE_XP and 10GE_XP cards

Y-cable protection switch time is higher than 50 ms in GE_XP and 10GE_XP cards under the following conditions:

- RX fibers extracted from client pluggable port module (PPM).
- The Trunk pluggable port module (PPM) status is OOS,DSBLD.
- Loss of signal (LoS), both LOS-P and SIGLOSS, when extracting the RX fiber on Trunk PPM port.
- User command (for example, FORCE) is issued.

No workaround is available for this issue. This issue will be resolved in a future release.

CSCsg22669—Traffic hit greater than 50 ms but less than 60 ms on MXP-2.5G-10E in Y cable configuration with fiber cut

When a fiber is cut on MXP-2.5G-10E cards in Y-cable configurations, a traffic hit of greater than 50 ms but less than 60 ms occurs. This issue will be resolved in a future release.

CSCsf04299 —WTR time does not trigger switch back of protection

When triggering the switch of optimized 1+1 protection and the failure is cleared, the WTR condition is raised, but after the WTR time expires, the switch back of protection is not triggered. The workaround is to manually force back the protection. This issue will be resolved in a future release.

CSCse97200 —Local and Express order-wire circuits do not work on ADM-10G card

On ADM-10G cards, attempts to preprovision local and express order-wire circuits on trunk ports are not successful. E1/E2 order-wire is not supported. This issue will be resolved in a future release.

CSCsm82422—CARLOSS alarm not raised when power is turned off on MXP-MR-10DME cards

On MXP-MR-10DME cards, the CARLOSS alarm is not raised when the power is turned off on the copper SFP due to squelching of that port. No workaround is available for this issue. This issue will not be resolved.

CSCsq33614 —Hard reset of MXP-MR-10DME and MXP-2.5G-10E cards raises IMPROPRVML alarm

A hard reset on MXP-MR-10DME and MXP-2.5G-10E cards sometimes causes the improper removal alarm to be raised on some ports. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsq46283— Packet loss on MXP-MR-10DME cards provisioned with 4G or 4G FICON

Continuous packet loss is seen for 10 to 15 minutes on MXP-MR-10DME cards provisioned with 4G or 4G FICON and the port is put from IS state to OOS,MT state, and then back to IS state. The workaround is to move the port to OOS,DSBLD and then to IS. This issue will be resolved in a future release.

CSCei19148—Client momentarily enabled and emits light before squelching due to the trunk OOS,DSBLD condition

When a port is placed in IS while the conditions necessary to squelch the port are present (for example, when the trunk port on a DWDM card is OOS,DSBLD and a client port is placed in IS), 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—IfInErrors counter does not report performance parameters

When using a 1GE payload over the TXP-MR-2.5G card, the IfInErrors counter does not report oversized, undersized, or CRC errored frames. The counter reports frame coding only. This issue will not be resolved.

CSCsb47323 —Unexpected RFI condition raised with OTUk-BDI for MXP-MR-10DME-C and MXP-MR-10DME-L cards

For MXP-MR-10DME-C and MXP-MR-10DME-L cards, an unexpected RFI condition might be raised along with an OTUk-BDI. When an LOS occurs downstream, the node receives OTUk-BDI. Because of the placement of dual OTN and SONET wrappers, the node can also receive an RFI. This issue will not be resolved.

CSCsb94736—MXP-MR-10DME card fails to detect the login message after fault condition

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 situation can occur in an N-F configuration with the Cisco MDS switch and MXP-MR-10DME distance extension on, where test equipment traffic is set to 2G Fiber Channel (FC) full-bandwidth occupancy and started. The workaround is to stop traffic or keep bandwidth occupancy below 80% during the login phase. This issue will not be resolved.

CSCsc36494—Manual Y-cable switches with squelching turned off in the MXP-MR-10G card causes Fiber Channel link with Brocade switches to go down

Manual Y-cable switches with squelching turned off in the MXP-MR-10G card can cause a Fiber Channel link with Brocade switches to go down. SIGLOSS and GFP-CSF alarms are seen in CTC. Cisco recommends that squelching be on when interworking with Brocade switches. If for some reason squelching must be off with Brocade switches, Cisco recommends using a FORCE command to perform Y-cable switches. This issue may not be resolved.

CSCsc60472—CTC is not able to discover TL1 OCHCC circuit provisioned over ITU-T line card

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.

CSCee45443 —FICON bridge in the MXP-MR-2.5G card transitions to SERV MODE

The FICON bridge in the MXP-MR-2.5G card transitions to SERV MODE when the FICON bridge does not receive the expected number of idle frames between the data packets. The workaround is to not use the MXP-MR-2.5G card with the FICON bridge. This issue will not be resolved.

CSCsl70268 —Severity is not cleared when the raised alarm is cleared

When an alarm raised on a port is cleared, the severity is not cleared. The workaround is to close and then re-open CTC Functional View. This issue will be resolved in a future release.

CSCso82618— UT module does not report the wavelength error when the error is caused by a laser drift

On TXP-MR-10E-UT2 cards, the UT module does not report the wavelength error when the error is caused by a laser drift. The alarm is reported only during the tuning process if the laser does not lock to the provisioned channel. No workaround is available for this issue. The issue will be resolved in a future release.

CSCso92518—TIM alarm is not cleared on TXP-MR-10E and MXP-MR-10DME cards

On TXP-MR-10E and MXP-MR-10DME cards, configuring a SONET section trace on the trunk port when G.709 is ON causes a stuck TIM alarm. This problem does not occur on a G.709 OFF trunk port. The workaround is to use OTUk/ODUk TTI. This issue will be resolved in a future release.

CSCsq16317—GE-XP card in L1 mode reports FEC Uncorrected Word (UNC-WORD) condition

The GE-XP card in L1 mode reports the FEC Uncorrected Word (UNC-WORD) condition when G.709 is enabled and FEC is disabled on both ends of the GE-XP trunk port. The workaround is to set the FEC to standard. This issue will be resolved in a future release.

Electrical I/O Cards

This section documents caveats for Electrical I/O Cards in Release 8.6.

CSCsq98420—DS1 port state (under a DS3 port) moves to OOS,DSBLD state on deletion of first VT circuit

All DS1 ports (under a DS3 port) move to OOS,DSBLD state after the first VT circuit is deleted. This occurs under the following conditions:

1. NE equipment includes DS3XM12 card.
2. Create five VT1.5 circuits (starting from DS1 port 1 to DS1 port 5) with state set to IS and apply the circuits to the selected drop, from DS3 port 1 to DS3 port2.
3. Check that the DS3 port 1 and port 2 state is IS, and check that the first five DS1 ports of DS3 port 1 and port 2 are in IS state.
4. Change the DS3 port 1 state to OOS,MT.
5. Delete the fifth circuit.
6. During this condition, check that all DS1 ports of DS3 port 1 move to OOS,DSBLD.
7. Only the DS1 port that was used in the fifth VT circuit should be moved to OOS,DSBLD after the fifth circuit is deleted. Instead, all DS1 ports move to OOS,DSBLD.

No workaround is available for this issue. This issue will be resolved in a future release.

CSCsq13945— DS3-12 card does not boot up in release 8.0 and later

The DS3-12 card (part number 87-31-00001/800-06785-01) does not boot up in release 8.0 and later. The workaround is to use a later version of the card. This issue will not be resolved.

CSCsq48070 —Standby TCC crashes during database restore

The standby TCC crashes during a database restore in the following scenarios.

Scenario 1:

1. Backup the database on a node.
2. Add DS3XM12 or DS3XM6 cards on the node.
3. Restore the database that was backed up.

Scenario 2:

1. Create a 1:1 or 1:N protection group of Ds3XM12 cards.
2. Backup the database.
3. Delete the protection group.
4. Restore the database.

Upon doing this operation, the standby TCC that should become active may reboot. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsq58173—TCC reboots when configuring DS3XM12 or mixed 1:1 or 1:N PG

TCC Reboot when configuring DS3XM12 or mixed 1:1 or 1:N PG. This issue occurs under the following conditions:

1. Configure the DS3XM12 or mixed 1:1 or 1:N PG.
2. The ACT TCC reboots in about 2 minutes.

No workaround is available for this issue. The TCC will stabilize on its own after rebooting.

CSCsu20391—FE-AIS and RAI alarms are incorrectly reported

The far-end AIS (FE-AIS) and remote alarm indication (RAI) alarms are incorrectly reported and persist on the DS3 ports even though the FE-AIS is not present. This issue occurs under the following conditions:

1. Set up an STS-1 circuit between a DS3 port on a DS312E card and an OC-48 port.
2. Connect a test set to the DS3 port.
3. Install a fiber jumper hairpin (loopback) on the OC-48 port.
4. Set up the DS3 port for C-bit.
5. Insert FE-AIS with a test set. For example, on Agilient 718, set the alarm type to DS3 FEAC, message DS3 AIS RECEIVED.
6. FE-AIS and RAI alarms are reported on the NE against the DS3 port.
7. Disconnect the cable on the DS3 RX port to cause an LOS on the DS3 port.
8. Stop inserting FE-AIS with the test set. Wait for 15 seconds.
9. Reconnect the cable on the DS3 RX port to clear the LOS alarm.
10. Observe that the FE-AIS and RAI alarms incorrectly return after the LOS clears.

Note This issue occurs when the FE-AIS is present, a higher priority alarm is raised (for example, LOS), and then the FE-AIS is fixed before the LOS is cleared. After the LOS clears, the Cisco ONS 15454 incorrectly raises the FE-AIS and RAI again. This issue is seen on Cisco ONS 15454 SONET 7.0.5 or SDH 7.0.7 and DS3 cards.

The workaround is to re-introduce the FE-AIS and clear the alarm, or reset the DS3 card. This issue will be resolved in a future release.

CSCsu39177—After deletion of VT circuit and creation of STS-1 circuit, there is traffic loss

After deleting a VT circuit and creating an STS-1 circuit, traffic loss occurs. A stuck AIS-V alarm causes the traffic loss.

This issue occurs under the following conditions:

1. Create 28 VT circuits on any 2 ports of an XM12.
2. Inject some line level errors (LOS) on all the VTs.
3. Delete the VT circuits and create STS circuits.
4. The stuck VT AIS is seen.

The workaround is to soft reset the card. This issue will be resolved in a future release.

CSCsu47448—For DS1 FEAC, loopcode in DS3 framing FAC is inserted on odd DS1 ports

In an XM12 portless operation in CTC, injecting far-end alarm and control (FEAC) codes on the odd port is reported on the even side of the portless circuit. This issue occurs under the following conditions:

1. Create an XM12 portless port between any two OC-N cards.
2. Execute a DS1 loopcode (DS3 FEAC) on the even side of the portless port. Loopcodes are reported on the odd side.

The workaround is to send a clear DS1 loopcode (DS3 FEAC) command on the even side. This issue will be resolved in a future release.

Hardware

This section documents caveats for Hardware in Release 8.6.

CSCei36415 —Retrieving Gigabit Interface Converter (GBIC) inventory for FC_MR-4 returns nothing for CLEI code

When retrieving Gigabit Interface Converter (GBIC) inventory for the FC_MR-4, nothing is returned for the CLEI code. In a future release, enhanced inventory information will be available for ONS GBICs, including the CLEI code. This issue will be resolved in a future release.

CSCeb36749 —In a Y-cable configuration, CARLOSS alarm is major and affects service even though traffic is fine

In a Y-cable configuration, if you remove the client standby RX fiber, a nonservice-affecting LOS is raised, as expected. However, if you then remove the trunk active RX fiber, a nonservice-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.

Maintenance and Administration

This section documents caveats for Maintenance and Administration in Release 8.6.

Caution VxWorks is intended for qualified Cisco personnel only. Use of VxWorks by customers is not recommended, nor is it supported by the Cisco Technical Assistance Center. Inappropriate use of VxWorks commands can have a negative and service-affecting impact on your network. Consult the troubleshooting guide for your release and platform for appropriate troubleshooting procedures. To exit without logging in, enter a Control-D (press 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 Cisco Transport Controller (CTC) does not support adding or creating more than five circuits in auto-ranged provisioning. This restriction is intentional.

Note In releases earlier than Cisco ONS Release 4.6, you could independently set proxy server gateway settings; however, with Cisco ONS Release 4.6.x and later, 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 upon upgrading to Cisco ONS Release 7.x. Current settings are displayed in Cisco Transport Controller (whether they were inherited from an upgrade or they were set using the current GUI).

CSCse38590— Station reports "remote WTR" on a space even though the neighboring station is not advertising Wait to Restore (WTR) state

In the RPR topology, one station reports a "remote WTR" on a space, even though the neighboring station is not advertising Wait to Restore (WTR) state. This issue is observed after many XC pulls/switches, deleting and recreating circuits, and replacing cross-connects completely. This issue does not appear to have any real impact to traffic, but can potentially complicate troubleshooting. The workaround is to configure a forced-switch on both ends of the problem span, and then remove the forced-switch from both ends.

CSCsd44081—Series of crashes and reboots occur when policy-map includes approximately 200 class-map entries and policers

A series of crashes and reboots may occur when a policy-map includes approximately 200 class-map entries and policers. This error appears to occur when the card boots up, the field-programmable gate array (FPGA) process is attempting to download the new FPGA, the policy-map has at least 200 class-map entries, and traffic has been sent to the host. These conditions may trigger a provisioning-message timeout on the ML card that can lead to a crash. Because the system boots up in the same state, a continuous series of crashes and reboots may occur. The workaround is to remove the circuits and wait until the node boots up with the latest FPGA image before reconfiguring the circuits.

CSCse23518—RPR SPAN-MISMATCH alarm not reported correctly

The RPR SPAN-MISMATCH alarm is not reported correctly in some situations. After creating and deleting an East-to-East RPR circuit through TL1 cross-connects and creating a West-to-West RPR circuit through the TL1 cross-connects script, both within less than 1 second of the other, the RPR-SPAN-MISMATCH alarm is seen only on one side of the circuit and not on the other side. This problem does not occur when the operations are made manually. This alarm indicates mis-cabling or cross-connects created between two East spans or two West spans. The workaround is to ensure more than 1 second between the deletion of one circuit and creation of the another.

CSCse53133—RTRV-COND-STS does not display path alarms on BLSR protect path

RTRV-COND-STS does not display path alarms on a BLSR protect path. When the BLSR is switched onto protection and the protect paths have conditions on them, the TL1 retrieval command does not show those conditions on protection paths. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsg10963—Connections remain in OOS-AU,FLT after roll is canceled

Connections remain in OOS-AU,FLT state after roll is canceled. This issue occurs under the following conditions:

1. Create an OC48/OC192 two-fiber BLSR ring among three Cisco ONS 15454 nodes.
2. Create five STS-1 two-fiber BLSR circuits from Cisco ONS 15454 Node 1 to Cisco ONS 15454 Node 2. All connections enter IS-NR state.
3. Perform bulk roll to roll all connections from East port to West port. Roll is not complete. UNEQ-P alarms are raised for rollTo paths. Connection states change to OOS-AU,FLT.
4. Cancel roll.

UNEQ-P alarms clear and connection states remain in OOS-AU,FLT. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsg16500—ROLL-PEND condition seen for VT circuits on CTC conditions pane

The ROLL-PEND condition is seen for VT circuits on the CTC conditions pane.

1. Create a two-node OC-12 unprotected setup among two Cisco ONS 15454 nodes.
2. Create one VT circuit from Cisco ONS 15454 Node 1, OC-3 card to Cisco ONS 15454 Node 2, OC-12 card.
3. Give autobulkroll to circuit on the OC-12 span from STS-1 to STS-4.
4. Force the valid signal using ED-BULKROLL command to “true.” Bulkroll completes and no rolls are present on any of the nodes.

The ROLL-PEND condition is now visible on VT circuits in Cisco Transport Controller, TL1. No workaround is available for this issue. This issue will be resolved in a future release.

CSCse91968—AINS-to-IS transition on BLSR four-fiber Protect does not function properly

The AINS-to-IS transition on BLSR four-fiber Protect is not functioning properly. When a BLSR four-fiber ring is used, the AINS-to-IS transition is not correct when protect is active (ring switched). Sometimes the wrong protect is transitioning at the IO. If the TSC card is notified incorrectly, it becomes out of sync with the IO, and becomes stuck in AINS, even when the protect switch is released. The Cisco PCA is also being incorrectly notified of an AINS-to-IS transition. This issue will be resolved in a future release.

CSCsl76684—Delay in AIC-I card becoming active

When activating or reverting an AIC-I card, there is a delay in becoming active. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsm04659—CTC does not report TL1 circuits when the software is upgraded to Release 8.5.1 and 8.6

Cisco Transport Controller does not report TL1 circuits when the software is upgraded to Release 8.5.1 and 8.6. The workaround is to close and re-launch CTC. This issue will be resolved in a future release.

CSCsm08019— MXP-MR-10DME card carries traffic even if trunk port is in OOS,DSBLD state

The MXP-MR-10DME card carries traffic even if the trunk port is in OOS,DSBLD state. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsm14521—Inconsistency between LOCKOUT command status and switching status on Y-cable protected MXP-MR-10DME card

Inconsistency occurs between LOCKOUT command status and switching status on Y-cable protected MXP-MR-10DME cards. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsm25619 —Traffic not restored after card reset

Traffic is not restored when the near-end and far-end nodes of a Y-cable protected MXP-MR-10DME card are unplugged and replugged. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsm43960— Intermediate switch to protect occurs when TIM alarm is generated on MXPP-MR-2.5G card

An intermediate switch to protect occurs when a TIM alarm is generated on an MXPP-MR-2.5G card. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsm61886 —Less accuracy of the Link Integrity timer on CE-MR-10 card

The Link Integrity timer is less accurate on CE-MR-10 cards than on G1000-4 or CE1000-4 Ethernet cards. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsg42366—Traffic outage occurs when FPGA upgrade is done with manual switch on Y-cable

A traffic outage of 120 seconds occurs when an FPGA upgrade is done with a manual switch on the Y-cable and the client port is in out of service.

To prevent traffic outages, follow the procedure for an FPGA upgrade:

1. Configure the following:
   - Near-end (NE) node, 2 MXP-MR-10DME, Working and Protect, with the Working Active and the Protect Stand by for each protection group supported on the client ports
   - Far-end (FE) node, 2 MXP-MR-10DME, Working and Protect, with the Working Active and the Protect Stand by for each protection group supported on the client ports
   - NE Working card trunk port connected to FE Working card trunk port
   - NE Protect card trunk port connected to FE Protect card trunk port
2. Ensure traffic is running on the Working cards, for each protection group is supported by the MXP-MR-10DME cards.
3. Issue a Lockout of Protect to ensure traffic does not switch to Protect. Perform this on both NE and FE protection groups.

4. Disable client ports on the Protect cards and complete the manual FPGA upgrade. The upgrade should be hitless because traffic is accommodated on the Working facilities.
5. After the card has completed the software reset, move back the client ports to IS-NR state. Ensure no unexpected alarm or condition is present on the Protect cards.
6. Release Lockout of Protection on both ends, on every protection group. This operation does not affect traffic. Traffic is still carried on Working facilities.
7. Issue a Force to Protect on both NE and FE protection groups so that traffic switches from Working to Protect facilities. Do this on every protection group supported by these cards. The Force to Protect switching affects traffic less than 50 ms.
8. Disable client ports on the Working cards and complete the manual FPGA upgrade. The upgrade should be hitless because traffic is accommodated on the Protect facilities.
9. After the card has completed the software reset, move back the client ports to IS-NR state. Ensure no unexpected alarm/condition is present on the Working cards.
10. Release Force to Protect on both ends, on every protection group. If the protection group is revertive, this operation will revert traffic to the Working facilities. Less than 50-ms hits are expected. The operation keeps traffic on the Protect facilities if the protection group is nonrevertive and hitless.

This issue will not be resolved.

NCP

This section documents caveats for NCP in Release 8.6.

CSCdu82934—Failure of VT circuit creation

When you auto-route a VT circuit on an ONS 15454 node, a path is computed based on the availability of STSs on the nodes involved. This selection process, when combined with a lack of VT matrix (or STS-VT connections) on an auto-route selected node, can result in the failure of VT circuit creation and displays the following message,

Error Message `Unable to create connection object at node`

To correct this situation, manually route VT circuits in cases when auto-routing fails. The error message will indicate which node is at issue.

CSCsu10564—DCN-EXT: OTS PPC problem with OSPF enabled on LAN

The provisionable patchcord (PPC) link does not show up in the CTC network view and it is not possible to route circuits. This issue occurs under the following conditions:

1. Connect two nodes with optical transport section (OTS) PPC. At least one of the two nodes does not have any other service channel, that is, optical service channel (OSC), data communication channel (DCC), or generic communications channel (GCC). Both nodes have OSPF enabled on a LAN with area ID 0.0.0.0.
2. Although the PPC link is correctly configured on both nodes it is not added to the OSPF link table, which prevents the link from showing in CTC.

The workaround for this issue is as follows:

1. Disable OSPF on the LAN on the node that does not have another service channel.

2. If OSPF cannot be disabled, make sure that at least one service channel (OSC, DCC, or GCC) is provisioned on both nodes involved in the PPC connection.

This issue will be resolved in a future release.

Optical I/O Cards

This section documents caveats for Optical I/O Cards in Release 8.6.

CSCsr76682—Bit errors observed on OC192XFP after both XC cards reboots

Bit errors are observed on the OC192XFP card after both the XC-10G cross-connect cards hard reboots.

Bit errors occur under the following conditions:

1. Traffic passes through the OC192 XFP card.
2. Both the XC (cross-connect) cards are hard reset at the same time (due to power cycling of the node), or you lock out one XC card and do a hard reset of the active XC card.
3. The XC card comes up and becomes active and the traffic is up again.
4. Dribbling bit errors are seen on some of the paths passing through the OC192 XFP card.

The workaround for this issue is to side-switch the cross-connect card. This issue will be resolved in a future release.

CSCei26718 —Different alarm behavior between one-way and two-way VT/VC circuit creation on path protection

On the 15454-MRC-12 card, when a one-way VT/VC circuit on path protection over 1+1 protection is created, the alarm behavior is not the same as in two-way circuit creation. In particular, for the one-way circuit creation, UNEQ-V and PLM-V alarms are reported, and the circuit state remains OOS. This issue will not be resolved.

CSCin29274—Same static route on two interfaces fails

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.

CSCsv54817—STS-96c circuits do not work with OC192XFP cards

STS-96c circuits raise path unequipped alarms if the circuit uses an OC192XFP card as a source, destination, or trunk. This issue occurs under the following conditions:

1. Provision an STS-96c circuit with one end of the circuit on an OC192XFP card or using an OC192XFP as the trunk card.

2. The path unequipped alarm is raised on the STS-96c circuit.

No workaround is available for this issue. However, you could use a fixed-port OC-192 card to have STS-96c circuits, because those circuits work correctly on those cards.

Note CTC/TL-1 does not stop provisioning the STS-96c circuit on OC192XFP cards, even though the circuit eventually fails to carry traffic later.

This issue will be resolved in a future release.

CSCsl87931— ALS condition permanently lost when manual restart is performed

When manual restart is performed on the OPT-BST-E card, an ALS alarm is cleared and a LASER-APR alarm is raised. The OPT-BST-E card shuts down because the line cannot be restored, and the LASER-APR alarm is cleared; however, the ALS alarm is not raised. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsu50003—Traffic loss when concatenated unidirectional circuit is provisioned through 1 + 1 protected clients

Traffic loss occurs when a concatenated unidirectional circuit is provisioned through 1 + 1 protected clients under the following conditions:

1. Set up the Cisco ONS 15454 NE with two ADM-10G cards as peer group (double card).
2. Create 1+1 protection group between client ports of ADM peer group.
3. Create a unidirectional concatenated circuit (STS-3c onward) with the source as the working port of the 1 + 1 group and the destination (drop) as the client or trunk on the card where the protect port of 1 + 1 is configured. Traffic goes down if the working port (1 + 1 protection group) state is ACTIVE.
4. Create a unidirectional concatenated circuit with the source as the working port of the 1 + 1 group and destination (drop) on the card where the working port of 1 + 1 is configured. Traffic goes down if the protect port (1 + 1 protection group) state is ACTIVE.

The workaround for this issue is to manually switch to another facility in the protection group when the traffic is down.

Path Protection

This section documents caveats for Path Protection in Release 8.6.

CSCee53579— Traffic hits occur in unprotected to path protection topology upgrade in unidirectional routing

Traffic hits can occur in an unprotected to path protection topology upgrade in unidirectional routing. You can create an unprotected circuit, then upgrade the circuit to a path protection circuit using the Unprotected to Path Protection wizard. Select unidirectional routing in the wizard, and the circuit will be upgraded to a path protection circuit. However, during the conversion, traffic hits of the order of 300 ms should be expected. This issue will not be resolved.

TL1

This section documents caveats for TL1 in Release 8.6.

Note To be compatible with TL1 and DNS, all nodes must have valid names. Node names should contain alphanumeric characters or hyphens, but no special characters or spaces.

CSCsc41650 —Node reboots during DS3XM card pre-provisioning

Using a TL1 script to rapidly preprovision or delete various cards repeatedly in the same slot will reboot the TCC approximately 1 out of 10 times. Configuring a delay of about 10 seconds between preprovisioning/deletion cycles causes the node to not reboot. This issue will be resolved in a future release.

Resolved Caveats for Release 8.6

This section documents caveats resolved in Release 8.6.

Alarms

This section documents resolved caveats for Alarms in Release 8.6.

CSCsj96051—CE100 port transitions from IS,AINS to IS when CARLOSS alarm is raised

Ports on CE1000 and CE100T cards with a CARLOSS alarm will transition into IS state if the state is changed from OOS,DSBLD to IS,AINS and provisioned with zero soak-time. This issue has been resolved.

Common Control Cards

This section documents resolved caveats for Common Control Cards in Release 8.6.

CSCso58291—TCC2P card resets and goes into EQUIPMENT FAIL state

When the TCC2P card reboots during an active Direct Memory Access (DMA) transfer, the card fails to boot up and goes into an EQUIPMENT FAIL state. This issue has been resolved.

CSCsr41128—TCC card reboots when many sockets are created

The traffic from a port scanner creates many sockets, causing the TCC card to reboot. This issue has been resolved.

CTC

This section documents resolved caveats for CTC in Release 8.6.

CSCsl68680— CTC indicates AIS insert on terminal loopback as default setting

When terminal loopback is activated on the DS3 card, and loopbacks are performed on the DS3 or DS3E cards, the column for AIS on Terminal Loopback is checked for each DS3 line. Checking this line indicates AIS and will be sent in a direction away from the loopback. This issue has been resolved.

CSCsi29266— CTC displays BIC_UNKNOWN

The CTC inventory window displays BIC_UNKNOWN, when EIA BIC is not installed in either the A or B position on ONS 15454-SA or 15454-SA-HD chassis. This issue has been resolved.

CSCsk59570—CTC does not display warning message regarding unauthorized access

When a user logs in to CTC, no warning message is displayed regarding unauthorized access. This issue has been resolved.

Data I/O Cards

This section documents resolved caveats for Data I/O Cards in Release 8.6.

CSCsm21404—Packet loss with soft reset of CE-MR-6/CE-MR-10 card

The traffic is affected for 1000 milliseconds when a CE-MR-6/CE-MR-10 card is soft reset after an SW-LCAS circuit is created between the CE-MR-6/CE-MR-10 card and the CE-1000-4 card. The traffic is affected for 30 milliseconds when the CE-MR-6/CE-MR-10 card is soft reset after an SW-LCAS circuit is created between the CE-1000 card and the CE-MR-6/CE-MR-10 card. This issue has been resolved.

CSCsq14370—ifspeed query results in incorrect value for circuit size

When queried, the ifspeed parameter returns a value of 1000 for the POS port regardless of the circuit size provisioned on CE-MR-6/CE-MR-10 cards. This issue has been resolved.

CSCsl10070—Gigabit Ethernet interface with autonegotiation disabled is down after shut and no shut commands are issued

A Gigabit Ethernet interface with autonegotiation disabled remains down after **shut** and **no shut** commands are issued. This issue has been resolved.

CSCsg92555— 20% CPU utilization without any configuration on ML100X-8 card

An ML100X-8 card shows 20% CPU utilization even without any configuration on the card. This issue has been resolved.

CSCsk04872— Multiple low-order VCATs do not transition to IS when created in TL1 or CTC

In Release 8.0, when multiple members (more than 16) are added to a low-order VCAT group using TL1 scripts or CTC with the service state set to In-Service (IS), not all members report being in IS state. This issue has been resolved.

CSCsg35077—Cisco IOS crashes while processing malformed ISAKMP message

A device with a valid IPSec configuration that is running Cisco IOS software may crash during processing of an Internet Key Exchange (IKE) message. This issue has been resolved.

DWDM

This section documents resolved caveats for DWDM in Release 8.6.

CSCsm82513—Support of far-end laser control

Far-End Laser Control (FELC) is supported on copper SFP modules in the current release for GE_XP cards. This issue has been resolved.

CSCsq16653—Far-end port will be in squelched state on GE-XP card until the card is reset

In GE-XP cards, when an optical SFP is inserted instead of a copper SFP and the optical module has SYNCLOSS (not from FELC) before the port is put in OOS state, the far-end port will be in squelched state until the card is reset. This issue has been resolved.

CSCsl34189—PDI-P is not detected by ADM-10G card

If PDI-P is injected to the active path of the path protection circuit on an ADM-10G card, the path protection circuit does not switch to the protected path. The PDI-P alarm is not raised. For unprotected circuits, the alarm is not raised if PDI-P is injected. This issue has been resolved.

CSCsl50180—ADM-10G card reboots after creating 1S-2D circuits

The ADM-10G card reboots after creating 1S-2D circuits when one of the destinations has an LOS. Rebooting occurs when the circuits switch to path protection while performing port-level provisioning on any of the ports. This issue has been resolved.

CSCsm73009—HW FAIL alarm is raised when optical module is not recognized

The HW FAIL alarm is raised when the optical module connected to a card is not recognized by the TCC2 card. This issue has been resolved.

CSCso92457—4G-FC switching on MXP-MR-10DME card takes longer time

4G-FC traffic switching on an MXP-MR-10DME card in a Y-cable configuration happens after 4 to 5 minutes instead of 20 seconds. This issue has been resolved.

CSCsq65534—CRC error on TX interface

Packet loss or a CRC error occurs on the TX interface when traffic with jumbo packets or high clock discrepancy is created between the far-end RX interface and the near-end TX interface. This issue has been resolved.

CSCsu26568—Traffic loss on 1G port of the GE-XP card

Loss of traffic occurs on the 1G port of the GE-XP card when a copper PPM is swapped or replaced with a fiber PPM or vice versa. This issue has been resolved.

CSCsd80965—Traffic hit on TXP_MR_2.5G cards while upgrading the nodes from 5.0 or 6.0 to 7.xx versions

A traffic hit is observed on TXP_MR_2.5G cards while upgrading the nodes from Release 5.0 or 6.0 to Release 7.xx versions. The trunk laser shuts down after the upgrade. This issue has been resolved.

CSCsr41096—Traffic is affected on 4G-FC switching on MXP-MR-10DME

The data traffic is affected on the egress side of the MXP-MR-10DME card connected either to an MDS or Brocade switch. This problem occurs only when the MXP-MR-10DME card receives small packets (36 bytes, that is, packets with a 0-byte payload) from either the MDS or Brocade switch. No alarm is raised on CTC. This issue has been resolved.

CSCsr75681—Packet drop for high throughput on MXP-MR-10DME card

Packet drop occurs for high throughput on an MXP-MR-10DME card connected to an MDS-9513 switch with 4G-FC provisioned on port 1. This issue has been resolved.

CSCsr91742—Maximum bandwidth of data communication channel (DCC) in subshelf is less than the bandwidth in the node controller

The implementation of DCCs in a multi-shelf configuration cannot handle congestion in the TX buffer of the subshelves. This issue has been resolved.

CSCso93458—False laser bias alarm is raised in UT2 optical modules

The transponder and muxponder cards connected to the UT2 optical modules, 15454-10DME-C and 15454-10E-L1-C, raise a false laser bias alarm that exceeds the end of life (EOL) threshold. This issue has been resolved.

Electrical I/O Cards

This section documents resolved caveats for Electrical I/O Cards in Release 8.6.

CSCso16864—Admin state of all the DS1 ports inside a DS3 port change

In a DS3XM-12 or DS3XM card, the admin state of all the DS1 ports inside a DS3 port change to the state of the VT circuit that is created on one of the DS1 ports and applied to the drop ports. When the admin state of the circuit is changed and applied to the drop ports, all the DS1 ports inside the DS3 port change to the new state of the circuit. This issue has been resolved.

CSCsv86077— DS3XM-12 card fails to boot

The DS3XM-12 card with Ultra mapper version 3.0 fails to boot. This issue has been resolved.

CSCso69768 —VT circuits cannot be created on the portless ports

The 15454-DS3XM-12 card allows STS-1 circuits to be present on the odd portless ports that are reserved for VT1.5 circuits, causing the DS1 ports to remain in the IS state even after the circuits are deleted. This problem prevents VT circuits from being created on the portless ports because the DS1 ports are still in the IS state. This issue has been resolved.

CSCsk27740— Port name labels do not show up in the circuits table when 8.0 software version is used

When ONS 15454 Release 8.0 is used, port name labels do not show up in the Source and Destination fields in the circuits table. This issue occurs on 15454-DS1E1-56 and 15454-DS1-14 cards when a port name label is created for a DS1 port and a circuit is created to or from that port. This issue has been resolved.

CSCsu40049— AIS does not pass the 56-port DS-1/E1 interface card

AIS does not pass the 56-port DS-1/E1 interface card when retiming is enabled. This issue has been resolved.

CSCsk61580— DS1 loopcodes detection may not work when re-timing is enabled.

DS1 loopcodes detection may not work when re-timing is enabled on port 1 of the 56-port DS-1/E1 interface card. This issue has been resolved.

Maintenance and Administration

This section documents resolved caveats for Maintenance and Administration in Release 8.6.

⚠ **Caution** VxWorks is intended for qualified Cisco personnel only. Use of VxWorks by customers is not recommended, nor is it supported by the Cisco Technical Assistance Center. Inappropriate use of VxWorks commands can have a negative and service-affecting impact on your network. Consult the troubleshooting guide for your release and platform for appropriate troubleshooting procedures. To exit without logging in, enter a Control-D (press 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 Cisco Transport Planner (CTP) does not support adding or creating more than five circuits in auto-ranged provisioning. This restriction is intentional.

Note In releases earlier than Cisco ONS Release 4.6, you could independently set proxy server gateway settings; however, with Cisco ONS Release 4.6.x and later, 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 upon upgrading to Cisco ONS Release 7.x. Current settings are displayed in Cisco Transport Controller (whether they were inherited from an upgrade or they were set using the current GUI).

CSCsk42322—Pointer justification counter increments only for port 1 on MRC-12 card

The Pointer Justification counter increments only for port 1 on MRC-12 cards. This issue has been resolved.

CSCsr50786—Optical threshold defaults reset when software is upgraded

When a software upgrade from a release earlier than Release 8.0 to Release 9.0 is made, the optical threshold defaults of Release 9.0 are applied and all previously configured optical threshold defaults are lost. When a software upgrade from Release 8.0 and later to Release 9.0 is made, the configured optical threshold values are not overwritten. This problem occurs for ADM-10G, MXP-2.5G-10E, MXP-2.5G-10G, MXP-MR-10DME, MXP-MR-2.5G, MXPP-MR-2.5G, OTU2-XP, TXP-MR-10E, TXP-MR-10G, TXP-MR-2.5G, TXPP-MR-2.5G, 10GE-XP, and GE-XP cards. This issue has been resolved.

CSCsv14375— Shared secret key greater than 16 characters corrupts after an upgrade

A shared secret key greater than 16 characters corrupts after an upgrade from Release 7.20 to Release 8.5.2. This issue has been resolved.

CSCsv13893—Admin state change from IS-NR to OOS-AUMA fails

Changing the Admin state of an electrical port or optical port from IS-NR to OOS-AUMA fails. This issue has been resolved.

CSCsk84133— Unable to archive audit log

The user cannot perform an audit log and “The archive is up to date” message is displayed. This issue has been resolved.

NCP

This section documents resolved caveats for NCP in Release 8.6.

CSCsx37297—FTP port issue for TCP Connect Scan

Line cards do not boot up, and software downloading and database synchronization between Active and Standby TSC cards fail under the following condition:

- The FTP server task is blocked at the external FTP socket because of the execution of port scanners.

The workaround is to perform an FTP to the node. This issue has been resolved.

Optical I/O Cards

This section documents resolved caveats for Optical I/O Cards in Release 8.6.

CSCsr99947—Unable to retrieve STS PM values and thresholds on ports 2, 3, and 4

The STS PM values and thresholds on ports 2, 3, and 4 on an MRC-25G-4 card cannot be retrieved. This issue has been resolved.

CSCso85529—The OPT-AMP-C amplifier card does not start

The OPT-AMP-C amplifier card does not start when it is removed and reinserted when the line TX port is off. This issue has been resolved.

CSCsm44367—False line PM values reported on facility loopback for OC12-1 card

False line PM values are reported on OC12-1 cards with facility loopback configured. This issue has been resolved.

Path Protection

This section documents resolved caveats for Path Protection in Release 8.6.

CSCsv30593—AIS-V alarm does not clear in VT1.5 cross-connect circuits

In VT1.5 cross-connect circuits, an AIS-V alarm does not clear even though there are no defects. This issue has been resolved.

CSCsw86999 —AIS-V alarm does not clear for STS that does not have circuit created on VT1

AIS-V alarm does not clear for an STS circuit that does not have a circuit created on VT1. This issue has been resolved.

New Features and Functionality

No new software features are included in Release 8.6.

Related Documentation

This section lists release-specific and platform-specific documents.

Release-Specific Documents

- *Release Notes for the Cisco ONS 15454, Release 8.5.2*
- *Release Notes for the Cisco ONS 15454 SDH, Release 8.5.2*
- *Release Notes for the Cisco ONS 15454, Release 8.5.3*
- *Release Notes for the Cisco ONS 15454 SDH, Release 8.5.3*
- *Release Notes for the Cisco ONS 15310-MA, Release 8.5.3*
- *Release Notes for the Cisco ONS 15454 SDH, Release 8.6*
- *Release Notes for the Cisco ONS 15310-MA, Release 8.6*
- *Release Notes for the Cisco ONS 15310-CL, Release 8.6*

Platform-Specific Documents

Cisco ONS 15454 Release 8.6 is based on Cisco ONS 15454 Release 8.5.2 and Cisco ONS 15454 Release 8.5.3. Refer to the Release 8.5.2 and 8.5.3 documents for more information.

- *Cisco ONS 15454 Procedure Guide*
  Provides installation, turn up, test, and maintenance procedures
- *Cisco ONS 15454 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 Troubleshooting Guide*
  Provides a list of SONET alarms and troubleshooting procedures, general troubleshooting information, transient conditions, and error messages
- *Cisco ONS SONET TL1 Command Guide*
  Provides a comprehensive list of TL1 commands
- *Cisco ONS SONET TL1 Reference Guide*
  Provides general information, procedures, and errors for TL1
- *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*
  Provides software feature and operation information for Ethernet cards
- *Cisco ONS 15454 Software Upgrade Guide, Release 8.5.x*

Obtaining Optical Networking Information

This section contains information that is specific to optical networking products. For information that pertains to all of Cisco, refer to the Obtaining Documentation and Submitting a Service Request section.

Where to Find Safety and Warning Information

For safety and warning information, refer to the *Cisco Optical Transport Products Safety and Compliance Information* document that accompanied the product. This publication describes the international agency compliance and safety information for the Cisco ONS 15454 system. It also includes translations of the safety warnings that appear in the ONS 15454 system documentation.

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.

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.