Release Notes for Cisco ONS 15454 Release 8.5.3

OL-17923-01
November 2008

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 8.5.3, 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 8.5.3

Cisco ONS 15454 Release 8.5.3 is based on Cisco ONS 15454 Release 8.5.1 and not Cisco ONS 15454 Release 8.5.2. The Release Notes for Cisco ONS 15454 Release 8.5.3 contain closed (maintenance) issues and caveats found in Cisco ONS 15454 Release 8.5.1. 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.

Note When a Cisco ONS 15454 node is upgraded from a release earlier than Release 8.5.3 to Release 8.5.3, the MXP-MR-10DME Data Muxponder FPGA has to be upgraded as well. Follow the FPGA upgrade procedure as described in CSCsg42366—Traffic outage occurs when FPGA upgrade is done with manual switch on Y-cable, page 11.
The FPGA upgrade will impact traffic.

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

Contents

Changes to the Release Notes

This section documents supplemental information that has been added to the *Release Notes for Cisco ONS 15454 Release 8.5.3* since the production of the Cisco ONS 15454 System Software CD for Release 8.5.3.

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.

Note The use of 40WXC units is supported only in the networks running software Release 8.5.1 and later.

Alarms

This section documents caveats for Alarms in Release 8.5.3.

CSCsj26750—DS1_14 card shows Act(Green) LED, instead of Fail(RED) LED

When the card type in Cisco Transport Controller (CTC) is changed from DS1_14 to DS1_E1_56 with a 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.

CSCsj39442—TheSYNCLOSS alarm on the standby Y-cable port is reported as Minor instead of Major

The SYNCLOSS alarm on the standby Y-cable port is reported as Minor instead of Major. This issue will be resolved in a future release.

CSCsj88469—Protect port of the Y-cable protected MXP-MR-10DME cards report SYNCLOSS alarm as Minor instead of Major

The protect port of the Y-cable protected MXP-MR-10DME cards report SYNCLOSS alarm as Minor instead of Major. This issue will be resolved in a future release.

CSCsj97288—PROV-MISMATCH alarm is raised on TXP_MR_10E card

The PROV-MISMATCH alarm is raised on TXP_MR_10E cards when a port with an ONS-XC-10G-L2 pluggable port module (PPM) is provisioned for ZR reach for 10GE. This issue will be resolved in a future release.

CSCsk15712—Trunk port of the Y-cable protected TXP-MR-2.5G card raises LOS-P alarm in critical state

The trunk port of the Y-cable protected TXP-MR-2.5G card raises an LOS-P alarm when the port is in Critical state. The workaround is to change the port status to OOS,DSBLD, which causes the LOS-P alarm to downgrade from Critical state to Minor. This issue will be resolved in a future release.

CSCsl04155—Transient alarms occur when upgrading the software

Transient alarms occur under the following conditions:

- When upgrading the software from Cisco ONS Release 4.x, 5.x, 6.x, and 7.x to Cisco ONS Release 8.5, the PMI and FDI alarms are raised. These alarms disappear after all the nodes of the network are upgraded to Cisco ONS Release 8.5.
- When upgrading the software from Cisco ONS Release 8.0 to Cisco ONS Release 8.5, the PMI, FDI, and APC-CORR-SKIP alarms are raised. These alarms disappear after all the nodes of the network are upgraded to Cisco ONS Release 8.5.

This issue will be resolved in a future release.

CSCsl57383—OPWR_LFAIL and OPWR_HFAIL alarms does not correlate the downstream alarms

The OPWR_LFAIL and OPWR_HFAIL alarms do not properly correlate the downstream alarms when Multipath Optical (MPO) ribbon is connected to the ADD port is removed from the ADD circuit passing through the WXC card. This issue will be resolved in a future release.

CSCsm00488—SYNCLOSS alarm is raised on a Y-cable switch

A SYNCLOSS alarm is raised for a long time on a Y-cable switch when switching back to a working card after an WTR alarm is cleared for MXP-MR-10DME cards. This issue will be resolved in a future release.

CSCsm12542—LOS-P alarm is reported in Critical severity on a Y-cable protected MXP-MR-10DME card

An LOS-P alarm is reported in Critical severity on a Y-cable protected MXP-MR-10DME card even when it is in standby mode. This issue will be resolved in a future release.

CSCsm38947—False LO-RXPOWER alarm raised on client port of a TXP-MR-2.5G card

A false LO-RXPOWER alarm is raised on the client port of a TXP-MR-2.5G card when the card is up and operational for a long time. This issue will be resolved in a future release.

CSCsm92317—AIS alarm on the DS1 port is not suppressed

The AIS alarm on the DS1 port is not suppressed when the circuit is OOS, MT and the DS3 port is in service. This issue will be resolved in a future release.

CTC

This section documents caveats for CTC in Release 8.5.3.

CSCsk83405—Retrieval of OSPF diagnostics raises the OSPF Hello Fail alarm

Performing a retrieval of OSPF diagnostic information from the CTC network raises the OSPF Hello Fail alarm and the controller card is locked. This issue will be resolved in a future release.

CSCsm85843—CTC displays the STS circuit in ROLL_PENDING state when a bridge and roll is Performed

The Circuit tab in CTC displays the STS circuit in the ROLL_PENDING state when a Bridge and Roll is performed under the following conditions:

1. Starting a Bridge and Roll on an STS circuit that is on the only circuit bearing port on a MRC card or a fixed rate card.
2. During a manual Bridge and Roll, performing the COMPLETE step but not the FINISH step.
3. Deleting the fixed rate card or the port or PPM on the MRC card.

The Roll object still exists on the node even though the parent object is deleted and no pool for the rollFrom Path field exits in the Roll Object database. The Circuit tab in CTC will display the circuit in the ROLL_PENDING state and the Roll tab will not have an entry to finish the roll. The workaround is to complete all the steps of the ROLL process including the FINISH step. This issue will be resolved in a future release.

CSCso08712—VCAT member cannot be put in an OOS,OOG state in an open VCAT circuit

A VCAT member cannot be put in an OOS,OOG state in an open VCAT circuit. This issue will be resolved in a future release.

CSCsq14054—CTC hangs when VCAT state changes from OOS,DSBLD to IS,AINS

CTC hangs when VCAT state transitions from OOS,DSBLD to IS,AINS. The workaround is to manually set the state for individual members. This issue will be resolved in Release 9.0.

Data I/O Cards

This section documents caveats for Data I/O Cards in Release 8.5.3.

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. The workaround is to enable autonegotiation and disable it again or flap the link. This issue will be resolved in Release 9.0.

CSCsm07215—Unconfiguring the port channel causes the ML-MR-10 card to crash

Unconfiguring the port channel using the CLI command **no int port-i** *port-channel no* causes the ML-MR-10 card to crash. This issue will be resolved in a future release.

CSCsm12390—LCAS VCG alarms are raised on CE-MR-10 cards

When a member of a link capacity adjustment scheme (LCAS) virtual concatenation group (VCG) member has signal fail (SF) or signal degrade (SD) conditions, no LCAS VCG alarms are raised on CE-MR-10 cards. The LCAS VCG member continues to carry traffic. This issue will be resolved in a future release.

CSCsm27602—Changing status from IS-to-OOS to DSBLD-to-IS state causes loss in traffic

On a G1000 port, changing status from IS-to-OOS to DSBLD-to-IS state may cause loss in traffic. The workaround is to change the port state to OOS-MT and then apply a facility loopback to restore traffic. Change the port state to IS to bring up the traffic. This issue will be resolved in a future release.

CSCsm64065—Pause resolution algorithm on CE-MR-10 card for 1000BaseX ports is incorrect

The Pause resolution algorithm on the CE-MR-10 card for 1000BaseX ports is not correct. The workaround is to disable the flow control on the CE-MR-10 card if the partner interface does not support symmetric flow control. This issue will be resolved in a future release.

CSCsm80622—Not possible to provision FCS to NONE for POS ports in the GFP-mode on CE-MR-10 card

For POS ports in the GFP-mode on a CE-MR-10 card, you cannot provision FCS to NONE. For GFP POS ports, FCS is always set to 32-bits. This issue will be resolved in a future release.

CSCsm84897—Packet loss is observed on ML-MR-10 and CE-MR-10 cards at high data rates

Packet loss is seen on ML-MR-10 and CE-MR-10 cards at high data rates. This issue will be resolved in a future release.

CSCso55327—TCC switch causes unexpected high traffic outage

A TCC switch (reset) causes a traffic hit of upto 180 milliseconds for all circuits on a CE-MR/ML-MR card. No workaround is available for this issue. This issue will be resolved in Release 9.0.

CSCso84751—LCAS members remain in LCAS Rx DNU alarm state after XC soft reset

After XC soft resets on CE-MR-10 and CE-MR-6 cards, LCAS members may remain in a LCAS Rx DNU alarm state. This issue will be resolved in a future release.

CSCsu58944—Moving VT1 VCAT members delays transition from OOS,DSBLD to IS state

When all the members of a VT1/VC12 VCAT/LCAS path protection circuit are moved from OOS,DSBLD to IS state, SF/SD conditions are be raised and cleared. Due to this move, the circuit takes long time to transition to IS state. No workaround is available for this issue. This issue will not be resolved.

CSCsu30587—VT members remain idle after trunk card is pulled multiple times

VT members remain idle on pulling trunk cards multiple times. The workaround is to move the affected members to OOG state and then to IS state. This issue will be resolved in Release 9.0.

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 port recovers from this condition. This workaround causes a one time traffic hit.

This issue will be resolved in a future release.

DWDM

This section documents caveats for DWDM in Release 8.5.3.

CSCsk50250—West terminals are converted to A terminals and East terminals are converted to B terminals

When the software is upgraded from Cisco ONS Release 7.0.1 to Cisco ONS Release 8.0, the West terminals are converted to A terminals and East terminals are converted to B terminals. When the B terminal is viewed after the upgrade, the APC screen (Maintenance > DWDM > APC) for the B terminals is blank. The workaround is to refresh or reload software on side B. This issue will be resolved in a future release.

CSCsl28270—Traffic outage occurs when Squelch is enabled on copper SFPs

Traffic outage occurs when Squelch is enabled on copper small form-factor pluggable (SFP) modules. This issue will be resolved in a future release.

CSCsl32370—Alternative optical channel path is not calculated when optical mesh network with OTS PPC is provisioned

When optical mesh network with OTS PPC is provisioned on the multidegree node, the alternative optical channel path is not calculated using the side constraints within the OCHNC circuit provisioning wizard. This issue will be resolved in a future release.

CSCsm59936—Non DWDM node type cannot be configured for a shelf

Non DWDM node type cannot be configured for a shelf where OPT-AMP-C card is used. This issue has been resolved

CSCsm70709—Importing card parameters into CTC before configuring the pluggable port modules causes error

Importing card parameters into before configuring the pluggable port modules (PPMs) causes error. This issue will be resolved in a future release.

CSCsm76171—New circuits cannot be created on an OADM node

New circuits cannot be created on an OADM node with two or more AD-xC cards connected on the same side of the node. This issue will be resolved in a future release.

CSCsm82513—Support of far-end laser control

Far-End Laser Control (FELC) is supported on copper SFP in the current release for GE_XP cards.

CSCso33395—CTC displays warning message when XML file is imported from CTP

When CTC imports an XML file from Cisco TransportPlanner (CTP), it displays a warning message if the versions are different. This issue will be resolved in a future release.

CSCso73537—Traffic is affected for FICON2G

A traffic hit of more than 24 seconds is observed for FICON2G during a software reboot or upgrade of the MXP-MR-2.5G card. This issue will be resolved in a future release.

CSCsr03797—VLAN range UNI to UNI does not work

Traffic from a UNI port that has its VLAN range as a QinQ entry is not forwarded to a UNI port that has a single CVLAN QinQ entry with same SVLAN. The workaround is to configure the VLAN range on both UNI ports of the same card. This issue will be resolved in a future release.

CSCsu49932—Changing port state results in both trunk ports in blocked state

Changing the port status on the card, with GR3 protection enabled, results in both the trunk ports in blocked (OOS-DSBLD) state. The workaround is to change the sequence used to put the trunk ports to IS state. This issue will be resolved in Release 9.0.

CSCsu50337—4G-FC laser does not come up on hard reset on MXP-MR-10DME card

A 4G FC laser does not come up on hard reset when there are more than four SFPs are on an MXP-MR-10DME card. The workaround is to move the port to OOS-IS state to recover the traffic. This issue will be resolved in Release 9.1.

CSCsu58895—Multiple WTR messages on client port after hard reset of MXP-MR-10DME card

When an MXP-MR-10DME card with a bidirectional Y-cable configuration is hard reset, multiple WTR assert or clear messages are observed on the working client port after the card comes up. The workaround is to configure a revertive timer on only one side of the Y-cable protection group. This issue will be resolved in Release 9.0.

Electrical I/O Cards

This section documents caveats for Electrical I/O Cards in Release 8.5.3.

CSCsl28775—VT or STS cross-connects to ports above number 12 cannot be created on a DS3XM-12 card

VT or STS cross-connects to ports above number 12 cannot be created on a DS3XM-12 card. The workaround is to use A-Z circuit provisioning and use the DS3XM-12 card for transmux functionality. This issue has been resolved

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 will be resolved in a future release.

Hardware

This section documents caveats for Hardware in Release 8.5.3.

CSCsi64440—Traffic outage on the MRC-12, MRC-4, or DS3XM-12 cards

A traffic outage on MRC-12, MRC-4, or DS3XM-12 cards could occur under certain conditions when upgrading to Cisco ONS 15454 Release 8.0.

A software upgrade from a release earlier than Release 8.0 to Release 8.0 causes the following outages:

- Multisecond outage on the DS3XM-12 card in the Main slots 1, 3, 5, 12, 14, and16 when an XC or XCVT cross-connect cards are used.
- Complete outage on the DS3XM-12 card in the Protect slots 2, 4, 6, 13, 15, and 17 when an XC or XCVT cross-connect cards are used.
- Multisecond outage on the MRC-12 card when an XC or XCVT cross-connect cards are used.

The MRC-4 card is first introduced in Release 8.0, so the software upgrade does not apply.

A soft reset in Release 8.0 causes the following outages:

- Multisecond outage on the MRC-12 card when an XC or XCVT cross-connect cards are used.
- Multisecond outage on the MRC-4 card when an XC or XCVT cross-connect cards are used.
- Multisecond outage on the DS3XM-12 card in the Main slots 1,3,5,12,14, and 16 when the active XC or XCVT cross-connect cards is in slot 8.
- Total outage of the DS3XM-12 card in the Main slots 1,3,5,12,14, and 16 when the active XC or XCVT cross-connect cards is in slot 10. A hard reset will clear the problem, but a further soft reset will cause annother outage again.
- Multisecond outage on the DS3XM-12 card in Protect slots 2, 4, 6, 13, 15, and 17 when the active XC or XCVT cross-connect card is in slot 10.
- Total outage of the DS3XM-12 card in Protect slots 2, 4, 6, 13, 15, and 17 when the active XC or XCVT cross-connect card is in slot 8. A hard reset will clear the problem, but a further soft reset will again cause another outage.

This issue will be resolved in a future release.

CSCsk48116—Traffic on a CE-MR-10 card is dropped when a loopback is applied on any member of LCAS circuit

The traffic on a CE-MR-10 card is dropped when a loopback is applied on any member of the link capacity adjustment scheme (LCAS) circuit. Applying loopback potentially affects other members of the LCAS circuit as the differential delay threshold changes. This change in differential delay causes other members in the LCAS circuit to exceed the differential delay threshold raising the VCG-LOA alarm. The workaround is to assign OOS,OOG state for any member of LCAS circuit before applying loopback. This issue will be resolved in a future release.

CSCsl26125—40-DMX unit can lower channel TX power upon provisioning

The 40-DMX unit can lower the channel TX power upon provisioning of a new optical circuit. This problem is created by the counter-propagating light reaching the VOA module on the COM-RX port when incorrect cabling is used to connect the DWDM source with the 40-DMX unit. This additional optical power results in the VOA to increasing its attenuation and the power of the already provisioned circuits to being reduced. This issue will be resolved in a future release.

CSCsl92447—Traffic in a split fiber circuit is dropped when the trunk port is shut down

The traffic in a split fiber circuit is dropped when the trunk port is shut down either by pulling the trunk port fiber or setting the admin state as OOS-DSBLD, and performing a soft reset on ML-MR card or hard reset on CE-MR-10 or CE-MR-6 card. This issue will be resolved in a future release.

Maintenance and Administration

This section documents caveats for Maintenance and Administration in Release 8.5.3.

Caution VxWorks is intended for qualified Cisco personnel only. Use of VxWorks by customers is not recommended, nor is it supported by the Cisco's 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).

CSCsb88234—No plug-in message when a filler card is plugged in without prior provisioning

When a card is provisioned and a filler card is plugged in, a DBCHG with ENT-EQPT alarm is raised, but when a filler card is plugged in without a prior provision there is no plug-in message. Similarly, there is no message upon removal of the filler card. The workaround for TL1 is to issue an inventory call and the filler card appears. For CTC, the card is displayed and removed when the card is removed. This issue will be resolved in a future release.

CSCse85652—HTTP access allowed if enable password is not configured

The Cisco IOS HTTP server and the Cisco IOS HTTPS server allow HTTP access without any authentication under the following conditions:

- An enable password is not present in the device configuration.
- Either the Cisco IOS HTTP server or the Cisco IOS HTTPS server is enabled.
- No other authentication mechanism has been configured for access to the Cisco IOS HTTP server or Cisco IOS HTTPS server. The following workarounds apply:
  - Enabling authentication of requests to the Cisco IOS HTTP server or the Cisco IOS HTTPS server by configuring an enable password
  - Enabling authentication of requests to the Cisco IOS HTTP server or the Cisco IOS HTTPS server by configuring an authentication mechanism other than the default
  - Disabling the Cisco IOS HTTP server and/or the Cisco IOS HTTPS server functionality

This issue will be resolved in a future release.

CSCsg32263—DBCHG message is not displayed when creating and deleting a proxy firewall tunnel

When DBCHG messages are turned on by using the ALW-MSG-ALL command, no DBCHG message is returned when a proxy firewall tunnel is created and then deleted. 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 Stdby 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 Stdby 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 be resolved in a future release.

CSCsg43777—Number of rows added is inconsistent in VLAN DB profile pane

The number of rows added is inconsistent when a non integer value is entered in the Add Rows field for the VLAN DB profile pane. This issue will be resolved in a future release.

CSCsj42162—Packets are corrupted with cyclic redundancy check errors

Packets are corrupted with cyclic redundancy check (CRC) errors and traffic is lost when the source Ethernet signal is dropped and applied again on a chain of MXP-MR-10DME cards. This issue will be resolved in a future release.

CSCsj82440—40MUX COM-TX Port status is not correct

When the ANS parameter is launched with default patchcords to regulate the ports, the 40MUX COM-TX port status is not shown correctly in the WDM-ANS > Port Status panel. Resetting the timing communication and control (TCC) card displays the 40MUX COM-TX port status correctly. This issue will be resolved in a future release.

CSCsj85066—VT members' state is displayed incorrectly

When creating or adding members to a new Low Order (LO) circuit on an STS and VT index that has not previously carried LO traffic (since the TCC card was last rebooted), some of the VT members' state is not displayed correctly. This issue will be resolved in a future release.

CSCsk40571—Terminal loopback does not happen in FCMR-4 card

Terminal loopback does not happen on an FCMR-4 card. The traffic is sent to the downstream side of the circuit. This issue will be resolved in a future release.

CSCsk95390—Database becomes corrupted when a few VC circuits are rolled into the same slot

The database becomes corrupted when a few among multiple VT circuits are rolled into the same slot or STS. The rest of the VT circuits cannot be rolled into single slot or STS. This issue will be resolved in a future release.

CSCsl04148—LINE-TX and LINE-RX power values for OSC-CSM card are not retrieved

When retrieving power values on Cisco Transport Controller and TL1, the LINE-TX and LINE-RX power values related to the OSC-CSM card are not retrieved. This issue will be resolved in a future release.

CSCsl04173—Active channel count is not reported correctly

When TCC is reset on a node that has either a LOS, LOS-P, or OPWR-LFAIL alarm, active channel count is not reported correctly in CTC and TL1. This issue will be resolved in a future release.

CSCsl22077—rxTotalPkts and txTotalPkts does not increment

The rxTotalPkts and txTotalPkts does not increment when jumbo frames (packets of more than 1522 bytes) with an MTU setting of 9700 are sent through the circuit. This issue will be resolved in a future release.

CSCsl34159—Traffic on the port with a copper SFP is affected

Traffic on the port with a copper SFP is affected when another copper SFP or optical SFP is inserted in another port. This issue will be resolved in a future release.

CSCsl39888—Upgrading or downgrading the software causes errors

Upgrading or downgrading the software from Cisco ONS Release 7.0.5 to Cisco ONS Release 7.0.7 or viceversa causes errors on some of the ports or Y-cable protected MXP-MR-10DME cards loaded with all copper SFPs. This issue will be resolved in a future release.

CSCsl85419—CTC and TL1 does not report standing alarms on MS-ISC-100T cards

CTC and TL1 does not report standing alarms on MS-ISC-100T cards when the cards are interconnecting multiple shelves in a multishelf node as part of an SMTP ring. This issue will be resolved in a future release.

CSCsm02122—Traffic is affected when the software is upgraded to Cisco ONS Release 8.5.1

Traffic is affected when the software is upgraded to Cisco ONS Release 8.5.1 on an MXP-MR-10DME card with eight copper SFPs. This issue will be resolved in a future release.

CSCsm02773—LOS alarm on the OPT-BST Card LINE-RX port is not correlated in DirLess node

A LOS alarm on the OPT-BST card LINE-RX port is not correlated in the DirLess node when a Mesh-X (4/8) node is connected toa DirLess node. This issue will be resolved in a future release.

CSCsu33773—STS PM counters cannot be cleared on protect STS in BLSR switched state

STS PM counters cannot be cleared on protect STS in BLSR switched state. No workaround is available for this issue. This issue will be resolved in a future release.

CSCsu37480—Y-Cable switch does not occur on TXP-MR-10E line card with OTN disabled

A Y-cable switch does not occur for 10G-FC with OTN disabled on a TXP-MR-10E line card. No workaround is available for this issue. This issue will be resolved in Release 9.0.

CSCsu62655—Threshold crossing alert alarms are not raised on the MRC-12/4 card after the card Reboots

STS PM threshold crossing alert (TCA) alarms are not raised on the MRC-12/4 card after the card reboots. The alarms are raised only after first provisioning is done on the card after rebooting. The workaround is to perform provisioning on the MRC-12/4 card after rebooting. This issue will be resolved in a future release.

CSCsu64845—The card does not work after software is reverted from Release 8.5.3 to Release 8.0

The card does not work after the software is reverted from Release 8.5.3 to Release 8.0. The workaround is to hard reset the card or change the card mode to a different value and set again the card mode to desired value. Card provisioning is lost when the card mode is changed. This issue will be resolved in Release 9.0.

Optical I/O Cards

This section documents caveats for Optical I/O Cards in Release 8.5.3.

CSCsr76682—Bit Errors are observed on OC192-XFP card after both XC-10G cards are hard rebooted

Bit errors are observed on the OC192-XFP card after both the XC-10G cross-connect cards are hard rebooted. The workaround is to side switch the cross-connect card. This issue will be resolved in a future release.

Path Protection

This section documents caveats for Path Protection in Release 8.5.3.

CSCsl52122—Revertive path protection circuit may not switch to protected path during activation

A revertive path protection circuit may not switch to protected path during activation when the path protection selector does not detect the working path as Active even if that path has errors. This issue will be resolved in a future release.

SNMP

This section documents caveats for SNMP in Release 8.5.3.

CSCso22135—Node reboots when the snmpwalk command is executed on entPhysicalDescr, cerentEnvMonVoltage

The node may reboot when the **snmpwalk** command is executed on entPhysicalDescr, cerentEnvMonVoltage. This issue will be resolved in a future release.

TL1

This section documents caveats for TL1 in Release 8.5.3.

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.

CSCsm34460—ENT-EQPT::SLOT-14&SLOT-16:81::DS3:PROTID=SLOT-15,PRTYPE=1-N,CMDMDE=FRCD; TL1 command returns wrong response

The following TL1 command returns an incorrect response ENT-EQPT::SLOT-14&SLOT-16:81::DS3:PROTID=SLOT-15,PRTYPE=1-N,CMDMDE=FRCD;. This issue will be resolved in a future release.

CSCsu24438—RTRV-TH-MOD2 command for the optical ports does not retrieve any value

The RTRV-TH-MOD2 command for the optical ports does not retrieve any value when the MONTYPE specified in the command is "ALL" with the FEND location, and returns the error "/* Far End Performance Monitoring Values Not Supported */." The workaround is to use the following commands to retrieve the threshold values of the optical ports:

- RTRV-TH-MOD2::AID:1::,FEDN;
- RTRV-TH-ALL:::1::,FEND;
- RTRV-TH-MOD2::AID:1::<MONTYPE>,FEND;

This issue will be resolved in a future release.

Resolved Caveats for Release 8.5.3

This section documents caveats resolved in Release 8.5.3.

Common Control Cards

This section documents resolved caveats for Common Control Cards in Release 8.5.3.

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.

Cross Connect Cards

This section documents resolved caveats for Cross Connect Cards in Release 8.5.3.

CSCso92212—Low-order VT1.5/VC12/VC11 circuits are in OOS-AU,FLT state after upgrading to post-Release 8.0 Software

Some of the low-order VT1.5/VC12/VC11 circuits on CE-MR-10 card go to OOS-AU,FLT state even though the traffic on the circuit is not affected. This problem occurs when the software is upgraded to a post Release 8.0 release. This issue has been resolved.

Data I/O Cards

This section documents resolved caveats for Data I/O Cards in Release 8.5.3.

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.

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 irrespective of the circuit size provisioned on CE-MR-6/CE-MR-10 cards. This issue has been resolved.

DWDM

This section documents resolved caveats for DWDM in Release 8.5.3.

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.

CSCsm50360—Egress CRC errors in 4FC mode on MXP-MR-10DME card

Single bit error events (error rate of around 1E-12) generated by the MXP-MR-10DME card occur in the egress (TX out) direction. Errors are captured by the mediaIndStatTXFramesBadCRC counter. The errors are reported when the MXP-MR-10DME card is configured in 4GFC mode on port 1 or port 5. 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.

CSCso17376—Packet loss in MXP-MR-10DME cards connected to MDS-9513 switch

Packet loss is observed when an MXP-MR-10DME card is connected to an MDS-9513 switch under the following conditions:

- The cards have an E-E configuration with MDS-9513 switches
- The MDS switches are connected to single mode 4G-FC ports
- Distance extension is enabled on the cards

This issue has been resolved.

CSCso20394—GFP-LFD alarm is raised at high temperatures

The GFP-LFD (Generic Framing Procedure-Loss of Frame Delineation) alarm is raised at high temperatures in 15454-10DME-C line cards. This issue has been resolved.

CSCso66818—IMPROPRMVL alarm is raised on copper and optical SFPs

The IMPROPRMVL alarm is raised on some copper and optical SFPs after the MXP-MR-10DME card is hard rebooted. 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.

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 threshold. 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.

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

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.

Maintenance and Administration

This section documents resolved caveats for Maintenance and Administration in Release 8.5.3.

Caution VxWorks is intended for qualified Cisco personnel only. Use of VxWorks by customers is not recommended, nor is it supported by the Cisco's 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.

CSCso60529—snmpwalk on entPhysicalChildIndex goes into a loop

On an ONS 15454 MSTP in multishelf configuration, **snmpwalk** executed on entPhysicalChildIndex goes into a loop. 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.

CSCsu56065—Threshold critical alert for EC1 port is raised at trunk ports

The threshold critical alert (TCA) alarm for path performance monitoring on an EC1 port is reported against the optical port (source port) instead of the EC1 port. This issue has been resolved.

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

Changing Admin State of electrical port or optical port from IS-NR to OOS, DSBLD fails. This issue has been resolved.

Optical I/O Cards

This section documents resolved caveats for Optical I/O Cards in Release 8.5.3.

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

False Line PM values are reported on an OC12-1 card with facility loopback configured. This issue has been resolved.

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.

New Features and Functionality

No new software features are included in Release 8.5.3.

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15454, Release 8.5.1*
- *Release Notes for the Cisco ONS 15454 SDH, Release 8.5.3*

- *Release Notes for the Cisco ONS 15310-CL, Release 8.5.3*
- *Release Notes for the Cisco ONS 15310-MA, Release 8.5.3*
- *Cisco ONS 15454 Software Upgrade Guide, Release 8.5.x*

Platform-Specific Documents

- *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

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.