Release Notes for Cisco ONS 15454 Release 6.2

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

August 2007

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15454 SONET multiplexer. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to the "Release 6.0" version of the *Cisco ONS 15454 DWDM Installation and Operations Guide*; and the "Release 6.0" version of the *Cisco ONS 15454 Procedure Guide; Cisco ONS 15454 Reference Manual; Cisco ONS 15454 Troubleshooting Guide*; and *Cisco ONS 15454 SONET TL1 Command Guide.* For the most current version of the *Release Notes for Cisco ONS 15454 Release 6.2*, visit 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, visit the following URL:

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

Contents

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

Obtaining Documentation and Submitting a Service Request, page 33

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15454 Release 6.2* since the production of the Cisco ONS 15454 System Software CD for Release 6.2.

The following changes have been added to the release notes for Release 6.2.

Changes to New Features and Functionality

The subsection for new DWDM SFPs has been removed. These SFPs will be supported in a future release.

Caveats

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

Hardware

CSCed18803

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

CSCuk48503

Under specific conditions the non-enhanced MXPD does not pass the Telcordia GR-253/G.825 Jitter generation mask test on 10G TX Trunk port. The 2.5 G TX Client jitter generation is always within mask and does not exhibit this issue. This occurs only when, in SONET mode, there is no FEC, no G.709, and client interfaces are looped back, with non-synchronous clocking, and the jitter testbox TX connected to Trunk RX port, while the jitter testbox RX is connected to the Trunk TX port. The jitter testbox TX clock recovers from RX with an additional 5 ppm offset added. This issue will not be resolved.

CSCuk44284

An optical connector and optical attenuators inserted into the SFP may force the fiber against the shelf door when it is closed. Use the following types of optical connectors and optical attenuators when connecting to the SFP:

- **Optical connectors**: The length of the connector (starting from the ferule tip) plus the fiber boot must be 50 mm or shorter.
- **Optical Attenuators**: The following attenuator Cisco P/Ns are recommended:
  - 39-0228-XX
  - 39-0229-XX
  - 39-0230-XX

Jitter Performance with XC10G

During testing with the XC10G, jitter generation above 0.10 UI p-p related to temperature gradient testing has been observed. This effect is not expected to be seen under standard operating conditions. Changes are being investigated to improve jitter performance in a future release. DDTS numbers related to this issue include CSCdv50357, CSCdv63567, CSCdv68418, CSCdv68441, CSCdv68389, CSCdv59621, and CSCdv73402.

CSCdz49928

When using KLM type fuses with specific types of fuse and alarm panels, the PWR-REDUN alarm may not be displayed once the fuse is blown. A KLM fuse does not have a blown fuse indicator built into it. As a result, the blown fuse detection circuitry on the FAP may continue to provide voltage on its output despite a blown fuse.

Maintenance and Administration

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

Note CTC does not support adding/creating more than 5 circuits in auto-ranged provisioning. This is as designed.

Note In releases prior to 4.6 you could independently set proxy server gateway settings; however, with Release 4.6.x and forward, this is no longer the case. To retain the integrity of existing network configurations, settings made in a pre-4.6 release are not changed on an upgrade to Release 6.0.x. Current settings are displayed in CTC (whether they were inherited from an upgrade, or they were set using the current GUI).

CSCsd39125

After activation from Releases 5.x, 6.0 and 6.0.1 to Release 6.2, OSC connections to the newly activated node might no longer be in place. A node previously reachable via OSC will be isolated, and a node with LAN connectivity will be reachable, but its OSC link will be down. OSC connections are rediscovered once all the NEs are activated and running Release 6.2.

OSC connections can be preserved during the upgrade of a network in the following manner:

- For a linear configuration with a single GNE, activate the node furthest from the GNE first, repeating this rule until all nodes including the GNE are activated.
- For a ring configuration with a single GNE, activate the node half way around the ring from the GNE first, then proceed with each remaining ring section as though for a linear configuration (furthest node first).

This issue will be resolved in a future release.

CSCsd27992

Nodes that have been up and running in excess of around 410 days are vulnerable to a CTM loss of performance monitoring abilities. To recover from this situation, reboot the standby TCC card, then, that card comes up, switch TCCs and restart CTC. This issue will be resolved in a future release.

CSCsc38170

When you upgrade from Release 6.2 to 7.0 CTC displays a popup window asking if you want to delay the ML-series card portion of the upgrade. This is the ML-series Version Up feature supported in Release 6.2. This feature is not supported in Release 7.0; and so, if you select the Version Up option, you should not expect the ML-Series upgrade delay to actually occur for Release 7.0. The display of the popup window in this case is an error. This issue only occurs when upgrading from a release that supports Version Up to one that does not, and will be resolved in a future release.

CSCei67897

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

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

CSCeh84908

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

CSCsb44920

The error message ('null') is invalid when, in a failed merge operation on two portless circuits, one circuit loses its connection after the merge. You can see this if you merge two portless intranode path protected circuits, where one circuit has one source and two drops, and the other circuit has two sources and one drop. Though the two drops of the first circuit might be aligned with the two drops of the second circuit, all of them are inside one physical link (not a valid path protection topology). To recover from this situation, open a new CTC session. This will return the circuits to their status prior to the failed merge. This issue is resolved in Release 7.0.

CSCei36415

When retrieving 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. This will include the CLEI code.

CSCeh92201

When you create a bidirectional BLSR-Path ProtectionIDRI circuit using autorouting and select the PCA option for secondary spans, the circuit is created over working BLSR spans and does not use PCA spans. To enforce the use of the PCA option, provision the circuit using manual routing. This issue will be resolved in a future release.

CSCee96164

The Wait To Restore (WTR) alarm does not appear to be raised for as long as the WTR timer is set for. The WTR is raised correctly, but the alarm is hidden for the first 12 seconds due to the clear soaking time for a CLDRESTART alarm. You can see this behavior if you set up a 1+1 bidirectional revertive protection group, remove the working card, and then reinsert the card. There are no plans to change this behavior.

CSCee25136

If you create a PM schedule with the Start time for the PM report equal to 00:00 (in TL1, “0-0”), after a few minutes the PM report start time might change to 23:59 (in TL1, “23-59”). This issue will not be resolved.

CSCed23484

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

CSCds88976

When a new circuit is created around a ring (path protection or BLSR), the SD BER or SF BER alarm can be raised depending on the order in which the spans are provisioned. The alarms will eventually clear by themselves. Traffic is not affected. This issue will not be resolved.

CSCdu82934

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 VT circuit creation failing with the 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.

CSCef28522

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

CSCuk49106

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

Step 1 Reduce the insertion loss of the span just before the amplifier.

Step 2 Execute the APC procedure.

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

CSCuk52850

In a fiber cut scenario on the LINE-RX, with OSC and channels provisioned, transient LOS-P or LOS-O alarms might be raised. This issue will be resolved in Release 7.0.

CSCef05162

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

CSCef29516

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

CSCeb36749

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

CSCee82052

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

CSCdx35561

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

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

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

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

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

You can avoid waiting for the ARP entries to expire on their own by removing the SDCC links from the affected ONS 15454 nodes. This will disconnect them for the purposes of the proxy ARP service and the nodes should become directly accessible over the Ethernet. Network settings on the nodes can then be provisioned as desired, after which the SDCC can be restored.

This issue will not be resolved.

CSCdy56693

Microsoft Windows XP uses more memory than previous Microsoft operating systems, and this may result in reduced CTC performance. To avoid reduced performance, you can:

- Limit the number of nodes you log into
- Avoid or limit bulk operations
- Avoid bulk circuit deletion
- Prevent CTC's discovery of DCC connected nodes by using the login "Disable Network Discovery" feature

- Prevent CTC's discovery of circuits unless needed by using the login "Disable Circuit Management"

CSCdy62092

When a node connected via SDCC has no Ethernet LAN connectivity, display of SDCC termination alarms is delayed if the fiber connecting a DCC connected node is removed. This issue cannot be resolved.

CSCdy10030

CVs are not positively adjusted after exiting a UAS state. When a transition has been made from counting UAS, at least 10 seconds of non-SES must be counted to exit UAS. When this event occurs, Telcordia GR-253 specifies that CVs that occurred during this time be counted, but they are not. There are no plans to resolve this issue at this time.

CSCdy11012

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

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

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

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

NE Defaults

The following caveats apply for NE defaults when managing older, non-Release 4.5 nodes.

- OC12-4 allows provisioning of PJStsMon from 0 to 48. The workaround is to limit provisioning to between Off and 1 to 12 only.
- CTC displays "PJStsMon=off" in the standard provisioning pane when provisioning PJStsMon off; however, TL1 and the NE Defaults editor both display 0 for this same condition.
- If you only make changes to a single default in the NE defaults editor, you must click on another default or column before the Apply button becomes functional.

ONS 15454 Conducted Emissions Kit

If you are deploying the Cisco ONS 15454 within a European Union country that requires compliance with the EN300-386-TC requirements for Conducted Emissions, you must obtain and install the Cisco ONS 15454 Conducted Emissions kit (15454-EMEA-KIT) in order to comply with this standard.

CSCdv10824: Netscape Plugins Directory

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

"Are you sure" Prompts

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

Common Control Cards

CSCdw27380

Performing cross connect card switches repeatedly might cause a signal degrade condition on the lines or paths that can trigger switching on these lines or paths. If you must perform repeated cross connect card switches, lock out the corresponding span (path protection, BLSR, or 1+1) first. This issue will not be resolved.

Active Cross Connect (XC10G/XCVT) or TCC2/TCC2P Card Removal

You must perform a lockout in BLSR, path protection, and 1+1 before physically removing an active cross connect (XC10G/XCVT) or TCC2/TCC2P card. The following rules apply.

Active cross connect (XC10G/XCVT) cards should not generally be physically removed. If the active cross connect or TCC2/TCC2P card must be removed, you can first perform an XCVT/XC10G side switch or TCC2/TCC2P reset and then remove the card once it is in standby, or you can perform a lockout on all circuits that originate from the node whose active cross connect or active TCC2/TCC2P will be removed (performing a lockout on all spans will also accomplish the same goal). No lockout is necessary for switches initiated through CTC or through TL1.

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

Ethernet Polarity Detection

The TCC2/TCC2P does not support Ethernet polarity detection. The TCC+ and TCCI both support this feature. If your Ethernet connection has the incorrect polarity (this can only occur with cables that have the receive wire pairs flipped), the TCC+/I will work, but the TCC2/TCC2P will not. In this event, a standing condition, "LAN Connection Polarity Reverse Detected" (COND-LAN-POL-REV), will be

raised (a notification will appear on the LCD, and there will be an alarm raised). This issue will most likely be seen during an upgrade or initial node deployment. To correct the situation, ensure that your Ethernet cable has the correct mapping of the wire wrap pins. For Ethernet pin mappings, consult the user documentation.

Optical IO Cards

CSCei26718

On the 15454_MRC-12, 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 be resolved in a future release.

CSCdw66444

When an SDH signal is sent into an ONS 15454 OC-12/STM-4 (IR, 1310 LR and 1550 LR) or an OC-48/STM-16 high-speed (IR and LR) port which has been configured to support SDH, an SD-P (Signal Degrade) alarm will appear as soon as the circuit is created. This alarm will continue to exist until the circuit is deleted.

To avoid this problem, when provisioning an OC-12/STM-4 (IR, 1310 LR and 1550 LR) or an OC-48/STM-16 high-speed (IR and LR) port to support SDH, disable the signal degrade alarm at the path level (SD-P) on the port.

Also, PM data at the path level will not be reliable. You must set associated threshold values to 0 in order to avoid threshold crossing alerts (TCA) on that port. The path threshold values to set to zero are CV-P, ES-P, SES-P, and UAS-P.

These issues are the result of a hardware limitation, and there are no current plans to resolve them.

CSCdw09604

If you are using an XC10G with OC-48, you must use either OC-48AS or OC-48 cards with a revision number higher than 005D.

Electrical IO Cards

CSCei59527

When an XC switch occurs, LOF is driven to the line side. On a DS1-14 this can cause us to see long switch times that are related to hardware issues if the “Treat LOF as a Defect” flag has been set. To avoid this issue, do not set the “Treat LOF as a Defect” flag to true on DS1-14 cards. A future release will remove the “Treat LOF as a Defect” option for this card.

CSCeh43011

An LOS alarm is cleared when switching to protect when the working card is on opposite side of the shelf from the protect card (in portless configuration) in a DS3XM-12 1:N protection group. An electrical port brought into IS state on the portless only card produces an LOS alarm. If you then switch to protect, the alarm appears to clear. To avoid this issue, do not bring electrical ports into IS state on a portless only card. This issue will be resolved in Release 7.0.

CSCsb48303

The DS-1 line state of the portless ports (13, 14 and greater) does not match the corresponding DS-3 line state when a DS3XM-12 conversion circuit is provisioned with the IS drop port state.

To see this, create a 1-way DS3XM-12 conversion circuit with the drop port state set to IS. Delete the conversion circuit, leaving the IS port state. Note that the DS-1 line state will now be OOS by design. If there is no circuit, DS-1 portless port lines will be placed in OOS state.

Create the DS3XM-12 conversion circuit again as before. The DS-1 portless port lines do not transition to IS.

To recover from this issue, change the DS-3 port state to OOS_MT and then to IS. The DS-1 portless port lines will transition properly. This issue is resolved in Release 7.0.

CSCdx40300

A transient WKSWPR condition is raised upon deletion of a DS3XM 1:1 protection group. This issue will be resolved in a future release.

CSCec39567

Deleting a DS3I 1:N protection group may leave the protect card LED in a standby state. This can occur in a DS3I 1:N protection group with a LOCKON applied to the working card (ONS 15454 ANSI chassis only). Upon deleting the protection group, the LED on the protect DS3I card and the CTC display are still in the standby state. Soft reset the protect card to update the LED on the card and in CTC. An alternative workaround is to remove the LOCKON before deleting the protection group. This issue will be resolved in a future release.

Data IO Cards

SONET and SDH Card Compatibility

Tables 1, 2, and 3 list the cards that are compatible for the ONS 15454 SONET and ONS 15454 SDH platforms. All other cards are platform specific.

Table 1 SDH Data Cards that are SONET Compatible

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

Table 1 SDH Data Cards that are SONET Compatible (Continued)

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

Table 2 SONET Data Cards that are SDH Compatible

Product Name	Description
CE-100T-8	8 port 10/100FE Ethernet Module
15454-G1000-4	4 Port Gigabit Ethernet
15454-E100T-G	10/100BT, 12 circuit, compatible w/ XC, XCVT and XC10G
15454-E1000-2-G	Gigabit Ethernet, 2 circuit, GBIC - G
15454-ML100T-12	10/100 Mbps Ethernet card, 12 ports, RJ-45, L2/L3 switching, SONET/ANSI system, includes console cable
15454-ML1000-2	1000 Mbps Ethernet card, 2 SFP slots, L2/L3 switching, SONET/ANSI system

Table 3 Miscellaneous Compatible Products

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

CSCsd37600

Before configuring an SPR interface that is already part of an RPR carrying traffic, close down the POS port of the SPR interface by starting a Cisco IOS CLI session for the ML-Series card featuring the desired SPR interface and completing the following Cisco IOS configuration, beginning in global configuration mode:

Step 1 `Router(config)# interface pos 0` (Enters interface configuration mode for the POS port 0 on the Delete Node.)

Step 2 `Router(config-if)# shutdown` (Closes the interface.)

Step 3 `Router(config)# interface pos 1` (Enters interface configuration mode for the POS port 1 on the Delete Node.)

Step 4 `Router(config-if)# shutdown` (Closes the interface.)

CSCin96350

If L2 protocol tunneling is disabled on an interface when it is not a member of a bridgegroup, this can cause the CAM programming of STP MAC addresses to be incorrect. The spanning tree received on a node is not passed on to the host, and the spanning tree process might not converge due to the STP packets failing to reach the host. If this occurs, add the affected interface to a

bridgegroup and disable protocol tunneling. This issue will be resolved in Release 6.2.

CSCsb40206

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

CSCdy37198

On Cisco ONS 15454s equipped with XCVT cross-connect cards, neither the E100T-12 nor the E1000-2 cards raise an alarm or condition in CTC when Ethernet traffic is predictably lost due to the following circumstances:

Circuits exist between Ethernet cards (E100T-12 and/or E1000-2) built over Protection Channel Access (PCA) bandwidth on BLSR spans. When BLSR issues a switch, the PCA bandwidth is preempted. Since there is no longer a connection between the ends of the Ethernet circuit, traffic is lost.

Note In nodes equipped with XC10G, these Ethernet cards will raise an AIS-P condition.

This issue will not be resolved.

CSCdr94172

Multicast traffic can cause minimal packet loss on the E1000-2, E100-12, and E100-4 cards. Packet loss due to normal multicast control traffic should be less than 1%. This issue was resolved in Release 2.2.1 for broadcast, and in Release 2.2.2 for OSPF, and some multicast frames. As of Release 3.0.3, the ONS 15454 supports HSRP, CDP, IGMP, PVST, and EIGRP, along with the previously supported broadcast and OSPF.

Note If multicast is used for such applications as video distribution, significant loss of unicast and multicast traffic will result. These cards were not designed for, and therefore should not be used for, such applications.

Note If the multicast and flood traffic is very rare and low-rate, as occurs in most networks due to certain control protocols and occasional learning of new MAC addresses, the loss of unicast frames will be rare and likely unnoticeable.

Note A workaround for this issue is to use the port-mapped mode of the E-series cards.

Multicast MAC addresses used by the control protocols in Table 4 have been added to the static MAC address table to guarantee no loss of unicast traffic during normal usage of these MAC addresses.

Table 4 Protocols Added to the MAC Address Table

Protocol	Release Protocol Introduced In
Broadcast MAC (used by many protocols)	2.2.1
Open Shortest Path First (OSPF)	2.2.2
Cisco Discovery Protocol (CDP)	2.2.2
Per-VLAN Spanning Tree (PVST)	2.2.2
Enhanced Interior Gateway Routing Protocol (EIGRP)	2.2.2
Internet Group Management Protocol (IGMP)	2.2.2
Hot Standby Routing Protocol (HSRP)	3.0.3

E1000-2/E100T

Do not use the repair circuit option with provisioned stitched Ethernet circuits.This issue is under investigation.

Single-card EtherSwitch

Starting with Release 2.2.0, each E100/E1000 card can be configured as a single-card EtherSwitch configuration to allow STS-12c of bandwidth to be dropped at each card. The following scenarios for provisioning are available:

1. 12c
2. 6c, 6c
3. 6c, 3c, 3c
4. 6c, six STS-1s
5. 3c, 3c, 3c, 3c
6. 3c, 3c, six STS-1s
7. Twelve STS-1s

When configuring scenario 3, the STS-6c must be provisioned before either of the STS-3c circuits.

Multicard EtherSwitch

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

CSCds02031 and CSCsb49501 E1000-2/E100

When you drop two 3c multicard EtherSwitch circuits onto an Ethernet card and delete only the first circuit, you should not provision STS-1 circuits to the card without first deleting the remaining STS-3c circuit. If you attempt to create an STS-1 circuit after deleting the first STS-3c circuit, the STS-1 circuit will not work and no alarms will indicate this condition. Under rare conditions, this could trigger a TCC reset. To avoid a failed STS-1 circuit and other possible problems, delete the second STS-3c prior to creating any STS-1 circuit.

CSCec52443

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

CSCec52372

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

CSCec51252

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

CSCea46580

SPR input counters do not increment on a BVI with an SPR interface. This issue will not be resolved.

CSCea35971

A monitor command may disappear from the configuration after a TCC reboots. To avoid this issue, use the exec command, “terminal monitor,” instead (a minor drawback is that this command applies to all VTYs), or, alternatively, reapply the monitor command after connection is lost. This is as designed.

CSCdz49700

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

CSCdz68649

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

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

CSCdz69700

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

CSCin29274

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

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

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

ip route vrf *vrf-name*

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

CSCin32057

If no BGP session comes up when VRF is configured and all interfaces have VRF enabled ensure that at least one IP interface (without VRF) is configured and add an IP loopback interface on each node. This issue will not be resolved.

CSCdy47284

ML-100 FastEthernet MTU is not enforced. However, frames larger than 9050 bytes may be discarded and cause Rx and Tx errors. This issue will not be resolved.

CSCdz74432

Issuing a “clear IP route *” command can result in high CPU utilization, causing other processes to be delayed in their execution. To avoid this issue do not clear a large number of route table entries at once, or, if you must use the “clear IP route *” command, do not install more than 5000 EIGRP network routes.

DWDM Cards

CSCei37691

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

CSCuk57046

An unexpected Mismatch Equipment Attributes (MEA) transient alarm can occur on rapidly inserting and removing a PPM. This issue can occur with a TXP_MR_10E-L for which you preprovision an OC-192 PPM. The transient alarm is raised on the PPM. This issue is resolved in Release 7.0.

CSCeh94567

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

This can occur under the following conditions.

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

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

CSCef15415

RMON TCAs are not raised on the TXPP_MR_2.5G client port after a hardware reset. To see this issue, provision two nodes with TXPP_MR_2.5G (TXP-1 and TXP-2) as follows.

Step 1 Connect the TXP-1 DWDM-A trunk to the TXP-2 DWDM-A trunk.

Step 2 Connect the TXP-1 DWDM-B trunk to the TXP-2 DWDM-B trunk.

Step 3 Create an external fiber loopback on the TXP-1 client.

Step 4 Connect the TXP-2 client to a traffic generator.

Step 5 Provision 1G FC payload on the TXP-1 and TXP-2.

Step 6 Ensure that traffic is running smoothly.

Step 7 Provision RMON thresholds using TL1 for all TXPP_MR_2.5G ports (client and trunks).

Step 8 Apply a hardware reset to the TXPP_MR_2.5G.

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

CSCef15452

RMON TCAs are not raised when the RMON history is cleared on TXPP_MR_2.5G card. To see this issue, provision two nodes with TXPP_MR_2.5G (TXP-1 and TXP-2) as follows.

Step 1 Connect the TXP-1 DWDM-A trunk to the TXP-2 DWDM-A trunk.

Step 2 Connect the TXP-1 DWDM-B trunk to the TXP-2 DWDM-B trunk.

Step 3 Create an external fiber loopback on the TXP-1 client.

Step 4 Connect the TXP-2 client to a traffic generator.

Step 5 Provision 1G FC payload on the TXP-1 and TXP-2.

Step 6 Ensure that traffic is running smoothly.

Step 7 Provision RMON thresholds using TL1 for all TXPP_MR_2.5G ports (client and trunks).

Step 8 While the traffic is running reset the RMON history by clicking the Clear button in the CTC Payload PM pane.

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

CSCuk48503

Under very specific conditions the MXPD fails the Telcordia GR-253/G.825 Jitter generation mask test on the 10G transmit trunk port. The 2.5 G transmit client jitter generation remains within mask and does not exhibit this issue.

This only occurs when, in SONET mode, with no FEC, no G,709, and client interfaces looped back, with non-synchronous clocking, and performing the following steps.

Step 1 Connect a jitter testbox TX to Trunk RX port.

Step 2 Connect a jitter testbox RX to Trunk TX port.

The jitter testbox TX clock recovers from RX with an additional 5 ppm offset added. This issue will not be resolved.

CSCef50726

Receive client fiber removal can cause a switch from the protect to the active in a TXPP_MR_2.5G. To see this issue, perform the following steps.

Step 1 Set up two nodes with TXPP_MR_2.5G (call the nodes TXP-1 and TXP-2).

Step 2 Ensure that TXP-1 DWDM-A trunk is connected to TXP-2 DWDM-A trunk with a 100 Km span.

Step 3 Ensure that TXP-1 DWDM-B trunk is connected to TXP-2 DWDM-B trunk with a 0 Km span.

Step 4 Ensure that TXP-1 client has an external fiber loopback.

Step 5 Connect the TXP-2 client to a traffic generator.

Step 6 Provision TXP-1 and TXP-2 with FICON 1G payload.

Step 7 Ensure that traffic is running smoothly on the protected span.

Step 8 Remove the receive client fiber at the near end.

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

CSCef13304

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

Step 1 Set up two nodes with TXPP_MR_2.5G (call these nodes TXP-1 and TXP-2).

Step 2 Connect the TXP-1 DWDM-A trunk to the TXP-2 DWDM-A trunk.

Step 3 Connect the TXP-1 DWDM-B trunk to the TXP-2 DWDM-B trunk.

Step 4 Provision the TXP-1 client with an external fiber loopback.

Step 5 Connect the TXP-2 client to a traffic generator.

Step 6 Ensure that TXP-1 and TXP-2 have 1G FC payload provisioned.

Step 7 Enable ALS on TXP-1 trunk port and set it to “Manual Restart.”

Step 8 When traffic is running, remove the receive and transmit fibers on TXP1 port 1 (client). Traffic goes down and shutdown on TXP-1 port 2 (trunk) displays “No.”

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

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

Note This issue is restricted to the TXPP_MR_2.5G card.

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

CSCuk51184

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

CSCec22885

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

Step 1 Change Port 2 to OOS-MT from IS.

Step 2 Change Port 3 to OOS-MT from IS.

Step 3 Change Port 2 to facility or terminal loopback.

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

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

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

CSCed76821

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

CSCef44939

Under certain conditions you may be unable to provision an Express Order Wire (EOW) circuit using an MXP_2.5G_10G or TXP_MR_10G card trunk port. This can occurs as follows.

Step 1 Provision an MXP_2.5G_10G or TXP_MR_10G card within a node.

Step 2 Disable OTN.

Step 3 Provision DCC on both client and trunk ports.

Step 4 Go to the Network view **Provisioning > Overhead Circuits** tab.

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

CSCuk51185

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

CSCuk50144

Neither E1 nor E2 circuits are available for EOW circuits on TXP_MR_2.5 TXT in Section and Line Termination mode. This issue will be resolved in a future release.

CSCee45443

When the FICON bridge does not receive the expected number of idle frames between data packets it will transition to SERV MODE. This issue will not be resolved.

CSCec40684

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

CSCec51270

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

CSCuk42668

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

CSCuk42752

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

CSCeb49422

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

CSCeb53044

The 2G Fiber Channel (FC) payload data type in the TXP_MR_2.5G and TXPP_MR_2.5G cards does not support any 8B/10B Payload PM monitoring. This is as designed.

CSCea78210

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

CSCeb32065

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

CSCuk42588

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

CSCea81219

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

CSCeb27187

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

CSCea87290

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

CSCeb12609

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

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

CSCea68773

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

Interoperability

CSCds13769: Fujitsu FLM-150 and Nortel OC-3 Express

You cannot provision the FLM-150 and OC-3 Express in 1+1 revertive switching mode. The problem occurs when the ONS 15454 issues a user request in revertive mode to the protect channel. When the user request is cleared, the ONS 15454 issues a No Request. However, the FLM-150 and OC-3 Express issues a Do Not Revert, which causes traffic to remain on the protection channel. Based on Telcordia GR-253, section 5.3.5.5, the FLM-150 and the OC-3 Express should respond with a No Request.

Alarms

CSCei37745

When VT and STS level alarms are raised at the same time, the VT level alarm is not demoted or promoted in correlation with other VT or STS level alarms. This issue is resolved in Release 7.0.

BLSR Functionality

CSCeh90643

Before secondary node isolation in a scenario where DRI PCA traffic is provisioned on a protect channel corresponding to a working channel for active DRI protected traffic, with the secondary node of the DRI PCA configured as the primary node of the protected DRI traffic, and the primary node of the DRI PCA configured as the secondary node of the protected DRI traffic, you must perform a user service selector switch command on DRI protected traffic on the secondary node for DRI PCA traffic (primary node for DRI protected traffic). Failing to issue the switch could result in loss of DRI protected traffic during the secondary node isolation. This issue will be resolved in Release 7.0.

CSCed10127

Extra traffic is not restored when an SF-R occurs on the same span where a lockout of protect is applied at the opposite node, and where the extra traffic is sourced, destined, or travels through the node with the SF-R. to work around this, issue a lockout on each end of the span at the node where the SF-R occurs. Extra traffic should then be restored. This issue will not be resolved.

CSCea59342

DS3 PCA traffic may take up to 20 seconds to recover after a BLSR switch is cleared. This can occur with DS3 PCA traffic on two-Fiber or four-Fiber BLSR configuration with XCVT cards in the same nodes as the DS3 cards. This issue will be resolved in a future release.

CSCdw58950

You must lock out protection BLSR, 1+1, and path protected traffic to avoid long, or double traffic hits before removing an active XCVT or XC10G card. You should also make the active cross connect card standby before removing it.

CSCdv53427

In a two ring, two fiber BLSR configuration (or 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 each broken.

CSCct03919

VT1.5 and VC3/VC12 squelching is not supported in BLSR/MS-SPRing.

Database Restore on a BLSR

When restoring the database on a BLSR, follow these steps:

Step 1 To isolate the failed node, issue a force switch toward the failure node from the adjacent east and west nodes.

Step 2 If more than one node has failed, restore the database one node at a time.

Step 3 After the TCC2/TCC2P has reset and booted up, ensure that the "BLSR Multi-Node Table update completed" event has occurred for all nodes in the ring.

Step 4 Release the force switch from each node.

Path Protection Functionality

CSCee53579

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

Active Cross Connect (XC10G/XCVT) or TCC2/TCC2P Card Removal

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

Active cross connect (XC10G/XCVT) cards should not generally be physically removed. If the active cross connect or TCC2/TCC2P card must be removed, you can first perform an XCVT/XC10G side switch or TCC2/TCC2P reset and then remove the card once it is in standby, or you can perform a lockout on all circuits that originate from the node whose active cross connect card or active TCC2/TCC2P will be removed (performing a lockout on all spans will also accomplish the same goal). No lockout is necessary for switches initiated through CTC or through TL1.

Bridge and Roll

CSCei37364

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

TL1

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.

CSCdu53509

When a TL1 session to a remote node (ENE) is established via a gateway node (GNE) and you have changed the node name of the ENE via either TL1, CTC or SNMP, then you must wait for about 30 seconds to issue a TL1 command via the GNE. This delay is to permit the updates to propagate to all nodes in the network. During this transition, neither the old node name nor the new node name can be used in the TL1 session to access the ENE. This 30 second window may be reduced in a future release.

Resolved Caveats for Release 6.2

This section documents caveats resolved in Release 6.2.

Hardware

CSCsb77209

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

Maintenance and Administration

CSCsd67191

Rarely, in a large network with many host routes the Proxy ARP server might run out of ring buffer storage, resulting in a subsequent failure of the driver to receive new packets. This can lead to DCC failure and loss of all connections. This issue is resolved in Releases 6.2 and 8.

CSCsd55460

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

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

This issue is resolved in Releases 6.2 and 7.0.1.

CSCsd04867

An ONS node with OSI enabled on DCC might have its control card reboot if certain conditions are met. This reboot can occur if the MTU size is set to 512 and if the DCC link is connected to certain releases of a specific third-party network element. This reboot does not occur with other NE vendors. Use any MTU size greater than 512 to avoid this issue. This issue is resolved in Release 6.2.

CSCin96350

If L2 protocol tunneling is disabled on an interface when it is not a member of a bridgegroup, this can cause the CAM programming of STP MAC addresses to be incorrect. The spanning tree received on a node is not passed on to the host, and the spanning tree process might not converge due to the STP packets failing to reach the host. If this occurs, add the affected interface to a bridgegroup and disable protocol tunneling. This issue is resolved in Release 6.2.

CSCsc16614

When creating a RADIUS server you can only enter up to a 16 character long shared secret. The user documentation recommends using a 22 character or longer shared secret (with a maximum of 128 characters). This issue is resolved in Release 6.2.

CSCsc16604

When a node is using a RADIUS server for authentication and one or more of the users authenticated by the RADIUS server uses a password containing special characters, you might be unable to log into the node via a CTC session. To avoid this issue, ensure that users only use alphanumeric characters and the TL1-accepted special characters. This issue is resolved in Release 6.2.

CSCei10981

When a physical loopback exists on an optical trunk (Physical, facility, or terminal) Ethernet traffic in RPR might be dropped. To avoid this turn off pos interfaces before inserting a loopback. This issue is resolved in Release 6.1.

CSCej00996

CTC might display an incorrect STS number on the span circuit pane. This issue can occur for incomplete tunnels and VT circuits that are partially TL1-created and partially CTC-created, and have a source or drop on the link on which you have issued a request to retrieve the circuit using the span circuit tool. There is no known workaround except to bring the circuits back to ACTIVE. This issue is resolved in Release 6.1.

CSCsb64455

When a node is in secure mode, attempting to change the default router for the backplane to another subnet results in an xSubnetsDifferent exception being raised that prevents the default router change from taking effect. If the node is not locked in secure mode, you can revert to unsecure mode, change the subnet, then use the secure mode wizard to return the node to secure mode. If the node is locked in secure mode, contact the Cisco TAC for support. This issue is resolved in Releases 6.1, 5.0.6 and 6.0.1.

CSCsb70881

In a DWDM node the alarm correlation at node level does not work. This issue can be seen in the presence of an upstream alarm. This issue is resolved in Release 6.1.

CSCsb80734

It is not possible to create a second circuit in a metro access network. This issue is resolved in Release 6.1.

CSCsb80699

In a metro access network the amplifiers don't switch to constant gain. This issue can be seen when recreating a circuit previously deleted without re-executing ANS. Relaunching ANS manually every time avoids this issue. This issue is resolved in Release 6.1.

CSCsb90576 Mismatch Equipment Attributes Alarm on EIA

In Release 6.0.x a Mismatch Equipment Attributes (MEA) alarm is raised incorrectly against the B-Side BIC (EIA) on an ONS 15454 node using the 15454-SA-HD (high density) chassis with 1BNCB48, 1BNCB24, or 1SMBB84 EIAs installed. The 1BNCB48, 1BNCB24, and 1SMBB84 EIA panels are compatible with the 15454-SA-HD shelf assembly; however, the software in Release 6.0 fails to recognize their compatibility. The MEA alarm raised as a result of this issue is not service impacting, but does cause a standing alarm.

As a workaround to the standing alarm, you can change the BIC-MEA alarm severity by creating and using a custom alarm profile following the steps that apply for your network in the NTP-A71 Create, Download, and Assign Alarm Severity Profiles procedure of the Manage Alarms chapter in the Cisco ONS 15454 Procedure Guide, Release 6.0. This issue is resolved in Release 6.1.

Common Control and Cross Connect Cards

CSCsb77897

Rarely, if there is an intermittent PLL issue the cross connect card detection logic for PLL failures might not correctly detect the failure and might fail to cause autonomous switching. If there is a PLL failure that is not resulting in autonomous switching a manual USER switch can be initiated via CTC or TL1 to recover from this situation. This issue is resolved in Release 6.2.

CSCsc75626

At a certain temperature range a faulty VCXO can cause PPM offsets outside the specification, resulting in traffic outage. A CLK buffer failure on an XCVXL can cause backplane loss of CLK, further causing an interconnection equipment failure on the IO card. In this case the XC should switch to a more stable XC, but no such autonomous switching occurs, and this might result in a traffic outage. To recover from either of these issues you must initiate a manual switch from CTC or TL1. This issue is resolved in Release 6.2.

CSCsb80449

CTC will fail to launch for any node with a TCC2P in secure mode when EMS security is also enabled, and when launching via the backplane Ethernet

port. This issue is resolved in Release 6.1.

CSCsb86924

Using the shellLock command, remote users can clear the TCC2P Backplane security setting. Only physical access users should be able to clear the security setting. This issue is resolved in Release 6.1.

CSCsb60756

An XCVXC-10G might fail to switch with DS3XM-12 cards after a cold boot. To recover from this, either hard reset the current standby XCVXC-10G or soft reset the DS3XM-12 cards. This issue is resolved in Release 6.1.

Electrical IO Cards

CSCsc11203

DS3/EC1-48 cards might fail to declare SF/SD with BPVs in DS3 Unframed mode. This issue is resolved in Release 6.1.

CSCsc01724

DS1-14 working cards in a 1:N configuration will continuously reboot once one of the working cards enters a wait to restore (WTR) state; for example, due to a hard or soft reset. If you remove and then reseat, or soft reset a working DS1-14 card in a 1:N protection group, after that card comes up any working cards in the protection group might continuously reboot, including the original card that was removed or reset. This causes traffic loss if more than one card is rebooting at the same time, which does happen. This issue is resolved in Releases 6.1, 6.2, 7.0, and maintenance Release 6.0.1.

CSCsc10010

DS1-14 cards can have borderline or long switch times when a manual switch command is issued to switch traffic from the protect card while the working card is in WTR. The longest switch time thus far observed is 100 ms. This issue can be seen in a 1:N protection group with 4 or 5 working cards. It is less likely to occur when there are 3 or less working cards, and not expected or known to occur in a 1:1 configuration. If you avoid using the manual switch command on the active protect card when the working card is in WTR, you will not see this issue. This issue is resolved in Releases 6.0.1, 6.1, 6.2, and 7.0.

CSCsc34405

Injecting a single CRC error on a DS1-56 card when framing mode is set to ESF can result in multiple CRCs being reported. This issue is resolved in Release 6.1.

Alarms

CSCsc80841

The alarm daemon fails to scale in large networks. Alarm Summary/TID SNMP traps exhaust the DCC buffers causing packet drop in large networks. There is no workaround for this; however, a workaround for the issue of the DCC buffer becoming exhausted is to divide the network into multiple OSPF areas. This issue is resolved in Release 6.2.

TL1

CSCsb69372

Nodes that are discovered through a TL1 tunnel might become permanently grayed out when the tunnel far end NE reboots. This condition can occur when one or more TL1 tunnels are active and a tunnel far end NE reboots. To recover from this condition, restart CTC. This issue is resolved in Release 6.1.

CSCsb82157

You cannot set the Gain (EXPGAIN) value using the TL1 ED-OTS command when the node is configured as Metro Access. Use CTC to set the gain in this case. This issue is resolved in Releases 6.1 and 7.0, and in maintenance Release 6.0.1.

New Features and Functionality

This section highlights new features and functionality for Release 6.2. For detailed documentation of each of these features, consult the user documentation.

New Software Features and Functionality

Release 6.2 adds the following new software features.

E1 Timing Option for SONET Nodes

With Release 6.2 the ONS 15454 supports E1 timing, enabling you to select between SONET and SDH timing hierarchies via a user provisionable field, Timing Mode. Release 6.2 E1 timing includes the following features:

- Two E1 and 2Mhz BITS in interfaces, supporting SSM conversion from ITU-T to GR
- Two E1 and 2Mhz BITS out interfaces, supporting SSM conversion from GR to ITU-T
- SDH SSM information can be sent out on any optical port
- System timing support, as per ITU-T G.813 Option 1, for networks optimized for E1

Release 6.2 CTC, EMS, and TL1 management interfaces fully support the E1 timing features only when dual TCC2P cards are installed. For further information on the E1 timing feature, consult the online version of the release notes (this document) for Release 6.2.

RPR Shortest Path Load Balancing

RPR Shortest Path Load-balancing adds a capability for unicast packets added to the RPR. It allows these unicast packets to recognize and take the shortest path to the destination node.

RPR Keep-alive

The RPR keep-alive feature adds an enhanced mechanism to check on the health of an RPR ring configuration. RPR nodes exchange “keep-alive” (KA) messages (similar to “hello” protocol messages) between one another to help quickly identify a non-SONET/SDH related failure. The KA mechanism for RPR interfaces (called SPR) sends KAs on SPR links connecting adjacent nodes. This mechanism protects against failures undetected by the SONET/SDH layer. If a failure is detected, this protocol will then trigger the generation of both an alarm to alert you of the failure and an RPR wrap to reroute traffic around the failure. This capability enhances ONS 15454 RPR resiliency mechanisms currently in place.

Alarm Generation on CRC Errors

The CRC_ALARM is raised on Ethernet interfaces when the rate of Ethernet frames with CRC errors exceeds a defined threshold. A raised CRC_Alarm initiates an RPR wrap. For the wrap to occur, the RPR POS interface (SPR) needs to belong to an RPR, and the RPR wrap option must be configured on the RPR wrap trigger.

Gigabit Ethernet Remote Failure Indication

Remote Failure Indication (RFI) is part of the 802.3z standard and is sent in order to exchange failure information as a part of link negotiation. This feature improves communication with non-Cisco equipment and is now added to the ML-Series card.

ML-Series Card Version Up

The ML-Series card Version Up feature allows you to independently upgrade ML-Series cards as part of the overall software upgrade process. With this feature enabled, you first activate the node, initializing the upgrade of all cards that are not ML-Series cards, then in a second pass you update the ML-Series cards (by initiating a software reset). Version Up is disabled by default.

You can initiate individual upgrades for each ML-Series card at any time after the initial node activation.

Note The software upgrade is not complete until all ML-Series cards have been upgraded. Consult the user documentation for specific effects of using the Version Up feature before you perform an upgrade.

In the case of redundant ML-Series cards, individual upgrades allow time to verify the proper operation of the first card before the second card is upgraded. No ML-Series card is upgraded until you specifically reset that card.

You can perform a Version Up upgrade using CTC or CTM. The Version Up feature is only supported on the ONS 15454 and ONS 15454 SDH platforms. TL-1 does not support Version Up, and you cannot enter TL-1 commands during an upgrade in which Version Up is turned on.

ML-Series Enhancements—EoMPLS

Release 6.2 supports three important ML-Series EoMPLS enhancements (these features were introduced in Release 5.0.5):

- EoMPLS over point-to-point circuits using GFP framing
- EoMPLS using RSVP signaled MPLS Traffic Engineering Tunnels
- FCS preservation over EoMPLS tunnels

With Release 6.2 ML data card enhancements, service providers can offer customers services that make use of EoMPLS-based implementation of pseudo wires over GFP, and also MPLS Traffic Engineering Tunnels using RSVP-TE as the signaling protocol.

EoMPLS pseudo wires over point-to-point circuits using GFP framing, without RPR, are supported on data cards for creating point-to-point pseudo wire circuits across the data network. Each data card supports 24 MPLS-TE tunnels, which can be used for carrying traffic over E-LSP connections. Data cards support MPLS-TE tunnels with RSVP signaling control of the EoMPLS over GFP pseudo wires. You have the option of selecting RSVP as the control protocol during the EoMPLS creation.

Data cards also support Ethernet Frame Check Sequence (FCS) preservation across EoMPLS over GFP pseudo wires. You have the option of selecting Ethernet FCS preservation, or not. The default value for FCS preservation is “off.”

Each access port on the data card can be simultaneously provisioned for both EoMPLS (to support point-to-point connections) and QinQ (to support multipoint connections). Data cards interoperate with the Tellabs 8860 for setup of EoMPLS connections. Interoperability testing can be done prior to deployment.

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15454, Release 6.1*
- *Release Notes for the Cisco ONS 15454 SDH, Release 6.2*
- *Release Notes for the Cisco ONS 15310-CL, Release 6.2*
- *Release Notes for the Cisco ONS 15327, Release 6.2*
- *Release Notes for the Cisco ONS 15600, Release 6.2*
- *Upgrading Cisco ONS 15454 to Release 6.2*

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, and hardware replacement procedures
- *Cisco ONS SONET TL1 Command Guide*
  Provides a comprehensive list of TL1 commands

Obtaining Documentation and Submitting a Service Request

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

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

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

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