Release Notes for Cisco ONS 15454 Release 6.0

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 6.0*, visit the following URL:

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

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

http://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 68

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15454 Release 6.0* since the production of the Cisco ONS 15454 System Software CD for Release 6.0.

The following changes have been added to the release notes for Release 6.0.

Changes to Caveats

The following caveat has been added.

Mismatch Equipment Attributes Alarm on EIA, page 4

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

DDTS # CSCed18803

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

DDTS # 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 be resolved in a future release.

DDTS # 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.

DDTS # 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).

Mismatch Equipment Attributes Alarm on EIA

In Release 6.0 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 will be resolved in Release 6.1.

DDTS # 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 under investigation.

DDTS # 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.

DDTS # 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 protection 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 will be resolved in a future release.

DDTS # 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.

DDTS # CSCeh92201

When you create a bidirectional BLSR-Path Protection IDRI 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 Release 7.0.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # CSCea81001

When a fault condition exists against a circuit or port that is in the OOS-MT or OOS-AINS state (or when you are using the “Suppress Alarms” check box on the CTC Alarm Behavior pane), the alarm condition is not assigned a reference number. If you were to place the circuit or port in service at this time, in the absence of the reference number, the CTC alarm pane would display the condition with a time stamp indicating an alleged, but incorrect, time that the autonomous notification was issued. Clicking the CTC alarm “Synchronize” button at this stage will correct the alarm time stamp. There is no way to remedy the lack of reference number. This issue will be resolved in Release 6.0.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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. It is not known when or if this issue will be resolved.

DDTS # 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.

DDTS # 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.

DDTS # 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"

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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

DDTS # 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

DDTS # 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.

DDTS # 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.

DDTS # 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

DDTS # 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.

DDTS # 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.

DDTS # 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 will be resolved in a future release.

DDTS # 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.

DDTS # 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
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

Table 2 SONET Data Cards that are SDH Compatible (Continued)

Product Name	Description
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

DDTS # 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 6.1.

DDTS # 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.

DDTS # CSCeg15044

IOS does not allow telnet connections when there are simultaneous Telnet requests, even though there might be unused tty lines available. If this issue occurs, a “No Free TTYs error” message is displayed. This issue will be resolved in a future release.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # CSCed96068

If an ML-Series card running Software Release 4.6.2 or later is interoperating with an ML-Series card running Software Release 4.6.0 or 4.6.1, then the pos vcat resequence disable command must be added to the configuration of the ML-Series card running R4.6.2 or later. For documentation of this command, consult the *Ethernet Card Software Feature and Configuration Guide*.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # CSCea46580

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

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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

DDTS # 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.

DDTS # 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 will be resolved in a future release.

DDTS # 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 be resolved in a future release.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # CSCuk51185

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

DDTS # 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.

DDTS # 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 be resolved in a future release.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # 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

DDTS # 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

DDTS # 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 will be resolved in Release 7.0.

BLSR Functionality

DDTS # 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.

DDTS # 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.

DDTS # 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.

DDTS # CSCdw58950

You must lock out protection BLSR, 1+1, and path protection 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.

DDTS # 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.

DDTS # 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

DDTS # CSCee53579

Traffic hits can occur in an unprotected to path protection topology upgrade in unidirectional routing. If you create an unprotected circuit, then upgrade the unprotected circuit to a path protection circuit using Unprotected to path protection wizard, selecting unidirectional routing in the wizard, the circuit will be upgraded to a path protection 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

DDTS # 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 will be resolved in a future release.

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.

DDTS # 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 6.0

This section documents caveats resolved in Release 6.0.

Hardware

DDTS # CSCdw57215

In a configuration with OC-48 Any Slot cards and an STS-24c circuit, provisioned between G1000-4 cards with traffic going over the OC-48 span, extracting the G1000-4 card at one end of the STS-24c circuit before deleting the circuit will result in a traffic hit on all existing SONET circuits defined over that same span. This only occurs when the STS-24c is provisioned on timeslot 25.

In the Cisco ONS 15454 Procedure Guide, Release 4.1.x, refer to the "NTP-77 Delete Circuits" procedure to delete the 24c circuit before removing the card. Once you have deleted the circuit, refer to the "DLP-191 Delete a Card from CTC" task (also in the procedure guide) to delete the G1000-4 card. This issue is resolved in Release 6.0.

Maintenance and Administration

DDTS # CSCeh33824

A Maintenance user is mistakenly allowed to edit Optimized 1+1 attributes that are only meant to be editable by a Superuser. The "Edit" button will be greyed out for user who have no permission to edit, but CTC doesn't prevent a user from double-clicking on the table entry to edit the attributes. This issue is resolved in Release 6.0.

DDTS # CSCdy57891

An LOP-P alarm can be inadvertently cleared by an LOS that is raised and cleared. On OC48AS, OC192, and OC12-4 cards, when an LOP condition and an LOS condition are both present on the input, an LOS will be raised as per Telcordia GR 253 alarm hierarchy. However, upon clearing the LOS with the LOP still present, the LOP alarm, which should then be raised, is not. An AIS-P condition will be visible. This issue is resolved in Release 6.0.

DDTS # CSCdy55556

In a 1:N protection group, where a protect card is protecting a failed card and another working card, which is missing, has a lockon condition, upon removing the lockon condition from the missing working card, the protect card may switch from the card it had been protecting to carry the traffic of the missing working card that just had the lockon removed. To avoid this issue, replace the failed working card before removing the lockon. This issue is resolved in Release 6.0.

Electrical IO Cards

DDTS # CSCeh63933

With a greater than 720 foot cable attached to EC1 ports, a port will declare LOS. This issue is resolved in Release 6.0.

DDTS # CSCeg79605

When a DS3 STS1 path protection circuit that is not a "Go and Return" circuit is upgraded to BLSR via ISTU, the circuit might take a long hit in one direction. To avoid this issue use Go and Return path protection circuits when upgrading DS3 STS circuits from Unprotected to path protection. This issue is resolved in Release 6.0.

DDTS # CSCea58275

In a 1:N protection group, the DS3N card will attempt to protect a preprovisioned card (that is, when you right-click an empty card slot in the CTC node view and select the DS3 card), leaving it unavailable to protect another, actual card that is also in the protection group, should that card fail. To avoid this issue, do not include the pre-provisioned card in the protection group. Once the card is physically installed, you can edit the protection group and add the card. This issue is resolved in Release 6.0.

DDTS # CSCuk54306

The DS1 port status on the DS3XM-12 card behaves differently from that of other cards. When you modify the DS3 state, the DS1 state is generated based on the DS3 state, and on the existence of STS or VT circuits. This difference is documented in Release 6.0.

Data IO Cards

DDTS # CSCef46191

A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) might block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

All other device services will operate normally.

The detail advisory is available at:

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

This issue is resolved in Release 6.0.

DDTS # CSCeg90341

A greater than 2 second traffic hit can occur with 255 subinterfaces on DRPRI. This issue can occur when the GEC member interface is shut/fiber-pull. This issue is resolved in Release 6.0.

DDTS # CSCeg90674

Occasionally when RPR is configured over path protection and a fiber is removed there might be up to a 20 second traffic hit as a result. This issue is resolved in Release 6.0.

DDTS # CSCeg86115

When traffic is switched from one GEC member to the other GEC member in a DRPRI node, the traffic hits could be between 400 ms and 2 seconds. This issue can occur when one of the GEC member interfaces goes down. This issue is resolved in Release 6.0.

DDTS # CSCeh26707

Loss of Ethernet signal on one of the front ports takes longer than expected to be propagated to the remote port. Link integrity operates slower than expected for Ethernet failures (though it works as expected for SONET failures). To see this, any condition that causes an Ethernet loss of signal (removal of a front port Ethernet cable, for example) will invoke the Ethernet integrity function. This issue is resolved in Release 6.0.

DDTS # CSCeg30605

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

DWDM Cards

DDTS # CSCuk56032

Facility Loopback on a TXP-MR-10E trunk port can cause a traffic outage. This can occur when you have two TXP-MR-10E cards on two ETSI systems connected to each other on trunk ports, with running traffic, and a GCC is created, then a Facility (LINE) loopback is set on the Trunk port of one TXPs. Traffic goes down permanently and the following conditions are reported by the transponder where the loopback has been set:

- ODUK-OCI-PM, NR, ODUk: Open Connection Indication
- PTIM, NR, Payload Type Identifier Mismatch
- OTUK-IAE, MN, OTUk: Incoming Alignment Error

The other transponder raises following alarms:

- OTUK-LOF: OTUk Loss Of Frame
- GCC-EOC: GCC Termination Failure.

Releasing the Facility loopback restores the original situation with traffic running fine. This issue is resolved in Release 6.0.

DDTS # CSCuk56248

The Span Loss Verification feature is not available in Release 5.0.x. This can be seen when a Booster Enhanced is present in the node (BST-ENH). This issue is resolved in Release 6.0.

DDTS # CSCuk56210

If, on a TXP-MR-10E card client port, the “synch msg” option is deselected (SSM-OFF) and then reselected, the message synchronization remains OFF. This can occur when you have two TXP-MR-10E cards connected via their trunk ports, the client port is the timing source for the node, and Synch messages are ON. When Synch messages are turned off from CTC, and then ON, the SSM-OFF message remains. To recover from this issue perform a software reset of the affected card. This is non-traffic affecting. This issue is resolved in Release 6.0.

DDTS # CSCef71428

If two TXPP-MR-2.5G units are connected via trunk ports, with the Working Trunk facility set to OOS,DSBLD state, and a FORCE switch is applied on the working trunk, and then the working port is put into OOS,DSBLD state, the WKSWPR condition in the Conditions pane fails to clear. This issue is resolved in Release 6.0.

SNMP

DDTS # CSCed05502 and CSCef43911

SNMP Traps are generated for TCA when the OC3-4 port state is OOS-AINS/MT (whereas TL1 TCAs are inhibited). This issue is resolved in Release 6.0.

Alarms

DDTS # CSCed64269

The “Failed SW-Prot-Ring” alarm reports inconsistently. The alarm only sometimes appears when a Lockout of Protection is present on the BLSR and a transmit or receive fiber is pulled on the node with the Lockout. This issue is resolved in Release 6.0.

Path Protection Functionality

DDTS # CSCef70522

A TL1 created VT Path Protection circuit in which only one path uses a tunnel is discovered as partial by CTC. Traffic is unaffected. This issue is resolved in Release 6.0.

DDTS # CSCec15064

A Path Protection/SNCP circuit with a defect signal present (for example, AIS-P or AIS-V) on the protect path will produce RDI-P or RDI-V upstream of the detection point, but these signals will not be detected or indicated. This issue is resolved in Release 6.0.

Online Documentation

DDTS # CSCeg63382

When you have never previously installed the online user manuals on your workstation (PC or UNIX) and you click the Help > User Manuals menu in CTC, there is no error message instructing you to install the online manuals. You must install the online help from the software or documentation CD prior to selecting it from the menu. An error message for the case in which the help is not installed is displayed in Release 6.0.

New Features and Functionality

This section highlights new features and functionality for Release 5.0.x. For detailed documentation of each of these features, consult the user documentation.

New Hardware

XC-VXC-10G Card

Release 6.0 introduces the XC-VXC-10G card. You can upgrade to the XC-VXC-10G from XC10G cards (as described in the user documentation). Upgrading a system to XC-VXC-10G from an earlier cross-connect module type is performed in-service, with hitless operation (less than 50-ms impact to any traffic). The XC-VXC-10G card is deployed in Slots 8 and 10 (only redundant operation is supported).

The XC-VXC-10G card establishes connections at the STS and VT levels. The XC-VXC-10G provides STS-192 capacity to Slots 5, 6, 12, and 13, and STS-48 capacity to Slots 1 to 4 and 14 to 17. STS cross-connections are nonblocking, so any STS-1 on any port can be connected to any other port.

XC-VXC-10G Functionality

The XC-VXC-10G card manages up to 1152 bidirectional STS-1 ports and 2688 bidirectional VT1.5 ports. The TCC2/TCC2P card assigns bandwidth to each slot on a per STS-1 or per VT1.5 basis. The switch matrices are fully crosspoint and broadcast supporting.

The XC-VXC-10G card provides:

- 1152 STS bidirectional ports
- 576 STS bidirectional cross-connects
- 2688 VT1.5 ports via 96 logical STS ports
- 1344 VT1.5 bidirectional cross-connects
- Nonblocking at the STS level
- VT1.5, STS-1/3c/6c/12c/48c/192c cross-connects

The XC-VXC-10G supports errorless side switches (switching from one XC-VXC-10G on one side of the shelf to the other XC-VXC-10G on the other side of the shelf) when the switch is initiated through software and the shelf is equipped with TCC2/TCC2P cards.

VT Mapping

The VT structure is designed to transport and switch payloads below the DS-3 rate. The ONS 15454 performs VT mapping according to Telcordia GR-253-CORE standards.

XC-VXC-10G Hosting DS3XM-6 or DS3XM-12

A DS3XM card can demultiplex (map down to a lower rate) M13-mapped DS-3 signals into 28 DS-1s that are then mapped to VT1.5 payloads. The VT1.5s can then be cross-connected by the XC-VXC-10G card. The XC-VXC-10G card can host a maximum of 1344 bidirectional VT1.5s.

XC-VXC-10G Compatibility

The XC-VXC-10G card supports the same features as the XC10G card. Either the XC10G or XC-VXC-10G card is required for OC-192, OC3-8, and OC12-4 operation and OC-48 AS operation.

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

Cross-connect and provisioning information is established through the user interface on the TCC2/TCC2P card. In turn, the TCC2/TCC2P card establishes the proper internal cross-connect information and relays the setup information to the XC-VXC-10G card so that the proper cross-connection is established within the system.

15454_MRC-12 Multirate Card

Release 6.0 introduces the 15454_MRC-12 multirate card. You can upgrade to a 15454_MRC-12 card from the one port OC12/STM-4 or OC48/STM-16 card. The 15454_MRC-12 card provides up to twelve OC-3/STM-1 ports, twelve OC-12/STM-4 ports, or four OC-48/STM-16 ports using Small Form-factor Pluggables (SFPs), in any combination of line rates. All ports are Telcordia GR-253 compliant. The SFP optics can use SR, IR, LR, coarse wavelength division multiplexing (CWDM), and DWDM SFPs to support unrepeated spans. Refer to the user documentation for more information about SFPs.

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

The 15454_MRC-12 port contains a transmit and receive connector (labeled) on the card faceplate. The card supports 1+1 unidirectional and bidirectional facility protection. It also supports 1+1 protection in four-fiber BLSR applications where both span switching and ring switching might occur. You can provision this card as part of a BLSR, path protection, or 1+1 linear configuration.

Slot Compatibility

You can install 15454_MRC-12 cards in Slots 1 through 6 and 12 through 17 with an XCVT, XC10G, or XC-VXC-10G.

The maximum bandwidth of the 15454_MRC-12 card is determined by the cross-connect card and slot position of the 15454_MRC-12 card. The maximum bandwidth differs for cards in a drop slot (Slots 1–4 or 14–17) and those in a trunk slot (Slots 5–6 or 12–13). Consult the user documentation for specific bandwidths available per slot cross connect card.

For ports and line rates refer to the user documentation.

Errorless Switching

The 15454_MRC-12 card supports an errorless software-initiated cross-connect card switch when used in a shelf equipped with XC-VXC-10G and TCC2/TCC2P cards.

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

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

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

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

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

Slot Compatibility

OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach card is used only in Slots 5, 6, 12, and 13, and only with 10-Gbps cross-connect cards, such as the XC10G and XC-VXC-10G.

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

Errorless Switching

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

DS1/E1-56 Card

Release 6.0 introduces the ONS 15454 DS1/E1-56 card. The ONS 15454 DS1/E1-56 card provides 56 Telcordia-compliant, GR-499 DS-1 ports per card, or 56 E1 ports per card. Each port operates at 1.544 Mbps (DS-1) or 2.048 Mbps (E1). The DS1/E1-56 card operates as a working or protect card in 1:N protection schemes, where N <= 2. For SONET applications, the DS1/E1-56 card requires a high-density (HD) shelf (15454-SA-HD), UBIC EIA, and Software Release 6.0 or greater.

Note The UBIC-H EIA supports the termination of both DS-1 and E-1 signals when used with the appropriate cables. The UBIC-V EIA only supports the termination of DS-1 signals.

The DS1/E1-56 card can be used with the XCVT, XC10G, or XC-VXC-10G cross-connect cards. For ONS 15454 DS1/E1-56 card slots, connectors, card level indicators, port level indicators, and operational constraints, see the user documentation.

Errorless Switching

The DS1/E1-56 card supports an errorless software-initiated cross-connect card switch when used in a shelf equipped with XC-VXC-10G and TCC2/TCC2P cards.

ML100X-8 Card

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

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

The card features two virtual packet over SONET (POS) ports with a maximum combined bandwidth of STS-48. The ports function in a manner similar to OC-N card ports, and each port carries an STS circuit with a size of STS-1, STS-3c, STS-6c, STS-9c, STS-12c, or STS-24c.

The ML-Series POS ports supports virtual concatenation (VCAT) of SONET circuits and a software link capacity adjustment scheme (SW-LCAS). The ML-Series cards support a maximum of two VCAT groups with each group corresponding to one of the POS ports. Each VCAT group must be provisioned with two circuit members. An ML-Series card supports STS-1c-2v, STS-3c-2v and STS-12c-2v.

Cross-Connect and Slot Compatibility

The ML100X-8 card works in Slots 1 to 6 or 12 to 17 with the XC10G or XC-VXC-10G cross-connect cards. It works only in high-speed slots only (Slots 5, 6, 12, or 13) with the XC or XCVT cross-connect card.

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

Small Form-Factor Pluggables

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

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

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

New Software Features and Functionality

XC-VXC-10G Errorless Side Switching

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

XC-VXC-10G Errorless Switch Types

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

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

XC-VXC-10G Errorless Configuration

High Order and Low Order traffic is Errorless on the ONS 15454 ANSI platform.

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

- The 15454_MRC-12 card
- The DS1/E1-56 card
- The OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach cards
- The ONS 15454 DS3/EC1-48 card

Note Only Version number 800-24445-02 (and higher) of the DS3/EC1-48 card supports errorless side switches. Hitless side switches are supported for Version number 800-24445-01 of the DS3/EC1-48 card in the specified configuration.

DS3/EC1-48 Card EC1 Functionality

Release 6.0 introduces EC1 functionality for the ONS 15454 DS3/EC1-48 card. The ONS 15454 DS3/EC1-48 card provides 48 Telcordia-compliant, GR-499 DS-3 ports per card. Each port operates at 44.736 Mbps over a single 75-ohm 728A or equivalent coaxial span. Ports can be individually configured for DS3 or EC1 mode. The DS3/EC1-48 card operates as a working or protect card in 1:N protection schemes, where N <= 2. Features offered with the addition of EC1 functionality include:

- Improved DS3/EC1 density for ONS 15454 MSPP to 48 ports per card (documented restrictions apply)
- DS3 Mode 1:N protection (N <= 2), up to 192 ports per shelf
- EC1 Mode 1:N protection (N <= 2), up to 192 ports per shelf
- Errorless XC support

Note Only Version number 800-24445-02 (and higher) of the DS3/EC1-48 card supports errorless side switches. Hitless side switches are supported for Version number 800-24445-01 of the DS3/EC1-48 card in the specified configuration.

- Intermediate path performance monitoring (IPPM)
- Increased B1 error checking on the back plane
- EC1 low density to DS3-EC1-48 high density protection switching support for upgrades
- J0 section trace support for EC1 mode with new TIM-S (Trace Identifier Mismatch – Section) alarm
- Configurable AIS/RDI generation for TIM-S and TIM-P defects
- Configurable AIS generation on facility and terminal loopbacks

Upgrade Low-Density DS1 Cards to High-Density DS1 Cards

As of Release 6.0, with the introduction of the DS1/E1-56 card, you can upgrade low-density DS1-14 or DS1N-14 electrical cards in a 1:N protection scheme (where N = 1 or 2) to high-density DS1/E1-56 electrical cards. Low density to high density upgrades, rules, and restrictions are outlined in the user documentation.

FC_MR-4 Enhanced Card Mode Differential Delay

Release 6.0 features FC_MR-4 differential delay support for VCAT circuits in enhanced card mode.

Differential Delay Features

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

With VCAT, SONET paths are grouped to aggregate bandwidth to form VCGs. Because each VCG member can follow a unique physical route through a network, there are differences in propagation delay, and possibly processing delays between members. The overall VCG propagation delay corresponds to that of the slowest member. The VCAT differential delay is the relative arrival time measurement between members of a VCG. The FC_MR-4 card supports VCAT differential delay with the following associated features.

- A maximum of 122 ms of delay difference between the shortest and longest paths
- Diverse fiber routing for VCAT circuits
- All protection schemes (path protection, automatic protection switching [APS], 2-fiber BLSR, 4-fiber BLSR)
- Routing of VCAT group members through different nodes in the SONET network
- Differential delay compensation automatically enabled on VCAT circuits that are diverse (split fiber) routed, and disabled on VCAT circuits that are common fiber routed

For further information on FC_MR-4 differential delay, consult the user documentation.

Detectable Filler Card

As of Release 6.0, filler cards are detectable in CTC node view when installed in the ONS 15454 shelf. The filler card is designed to occupy empty I/O and AIC slots in the Cisco ONS 15454 (Slots 1 - 6, 9, and 12 - 17). The filler card cannot operate in the XC slots (Slots 8 and 10) or TCC slots (7 and 11). When installed, the filler card aids in maintaining proper air flow and electromagnetic interference (EMI) requirements.

Bridge and Roll

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

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

CTC Rolls Window

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

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

- Roll From Circuit
- Roll To Circuit
- Roll State
- Roll Valid Signal
- Roll Mode (automatic or manual)
- Roll Path
- Roll From Circuit
- Roll From Path
- Roll To Path
- Complete
- Force Valid Signal
- Finish
- Cancel
- Types of Rolls

TL1 Bulk Roll

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

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

DLT-BULKROLL-<OCN_TYPE>

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

ED-BULKROLL-<OCN_TYPE>

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

ENT-BULKROLL-<OCN_TYPE>

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

RTRV-BULKROLL-<OCN_TYPE>

This command retrieves roll data parameters.

Single and Dual Rolls

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

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

For dual roll constraints, consult the user documentation.

Protected Circuits

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

Enhanced Security Features

Security Policy Enhancements

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

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

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

Secure Shell Encryption and Node Access Security

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

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

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

RADIUS Security

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

RADIUS Authentication

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

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

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

An ONS node operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and returning all configuration information necessary for the client to deliver service to the user. RADIUS servers can act as proxy clients to other kinds of authentication servers. Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. User passwords are sent encrypted between the client and RADIUS server. This eliminates the possibility that someone illicitly monitoring an unsecured network might detect a user's password.

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

RADIUS Session Time Limits

Release 6.0 RADIUS supports RADIUS session time limits. This feature applies only when a RADIUS server is used for authentication. When RADIUS indicates that a session is to have a time limit, that session is terminated immediately after the time expires. There is no local database support for session time limits. Rather, when EMS users are forcibly logged out by the RADIUS server, they are presented

with a notification dialog box indicating that they have been forcibly logged out due to session time expiration. Similarly, when a TL1 user is logged out, an autonomous REPT_EVT_SESSION is sent. After a TL1 user is logged out, the next command the user enters receives a DENY response with a reason code of PLNA (Login Not Active).

AAA Server Enable/Disable

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

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

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

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

Audit Trail Enhancements

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

- Archival of the audit trail in TL1, with a supporting archival failure transient alarm, AUD-ARCHIVE-FAIL
- Audit trail initiation support for IOS-based data cards in the L2/L3 mode (available over the Syslog/IOS CLI)
- Tracking of all Release 6.0 supported failed login types (incorrect password, disabled account, locked account, single login per user per node denial)
- Shell session login, logout, and activity trail
- Tracking of FTP/sftp logins and logouts
- Sustained audit trail for all logins and logouts whether or not an AAA server is used for user authentication
- Tracking of all user attempts to log in to the node
- When a login is denied, the audit trail records the reason (type of login failure)

CTC Enhanced Security Support

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

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

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

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

Active Logins

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

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

- TL1
- EMS
- FTP
- sftp
- telnet shell sessions (via serial port only; not the debug port)
- SSH shell sessions

Policy

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

- Idle User Timeout—Sets the hours and minutes a user can remain idly logged in before a timeout will occur; settings are provided for each user level.

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

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

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

Node Access

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

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

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

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

- Other—(Same as in previous releases.) Sets the PM clearing privilege as Provisioning or Superuser.

RADIUS

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

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

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

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

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

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

IOS Security Enhancements

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

Security features configured with Cisco IOS include:

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

Security features configured with CTC or TL1 include:

- Disabled console port
- AAA/RADIUS relay mode

Disabling the Console Port on the ML-Series Card

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

You can disable console port access through CTC or TL1.

Secure Login on the ML-Series Card

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

Secure Shell on the ML-Series Card

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

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

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

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

RADIUS on the ML-Series Card

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

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

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

IP and OSI on DCC

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

Release 6.0 uses PPP, a Layer 2 encapsulation protocol, with high-level data link control (HDLC) datagram encapsulation to transport IP and OSI data, and link control protocol (LCP) to establish, configure, and test the point-to-point connections. CTC automatically enables IP over PPP whenever you

create an SDCC or LDCC. The SDCC or LDCC can also be provisioned to support OSI over PPP. Link access protocol on the D channel (LAP-D), a data link protocol used in the OSI protocol stack, provides provisionable parameters when you elect to provision an ONS SDCC as OSI only.

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

OSI Connectionless Network Service

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

OSI Routing

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

TARP

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

TCP/IP and OSI Mediation

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

OSI Virtual Routers

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

IP-over-CLNS Tunnels

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

OSI Provisioning in CTC

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

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

64-Bit RMON Monitoring Over DCC

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

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

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

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

FLT Secondary State

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

- FLT (Fault) The entity has a raised alarm or condition.

The FLT SST is an extension to the existing ONS state model. As such, the FLT state is a Telcordia GR-1093 secondary state. It identifies that the affected entity is OOS because it is faulty. The FLT secondary state affects the service state only. The AdminState (the state you manage the entity into) is not affected. The FLT SST is the result of autonomous action; you cannot manage an entity into the FLT SST. The FLT SST is for retrieval purposes only. An entity's service state will transition into the OOS-AU or OOS-AUMA (AU for autonomous) service state if alarms or conditions are present. The FLT SST is appended to the existing secondary state for the entity when an alarm or condition exists.

Equipment FLT Service State

Some Equipment alarms will not generate an FLT SST transition. If a state already exists to represent the equipment condition, FLT will not be added to the secondary state list:

- MEA–Mismatch of equipment is represented as MEA SST
- IMPROPRMVL–Improper Removal is represented as UEQ SST
- No FLT will be added, and there will be no alarms, when equipment is in AINS

FLT SST with Ports

In pre-6.0 releases, an IS-NR port with an LOS alarm remains as IS-NR service state. There is no service state change to reflect the port is down. A new PST-PSTQ service state is introduced in Release 6.0 to reflect a port in MT state that is alarmed, OOS-AUMA (Autonomous, Management).

Any port alarm that results in the AINS countdown being inhibited will result in an FLT SST transition for the port. Loopback alarms will not result in an FLT SST transition, as there is a LPBK state to represent this information. There is NO FLT SST in the DSBLD state, as all alarms are cleared in the DSBLD state.

Connection FLT Service State

FLT SST connection changes are the same as for port changes. As with the port, the connection with an alarm in pre-6.0 releases has a service state of IS-NR. A new PST-PSTQ pair is introduced in Release 6.0 to reflect a cross connect in maintenance with an alarm, OOS-AUMA (Autonomous, Management). Any connection alarm that results in the AINS countdown being inhibited will result in the FLT SST transition for the connection. There is no FLT SST in the DSBLD state, as all alarms are cleared in the DSBLD state.

Manage Pluggable Port Modules

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

Change Pluggable Port Module Service States

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

Cisco Service Assurance Agent ML-Series Support

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

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

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

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

Cisco Service Assurance Agent on the ML-Series

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

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

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

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

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

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

CTC Launcher

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

CTC Launcher provides two connection options. First, it can be used to access ONS NEs that have IP connectivity to the CTC computer. Second, CTC Launcher can establish connectivity to ONS NEs that reside behind a third party, OSI-based GNE. To create a connection through the OSI-based GNE, CTC Launcher creates a TL1 tunnel. This tunnel is similar to the static IP-over-CLNS tunnels that are available in CTC Release 6.0. (For information about IP-over-CLNS tunnels, refer to the Release 6.0 ONS product documentation.) However, unlike the static IP-over-CLNS tunnels, the TL1 tunnel does not require provisioning on the third party GNE, the DCN routers, or the ONS NEs. The tunnel connection is created using the CTC Launcher. It can then be managed using CTC.

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

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

Step 1 Go to http://www.cisco.com.

Step 2 Choose Technical Support & Documentation.

Step 3 Choose Optical Networking.

Step 4 Choose the ONS 15300, ONS 15400, or ONS 15600 product category.

Step 5 Choose the Configuration Guides category.

Step 6 Click the CTC Launcher Application Guide link under the appropriate product.

TL1

TL1 Open GNE

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

Open GNE Commands

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

RTRV-TADRMAP

- RETRIEVE-TID_ADDRESS_MAP

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

DLT-TADRMAP

- DELETE-TID_ADDRESS_MAP

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

ENT-TADRMAP

- ENTER-TID_ADDRESS_MAP

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

ENT-TUNNEL-PROXY

- ENTER-TUNNEL_PROXY

  This command is used to create a proxy tunnel.

DLT-TUNNEL-PROXY

- DELETE-TUNNEL_PROXY

  This command is used to delete a proxy tunnel.

RTRV-TUNNEL-PROXY

- RETRIEVE-TUNNEL_PROXY

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

ENT-TUNNEL-FIREWALL

- ENTER-TUNNEL_FIREWALL

  This command is used to create a firewall tunnel.

DLT-TUNNEL-FIREWALL

- DELETE-TUNNEL_FIREWALL

  This command is used to a delete a firewall tunnel.

RTRV-TUNNEL-FIREWALL

- RETRIEVE-TUNNEL_FIREWALL

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

Changed Commands for Open GNE

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

ED-<OCN_TYPE>

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

RTRV-<OCN_TYPE>

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

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

REPT^DBCHG

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

New Card Support

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

- DS1-E1-56
- OC192-XFP
- MRC-12
- XCVXC
- Detectable filler card
- ML100X-8
- OPT-BST-E

TL1 Command Changes

New Commands

The following new TL1 commands are added for Release 6.0.

- RTRV-BFDLPM
- CHG-EQPT
- ALW-CONSOLE-PORT
- DLT-BULKROLL
- DLT-ROLL
- DLT-ROUTE-GRE
- DLT-TADRMAP
- DLT-TUNNEL-FIREWALL
- DLT-TUNNEL-PROXY
- ED-BULKROLL
- ED-PROTOCOL
- ED-ROLL
- ENT-BULKROLL
- ENT-ROUTE-GRE
- ENT-TADRMAP
- ENT-TUNNEL-FIREWALL
- ENT-TUNNEL-PROXY
- INH-CONSOLE-PORT
- RTRV-AUDIT-LOG
- RTRV-BULKROLL
- RTRV-TUNNEL-FIREWALL
- RTRV-TUNNEL-PROXY
- RTRV-FFP
- RTRV-ROLL
- RTRV-ROUTE-GRE
- RTRV-TADRMAP

Command Syntax Changes

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

Note These changes apply to all ONS platforms.

COPY-IOSCFG syntax:

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

Is changed to:

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

COPY-RFILE syntax:

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

Is changed to:

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

DLT-ROUTE syntax:

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

Is changed to:

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

ED-10GIGE syntax:

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

Is changed to:

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

ED-BITS syntax:

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

Is changed to:

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

ED-CRS-STS-PATH syntax:

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

Is changed to:

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

ED-E1 syntax:

ED-E1[:<TID>]:<aid>:<CTAG>[:::LINECDE=<linecde>,][FMT=<fmt>,][TACC=<tacc>,][TAPTYPE=<taptype>,][SFBER=<sfber>,][SDBER=<sdber>,][SOAK=<soak>,][NAME=<name>,][CMDMDE=<cmdmde>][:<pst>[,<sst>]];

Is changed to:

ED-E1[:<TID>]:<aid>:<CTAG>[:::LINECDE=<linecde>,][FMT=<fmt>,][TACC=<tacc>,][TAPTYPE=<taptype>,][SFBER=<sfber>,][SDBER=<sdber>,][SOAK=<soak>,][NAME=<name>,][CMDMDE=<cmdmde>,][SYNCMSG=<syncmsg>,][SENDDUS=<senddus>,][ADMSSM=<admssm>,][SABIT=<sabit>][:<pst>[,<sst>]];

ED-EC1 syntax:

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

Is changed to:

ED-EC1[:<TID>]:<aid>:<CTAG>[:::PJMON=<pjmon>,][LBO=<lbo>,][SOAK=<soak>,][SFBER=<sfber>,][SDBER=<sdber>,][NAME=<name>,][AISONLPBK=<aisonlpbk>,][CMDMDE=<cmdmde>,][EXPTRC=<exptrc>,][TRC=<trc>,][TRCMODE=<trcmode>,][TRCFORMAT=<trcformat>][:<pst>[,<sst>]];

ED-FFP-MOD2 syntax:

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

Is changed to:

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

ED-G1000 syntax:

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

Is changed to:

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

ED-GIGE syntax:

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

Is changed to:

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

ED-NE-GEN syntax:

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

Is changed to:

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

ED-POS syntax:

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

Is changed to:

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

ED-T1 syntax:

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

Is changed to:

ED-T1[:<TID>]:<aid>:<CTAG>[:::LINECDE=<linecde>,][FMT=<fmt>,][LBO=<lbo>,][TAC
C=<tacc>,][TAPTYPE=<taptype>,][SOAK=<soak>,][SFBER=<sfber>,][SDBER=<sdber>,][
SYNCMSG=<syncmsg>,][SENDDUS=<senddus>,][NAME=<name>,][CMDMDE=<cmdmde
>,][AISONLPBK=<aisonlpbk>,][MODE=<mode>,][SYNCMAP=<syncmap>,][ADMSSM=<
admssm>,][VTMAP=<vtmap>,][AISVONAIS=<aisvonais>,][AISONLOF=<aisonlof>,][INHF
ELPBK=<inhfelpbk>][:<pst>[,<sst>]];

ED-T3 syntax:

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

Is changed to:

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

ED-VC3 syntax:

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

Is changed to:

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

ED-VT1 syntax:

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

Is changed to:

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

ED-VT2 syntax:

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

Is changed to:

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

ENT-EQPT syntax:

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

Is changed to:

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

ENT-ROLL syntax:

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

Is changed to:

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

SET-ATTR-SECUDFLT syntax:

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

Is changed to:

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

Miscellaneous syntax changes:

Syntax:

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

Is changed to:

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

Response:

<aid>:<sc>,[<switchtype>]

Is changed to:

[<vendor>],[<netype>]

Command Response Changes

The following TL1 responses have changed in Release 6.0.

Note These changes apply to all ONS platforms.

RTRV-10GIGE response:

<aid>:,,[<role>],[<status>]:[<portname>],[<macaddr>],[<lbcl>],[<opt>],[<opr>],[<mfs>]:<pst>,[<sst>]

Is changed to:

<aid>:,,[<role>],[<status>]:[<portname>],[<macaddr>],[<lbcl>],[<opt>],[<opr>],[<mfs>],[<freq>],[<lossb>]:<pst>,[<sst>]

RTRV-DS3I response:

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

Is changed to:

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

RTRV-E1 response:

<aid>::<linecde>,<fmt>,[<tacc>],[<taptype>],[<sfber>],[<sdber>],[<soak>],[<name>]:[<pst>],[<sst>]

Is changed to:

<aid>::<linecde>,<fmt>,[<tacc>],[<taptype>],[<sfber>],[<sdber>],[<soak>],[<soakleft>],[<name>],[<syncmsg>],[<senddus>],[<retime>],[<admssm>],[<providesync>],[<aisonlpbk>],[<saBit>]:[<pst>],[<sst>]

RTRV-E3 response:

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

Is changed to:

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

RTRV-E4 response:

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

Is changed to:

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

RTRV-EC1 response:

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

Is changed to:

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

RTRV-EQPT response:

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

Is changed to:

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

RTRV-FSTE response:

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

Is changed to:

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

RTRV-GIGE response:

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

Is changed to:

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

RTRV-INV response:

<aid>,<aidtype>::[<plugtype>],[<pn>],[<hwrev>],[<fwrev>],[<sn>],[<clei>],[<twl1=nwl in code>],[<twl2= wl1 in code>],[<twl3=wl2 in code>],[<twl4=wl3 in code>],[<pluginvendorid>],[<pluginpn>],[<pluginhwrev>],[<pluginfwrev>],[<pluginsn>],[<ilossref>],[<productId>],[<versionId>],[<fpgaVersion>]

Is changed to:

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

RTRV-STM1E response:

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

Is changed to:

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

RTRV-T1 response:

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

Is changed to:

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

RTRV-VT2 response:

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

Is changed to:

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

SET-TOD response:

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

Is changed to:

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

TL1 ENUM Changes

Note These changes apply to all ONS platforms.

TL1 ENUM Types Changed

The following enum types have been merged into the EQUIPMENT_TYPE enum type.

- EQUIPMENT_TYPE_15310
- EQUIPMENT_TYPE_15327
- EQUIPMENT_TYPE_15454

TL1 ENUM Items Added or Removed

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

Table 5 ADDRTYPE enum items added to Release 6.0

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

ADDRTYPE is used in the following commands:

- DLT-TADRMAP

Table 6 CARDMODE enum items added to Release 6.0

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

CARDMODE is used in the following commands:

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

Table 7 DL_TYPE enum items added to Release 6.0

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

DL_TYPE is used in the following commands:

- APPLY

Table 8 ENCODING enum items added to Release 6.0

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

ENCODING is used in the following commands:

- ENT-TADRMAP

Table 9 ENV_ALM enum items added to Release 6.0

ENUM Name	ENUM Value
ENV_ALM_ENV_ALM_ENGTRANS	“ENGTRANS”
ENV_ALM_ENV_ALM_FUELLEAK	“FUELLEAK”
ENV_ALM_ENV_ALM_GASALARM	“GASALARM”
ENV_ALM_ENV_ALM_HATCH	“HATCH”
ENV_ALM_ENV_ALM_LEVELCON	“LEVELCON”
ENV_ALM_ENV_ALM_LVDADSL	“LVDADSL”
ENV_ALM_ENV_ALM_LVDBYPAS	“LVDBYPAS”
ENV_ALM_ENV_ALM_PWRMJ	“PWRMJ”
ENV_ALM_ENV_ALM_PWRMN	“PWRMN”
ENV_ALM_ENV_ALM_PWR_139	“PWR-139”
ENV_ALM_ENV_ALM_PWR_190	“PWR-190”
ENV_ALM_ENV_ALM_RINGENMN	“RINGENMN”
ENV_ALM_ENV_ALM_RINGGENMJ	“RINGGENMJ”
ENV_ALM_ENV_ALM_RTACADSL	“RTACADSL”
ENV_ALM_ENV_ALM_RTACCRIT	“RTACCRIT”
ENV_ALM_ENV_ALM_RTACPWR	“RTACPWR”
ENV_ALM_ENV_ALM_RTACPWRENG	“RTACPWRENG”
ENV_ALM_ENV_ALM_RTBAYPWR	“RTBAYPWR”
ENV_ALM_ENV_ALM_RTRVENG	“RTRVENG”

Table 9 ENV_ALM enum items added to Release 6.0 (Continued)

ENUM Name	ENUM Value
ENV_ALM_ENV_ALM_TEMP	“TEMP”
ENV_ALM_ENV_ALM_TREPEATER	“TREPEATER”

ENV_ALM is used in the following commands:

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

Table 10 EQUIPMENT_TYPE enum items added to Release 6.0

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

EQUIPMENT_TYPE is used in the following commands:

- CHG-EQPT
- ENT-EQPT

Table 11 EQPT_TYPE enum items added to Release 6.0

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

EQPT_TYPE is used in the following command response:

- REPT_EVT

Table 12 FC_LINKRATE enum items dropped from Release 5.0.x

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

FC_LINKRATE is used in the following commands:

- RTRV-FC

Table 13 FC_LINKRATE enum items added to Release 6.0

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

FC_LINKRATE is used in the following commands:

- RTRV-FC

Table 14 FRAME_FORMAT enum items added to Release 6.0

ENUM Name	ENUM Value
FRAME_FORMAT_LT_JESF	“JESF”

FRAME_FORMAT is used in the following commands:

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

Table 15 LO_XC_MODE enum items added to Release 6.0

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

LO_XC_MODE is used in the following commands:

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

Table 16 LPBK_TYPE enum items dropped from Release 5.0.x

ENUM Name	ENUM Value
LPBK_TYPE_FE_CMD_ESF_PAYLD_LPBK	“PAYLOAD”

FC_LINKRATE is used in the following commands:

- RTRV-FC

Table 17 LPBK_TYPE enum items added to Release 6.0

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

LPBK_TYPE is used in the following commands:

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

Table 18 MOD2 enum items added to Release 6.0

ENUM Name	ENUM Value
MOD2_M2_VC11	“VC11”

MOD2 is used in the following commands:

- RTRV-FFP-MOD2
- RTRV-LNK-MOD2LNK
- RTRV-NE-APC
- RTRV-NE-WDMANS
- RTRV-TRC-OCH
- SCHED-PMREPT-MOD2

Table 19 MOD2ALM enum items added to Release 6.0

ENUM Name	ENUM Value
MOD2ALM_M2_VC11	“VC11”

MOD2ALM is used in the following commands:

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

Table 20 MOD2B enum items added to Release 6.0

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

MOD2B is used in the following commands:

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

Table 21 MOD_PATH enum items added to Release 6.0

ENUM Name	ENUM Value
MOD_PATH_M2_VC11	“VC11”

MOD_PATH is used in the following commands:

- ENT-VCG
- RTRV-CRS
- RTRV-PATH
- RTRV-TRC-OC48
- RTRV-VCG

Table 22 OPTICAL_WLEN enum items added to Release 6.0

ENUM Name	ENUM Value
OPTICAL_WLEN_WL_1310	“1310”
OPTICAL_WLEN_WL_1470	“1470”
OPTICAL_WLEN_WL_1490	“1490”
OPTICAL_WLEN_WL_1510	“1510”
OPTICAL_WLEN_WL_1530	“1530”
OPTICAL_WLEN_WL_1550	“1550”

Table 22 OPTICAL_WLEN enum items added to Release 6.0 (Continued)

ENUM Name	ENUM Value
OPTICAL_WLEN_WL_1570	“1570”
OPTICAL_WLEN_WL_1590	“1590”
OPTICAL_WLEN_WL_1610	“1610”

OPTICAL_WLEN is used in the following commands:

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

Table 23 OPTICS enum items added to Release 6.0

ENUM Name	ENUM Value
OPTICS_OP_100_BASE_FX	“100_BASE_FX”
OPTICS_OP_100_BASE_LX	“100_BASE_LX”

OPTICS is used in the following commands:

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

Table 24 PROTOCOLAID enum items added to Release 6.0

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

PROTOCOLAID is used in the following commands:

- ED-CMD-SECU

Table 25 PROTOCOLSTAT enum items added to Release 6.0

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

PROTOCOLSTAT is used in the following commands:

- ED-PROTOCOL

Table 26 REACH enum items added to Release 6.0

ENUM Name	ENUM Value
REACH_AUTOPROV	“AUTOPROV”
REACH_CX	“CX”
REACH_DX	“DX”
REACH_ER	“ER”
REACH_EW	“EW”
REACH_HX	“HX”
REACH_I1	“I1”
REACH_I2	“I2”
REACH_I3	“I3”
REACH_I5	“I5”
REACH_IR_1	“IR-1”
REACH_IR_2	“IR-2”
REACH_IR_3	“IR-3”
REACH_IR_5	“IR-5”
REACH_L1	“L1”
REACH_L2	“L2”
REACH_L3	“L3”

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

ENUM Name	ENUM Value
REACH_L5	“L5”
REACH_LR	“LR”
REACH_LRM	“LRM”
REACH_LR_1	“LR-1”
REACH_LR_2	“LR-2”
REACH_LR_3	“LR-3”
REACH_LR_5	“LR-5”
REACH_LW	“LW”
REACH_LX	“LX”
REACH_MM	“MM”
REACH_MX	“MX”
REACH_P1L1	“P1L1”
REACH_S1	“S1”
REACH_S2	“S2”
REACH_S3	“S3”
REACH_S5	“S5”
REACH_SM	“SM”
REACH_SR	“SR”
REACH_SR_1	“SR-1”
REACH_SR_2	“SR-2”
REACH_SR_3	“SR-3”
REACH_SR_5	“SR-5”
REACH_SW	“SW”
REACH_SX	“SX”
REACH_T	“T”
REACH_V2	“V2”
REACH_V3	“V3”
REACH_VX	“VX”
REACH_ZX	“ZX”

REACH is used in the following commands:

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

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

Table 27 REQTYPE enum items added to Release 6.0

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

REQTYPE is used in the following commands:

- RTRV-BFDLPM-MOD2

Table 28 RFILE enum items added to Release 6.0

ENUM Name	ENUM Value
RFILE_LOG	“RFILE-LOG”

RFILE is used in the following commands:

- COPY-IOSCFG
- COPY-RFILE

Table 29 SYNCMAP enum items added to Release 6.0

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

SYNCMAP is used in the following commands:

- ED-T1
- RTRV-T1

Table 30 SYNC_CLOCK_REF_QUALITY_LEVEL enum items dropped from Release 5.0.x

ENUM Name	ENUM Value
SYNC_CLOCK_REF_QUALITY_LEVEL_QREF_RES_SDH	“RES-SDH”

SYNC_CLOCK_REF_QUALITY_LEVEL is used in the following commands:

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

Table 31 TIDADRMODE enum items added to Release 6.0

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

TIDADRMODE is used in the following commands:

- RTRV-TADRMAP

Table 32 TRANSMODE enum items added to Release 6.0

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

TRANSMODE is used in the following commands:

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

Table 33 VTMAP enum items added to Release 6.0

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

VTMAP is used in the following commands:

- ED-T1
- RTRV-T1

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15454, Release 5.0.2*
- *Release Notes for the Cisco ONS 15454 SDH, Release 6.0*
- *Release Notes for the Cisco ONS 15327, Release 6.0*
- *Release Notes for the Cisco ONS 15600, Release 6.0*
- *Release Notes for the Cisco ONS 15310-CL, Release 6.0*
- *Cisco ONS 15454 Software Upgrade Guide, Release 6.0*

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.

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