Release Notes for Cisco ONS 15454 Release 4.6.5

August, 2007

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.

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 4.6" version of the *Cisco ONS 15454 Procedure Guide*; *Cisco ONS 15454 Reference Manual*; *Cisco ONS 15454 Troubleshooting Guide*; *and Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide.* For the most current version of the *Release Notes for Cisco ONS 15454 Release 4.6.5*, visit the following URL:

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

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

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

Contents

Changes to the Release Notes, page 2

Caveats, page 2

Resolved Software Caveats for Release 4.6.5, page 25

New Features and Functionality, page 39

Related Documentation, page 72

Obtaining Documentation, page 73

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

Obtaining Technical Assistance, page 75

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15454 Release 4.6.5* since the production of the Cisco ONS 15454 System Software CD for Release 4.6.5.

No changes have been added to the release notes for Release 4.6.5.

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 # CSCec73848

When you modify VOA attenuation calibration, an optical power transient can occur. This issue will be resolved in Release 5.0.

DDTS # CSCdy48478 Fan Tray Assembly Fan Fail Lamp Test Failure

A user-initiated lamp test does not illuminate the fan fail LED on the fan tray assembly for the ONS 15454 or the ONS 15454 SDH. The lamp test successfully lights the LEDs for major, minor, and critical alarms on the fan tray, and for all cards in the chassis, but does not light the fan fail LED. An actual fan failure, however, will light the fan fail LED.

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 will be resolved in Release 5.0.

Upgrades

DDTS # CSCec82344

CTC SendPDIP alerts might be raised on upgrades if any of the nodes in your network have the flag for SendPDIP set to “false” in their associated NE Defaults. This is because the upgraded node will have the value set to “true,” which is the default setting. You do not need to clear these alerts. They will clear when the upgrade is finished.

Line Cards

Note Rarely, when the active TCC2 is removed, small traffic errors of 2 to 30 ms can sometimes occur. To avoid this issue, switch to the protect TCC2 before removing the working TCC2.

DDTS # CSCef97420

Rarely, if a the client associated with a TL1 ENE/GNE session stops responding to TL1 updates, then a common control card might autonomously reset.

For example, say, Node A is a GNE, and Node B is an ENE. Client C opens GNE TL1 sessions with Node A, and from within that sessions, opens an ENE sessions to Node B. If Client C locks up and stops processing autonomous messages from Node B, but does not close the connection, then it is possible that the controller card on Node A will reboot.

This is resolved in Releases 4.6.5 and 5.0.

DDTS # CSCeh41482

Rarely, the active common control card can autonomously reset when an IOS telnet session is established to an ML card. This does not always occur, but might occur and is repeatable in rare circumstances. This issue is resolved in Releases 4.6.5 and 5.0.

DDTS # CSCed34189

An expected far end LOF is never raised, and RAI becomes stuck on the DS3XM. This can occur with two connected DS3XMs, when a loss of frame is raised for one, and then FE-LOF is expected on the other. This issue will be resolved in Release 5.0.

DDTS # CSCed24599

While the DS3E protect card is active, invoking the auto frame format provisioning feature (AUTL) for a port might result in a misprovisioned frame format on that port (as compared to the actual frame format received on the DS3 receive line). If you must provision the frame format for a port while the protect card is active, provision it explicitly (manually select UNFRAMED, M13 or CBIT) instead of using the AUTL feature to ensure appropriate frame format provisioning on that port. This issue will be resolved in Release 5.0.

DDTS # CSCec09783

Rarely, loss of traffic on an EC1 card can occur if you pull the card and quickly reinsert it. To avoid this issue, wait 5 seconds before reinstalling the card. This issue will be resolved in a future hardware release.

DDTS # CSCec57665

When changing the tunnel type from IP Tunnel to a traditional SDCC tunnel, the rollback does not restore the original tunnel. If this occurs, manually recreate the tunnel. This issue will be resolved in Release 5.0.

DDTS # CSCed01244

With a 1+1 protection group configured on an OC3-8 card, an APSCM alarm might be raised unexpectedly. Any switch on the protection group will clear the alarm. This issue will be resolved in Release 5.0.

DDTS # CSCec79028

UNEQ-P & LOP-P CR alarms might be reported momentarily when PCA traffic is preempted while applying a force switch ring or manual switch ring. The issue is more common when there are PCA circuits on multiple node OC-192 rings. This issue will be resolved in Release 5.0.

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.

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 build 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.

Ethernet Polarity Detection

The TCC2 does not support polarity detection & correction on the LAN Ethernet port. This is a change from prior common control cards, such as the TCC+. If your LAN Ethernet connection has the wrong polarity (due to incorrect wiring on the backplane wire-wrap pins), the connection will work when using a TCC+, but not with a TCC2. To avoid possible problems, ensure that your Ethernet cable has the correct mapping of the backplane wire-wrap pins. For Ethernet pin mappings, consult the “DLP-A 21 Install LAN Wires on the Backplane” procedure in the user documentation.

If you are using a TCC+, the Release 4.0 or 4.1.x software will report the polarity issue (previous releases do not), by raising the standing condition: LAN Connection Polarity Reverse Detected (COND-LAN-POL-REV). Also, notification will appear on the fan tray LCD, which will display "BP LAN POL. NEG." The issue will typically be reported during the software upgrade process, but can also be raised during a new installation when using TCC+ and Release 4.0 or 4.1.x.

If this is a new installation with a TCC2 and you have the Ethernet polarity reversed, the TCC2 will not communicate over the LAN Ethernet interface (no polarity correction will occur), and no condition will be reported, nor will the fan tray LCD indicate an issue.

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

Table 3 Miscellaneous Compatible Products

Product Name	Description
15454-BLANK	Empty slot Filler Panel
15454-GBIC-LX	1000Base-LX, SM or MM, standardized for 15454/327

Table 3 Miscellaneous Compatible Products

Product Name	Description
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 # 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.

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.

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.

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

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

Active cross connect (XC/XC10G/XCVT) cards should not generally be physically removed. If the active cross connect or TCC2 card must be removed, you can first perform an XC/XCVT/XC10G side switch or TCC2 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 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.

DDTS # CSCdv62565, CSCdv62573

In a 1:N protection group, traffic loss could occur if a DS-N card is preprovisioned and then added to the group while another working card in the group is removed from its slot. To avoid this, before adding slots to a protection group ensure that:

- The protect card is not actively carrying traffic (that is, the card is in standby)
- Any working slot you add to the group actually contains a working card at the time you add it

This issue will be resolved in Release 6.0.

DWDM Cards

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 # 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 # CSCed05006

In the Defaults pane, when you change the default ALS mode for the TXP/TXPP_2.5G_10G cards to "Manual Restart for Test," CTC issues an error message. The mode can be successfully changed but you must click Reset to proceed with further changes to defaults. Changes to other defaults on that pane may have to be reapplied. To prevent the error, change the default pulse width at the same time as changing the default ALS mode to "Manual Restart for Test." The default pulse width must be in the appropriate range for this mode (80-100). This issue will be resolved in a Release 5.0.

DDTS # CSCec78443

You cannot provision an end-to-end circuit through a TXP regen group (a pair of transponders connected back to back via the client interface that provide for regeneration for DWDM) with G.709 on, and in line termination on the TXP cards, which are feeding traffic to the regen group. To avoid this issue turn G709 off for all TXPs. This issue will be resolved in Release 5.0.

DDTS # CSCeb25490

Occasionally the system displays a LO-TXPOWER alarm when SMT4 and STM1 SFP is installed at the client port of a TXP or TXPP card. The LO-TXPOWER alarm is displayed when the alarm threshold is set to the default value in the TX POWER LOW field of the Optical Threshold in the CTC provisioning window. To work around this issue, lower the alarm threshold value (TX POWER LOW (dBm)) of Optical Threshold in the CTC provisioning window. Refer to Table XX for threshold values. This issue will be resolved in Release 5.0.

Table 4 contains the High and Low Alarm Thresholds of Tx-power and Rx-power of SFPs in TXP and TXPP cards. The values of these thresholds are read from the EEPROM inside the SFPs. This table can be used as a reference in PM alarm provisioning and Threshold Alarm verification.

Table 4 Alarm Thresholds

Part#	Rate	TxHi[1]	TxLow	RxHi	RxLow
10-1421-02	OC48-SR	2.0	-14.6	0	-21.0
10-1422-01	OC48-IR	4.0	-9.6	3.0	-23.2
10-1829-01	OC12-IR	-6.9	-13.1	-6.0	-31.0
10-1828-01	OC3-IR	-6.9	-13.9	-6.0	-31.0
10-1832-01	2FC/2GB-LX	0.9	-13.2	1.0	-24.0
10-1590-01	2FC	1.0	-14.6	N/A[2]	N/A
10-1750-01	ESCON	N/A	N/A	N/A	N/A

1. The power unit for TxHi/TxLow/RxHi/RxLow used is dBm.
2. N/A means Not Available. The vendor did not provide the information in this field.

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.

DDTS # CSCeb26662 and CSCea88023

With TXP-MR-2.5G cards, when the current 1 day Optics PM rolls over, the information is inaccurate for “avgs.” 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.

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.

E Series and G Series Cards

DDTS # CSCdy37198

On Cisco ONS 15454s equipped with XC or 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 be resolved in a future release.

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 following control protocols have been added to the static MAC address table to guarantee no loss of unicast traffic during normal usage of these MAC addresses:

Table 0-1 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 on page 11 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 E1000-2/E100

Whenever 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. To avoid a failed STS-1 circuit, delete the second STS-3c prior to creating any STS-1 circuit.

ML Series Cards

DDTS # CSCee66238

Non-zero Port Drop Counts (renamed EtherStatsDropEvents in R5.0 and forward) are displayed in the Performance tab for ML-100 or ML-1000. The Port Drop Counts are packets dropped by layer-2 or layer-3 forwarding microcode in the data plane. A common reason this might occur is VLAN filtering due to a mismatch in VLAN configurations on a link.

There is also one misleading condition that increments the Port Drop Counts: When using RPR "int spr," multicast and layer-2 flood packets circle the entire ring and are removed from the ring by the station that sourced them onto the ring. This packet removal is counted in Port Drop Counts for the POS interface. This is normal behavior and does not indicate an error or lost packet. This issue is resolved in Releases 4.6.5 and 5.0.

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, see the "Documentation" section on page 24.

DDTS # CSCee65395

On ML100T and ML1000, setting one member of a VCG to the OOS admin state can cause the other member to go down. This causes the whole VCG and POS port to go down. This has been seen only on STS12c-2v. This issue will be resolved in a future maintenance release.

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 be resolved in a future release.

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 in Release 4.0. This issue will be resolved in a future release.

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.

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.

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

DDTS # CSCee88405

In Release 4.6.5 the option to change the admin state of a port while deleting or editing an SDCC or LDCC has been removed.

JRE Updates

Cisco ONS platforms ship with a Java Runtime Environment (JRE) from Sun Microsystems. Occasionally Sun releases maintenance releases to the JRE. The Sun Microsystems website lists JRE maintenance releases and the issues resolved for each. Cisco recommends that you review these listings to determine if the issues resolved in any given JRE maintenance release warrant a JRE upgrade for your particular network. Cisco tests only with the specific JRE actually shipped with the ONS software CD.

Circuit State Transition from OOS-AINS

For the following cards, a circuit might inappropriately transition from the OOS-AINS state to the IS, or OOS-AINS-PARTIAL state.

- DS3I (SONET and SDH)
- DS1 (STS circuits only)
- DS3XM
- E1-42
- E1-14
- E3

This can occur when the circuit and the port for the circuit are both in the OOS-AINS state. Upon a soft reset of the card or a software upgrade, the circuit might transition into the IS or the OOS-AINS PARTIAL state, resulting in false path level alarms. For the DS1 card, this issue occurs only on STS circuits. This issue is non-service affecting and will be resolved in a future release.

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 is under investigation.

DDTS # CSCec17281

When the “Status” field for a circuit in the circuit table shows “INCOMPLETE,” this can be interpreted as an alarm or traffic-affecting condition on the circuit. On path protection and BLSR circuits, a circuit is shown as INCOMPLETE if either the working or protect path is missing a network span or connection, even if traffic is flowing without error on the other, redundant path. This can lead to confusion, since the

meaning of “INCOMPLETE” is not well-defined. You can see this if you, for example, introduce LOS on a span in a BLSR network such that traffic is switched to another path around the ring. Ignore the INCOMPLETE circuit status in such cases and instead look for any alarms in the network. The circuit Status will be defined more clearly in Release 5.0.

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 # CSCec61769

The time zone shows the incorrect zone when changed via TL1. This issue will correct itself once a TCC2 reset occurs. This issue will be resolved in an future release.

DDTS # CSCec67324

The Generation II SSM value is not sent out correctly when changed from Gen 1 to Gen 2. Perform a TCC2 switch to correct this issue. This issue will be resolved in a future release.

DDTS # CSCec29230

The NE PWR-B alarm is not reported in CTC after an upgrade to Release 3.4.2. You can view the alarm through TL1. This issue will be resolved in a future release.

DDTS # CSCea78364

Simultaneous failure of working and protect cards in 1:N protection groups may not be alarmed as service affecting. This can occur when the working card of the protection group has been removed from the chassis, and the protect card of the protection group is subsequently issued a Manual Reset. Since the working and protect facilities are impaired, the Improper removal alarm should clear and be reissued as a Critical and service affecting condition. This issue will be resolved in Release 6.0.

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 # 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 # 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 will be resolved in Release 6.0.

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" feature

DDTS # CSCdy61275

Far end path FC-P is not counted on EC1 or OC3 cards. When a path defect is transmitted to the far end, it reports RDI-P. However, the condition is not examined and reported as a PM count. This issue will be resolved in a Release 6.0.

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. This issue will not be resolved.

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 will be resolved in Release 6.0.

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.

NE Defaults

The following caveats apply for NE defaults.

- 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.

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.

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.

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.

“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.

Alarms

DDTS # CSCee60922

When you have dual TCCs and one is faulty, and you remove the faulty TCC, the equipment failure alarm fails to clear after the TCC card is removed. This issue will be resolved in a future release.

DDTS # CSCuk47488

A soft reset of the active TCC2 causes a TCC2 switch. In rare cases, subsequently, all BTC based cards XC. This issue will be resolved in Release 5.0.

SNMP

DDTS # CSCeb34423

All 8B10B TCA events show a negative value for the Current Value field. When 8B10B errors cross their threshold, a TCA event is raised. Included in the TCA event is the current value. If either the current value or the threshold exceeds a 32 bit number in a given period (15 MIN or 1 DAY), it will be shown as a negative value. This issue will be resolved in a future release.

DDTS # CSCed05502

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

DDTS # CSCed05742

Issuing an SNMP get on UASL does not result in the same output as for TL1 and HTTP when you query a node with PM data for UASL. This issue will be resolved in a future release.

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 GR-253, section 5.3.5.5, the FLM-150 and the OC-3 Express should respond with a No Request.

BLSR Functionality

DDTS # CSCee57049

When BLSR circuit is switched, TIM-P is not raised on the switched path. This issue will be resolved in a future release.

DDTS # CSCec77697

With a four-fiber non-revertive BLSR in WTR, a soft reset locks the active XC10G on an adjacent NE, causing traffic loss. To avoid this, issue a lockout on the BLSR prior to the soft reset. This issue will be resolved in a future release.

DDTS # CSCec75064 and CSCec75019

On a four-fiber BLSR after a BLSR switch and soft reset of the XC10G, LOP-P and/or UNEQ-P alarms might become stuck. If this occurs, lock out the span card that report the alarm and soft reboot it. This issue will be resolved in a future release.

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 # CSCeb09217

Circuit states are not updated after a span update. If you update a four node OC-12 two-fiber BLSR to a four node OC-192 two-fiber BLSR, the previous PCA circuits should be shown as two-fiber BLSR protected, but they are shown as "UNKNOWN" protected. If you relaunch CTC this situation is corrected. This issue will be resolved in Release 5.0.

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 # CSCea81000

In a two-fiber or four-fiber BLSR, MS-RFI is not reported for an LOS or LOF with a ring lockout in place on a different span. This issue will be resolved in Release 5.0.

DDTS # CSCdy45902

Traffic that should be dropped remains unaffected when a BLSR Protection Channel Access (PCA) VT tunnel is placed OOS. You must place all circuits in the tunnel OOS before the traffic will be dropped. This issue will be resolved in Release 5.0.

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 XC, XCVT, or XC10G card. You should also make the active cross connect card standby before removing it.

DDTS # CSCdv70175

When configuring a node with one 4 Fiber BLSR and one 2 Fiber BLSR, or with two 2 fiber BLSRs, an issue exists related to the version of XC deployed. Revision 004H and earlier revisions of the XC do not support these configurations. All later revisions of the XC and all versions of the XCVT and XC10G cross connects support all permutations of two BLSRs per node.

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/MSSPR.

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 TCC+/TCC2 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 # CSCee68239

Low order circuits cannot be created over Integrated path protection DRI. Circuit creation fails with an xUpsrSelectorPayloadMismatch error. This issue will be resolved in a future release.

DDTS # CSCeb37707

With a VT path protection circuit, if you inject signals with a thru-mode test set into one path of the circuit in a particular order, you may not see the appropriate alarms. This can occur when you first inject LOP-P, then clear, then inject LOP-V. This issue will be resolved in Release 6.0.

DDTS # CSCdv42151

When a path protection circuit is created end-to-end, CTC might not create the cross-connection on all the nodes along the path at the same time. This might cause an SD-P condition along the path. When the circuit is fully provisioned on all nodes, the SD-P will clear automatically. Other conditions that can be expected while the circuit is being created are LOP-P and UNEQ-P. To reduce the risk of unexpected transient conditions, circuits should be created in the OOS_AINS state.

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

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

Active cross connect (XC/XC10G/XCVT) cards should not generally be physically removed. If the active cross connect or TCC2 card must be removed, you can first perform an XC/XCVT/XC10G side switch or TCC2 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 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.

Performance Monitoring

DDTS # CSCeb85353

Bulk PM does not show 8b10b PM statistics for the TXPP_MR_2.5G card when Payload Type is set to "1G Ethernet." To see these statistics, go to the CTC card view > Performance > Payload PM tabs. This issue will be resolved in Release 5.0.

DDTS # CSCeb41916

If you create a 1+1 protection group, create a circuit on the working line, and then try to retrieve the path PMs on the protect side using TL1, the request is denied. To work around this issue, use CTC to retrieve the Path PMs on the protect line. This issue will be resolved in Release 5.0.

TL1

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

DDTS # CSCef18213

TL1 agent-related connections might remain in a CLOSE_WAIT state, unable to read or write data, for a long time after you issue several TL1 commands over TCP/IP, then disconnect the source that generated the commands. This issue is resolved in Releases 5.0, 4.6.5, and 4.0.4.

DDTS # CSCeg04772

Heavy traffic to TL1 agents and a subsequent loss of IP connectivity might leave the memory buffers full of pending data. The result is that tasks will attempt to read/write data, but will fail. It takes 30 minutes for TCP level clean-up to occur, enabling the tasks to complete. Rarely, if a the client associated with a TL1 ENE/GNE session stops responding to TL1 updates, then a common control card might autonomously reset. This issue is resolved in Release 5.0.

DDTS # CSCed08144

Rarely, TL1 autonomous messages might not be displayed in a session after several days of PM-related provisioning changes. This issue will be resolved in a future release.

DDTS # CSCeb33033

An exception is raised when retrieving PM stats via TL1 for the protect card of a 1:1 protection group when the working card is active. To avoid this issue, retrieve stats from the working card instead of the protect card. This issue will be resolved in a future release.

DDTS # CSCdz26071

The TL1 COPY-RFILE command, used for SW download, database backup, and database restore, currently does not allow a user-selected port parameter to make connections to the host. The command expects the default parameter of Port 21 and will only allow that number. This issue will be resolved in Release 5.0

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 Release 6.0.

Documentation

The following ML-series command documentation applies for Release 4.6.2 through 4.6.5. This command is not in the user documentation for the 4.6 general release. Users of Releases 4.6.2 through 4.6.5 should refer to the release notes for this command.

[no] pos vcat resequence {enable | disable}

Enables or disables the SW-LCAS H4 byte sequence number re-sequence feature. 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 Software Release 4.6.2 or later.

Syntax Description	Parameter	Description

Enable	Enables the re-sequencing of the H4 byte sequence numbers when a member is added to the VCAT group or removed from the VCAT group. If both members are up, then member #0 will have sequence number of zero (0) and member #1 will have sequence number one (1). If only one member is up, then the sequence number of that member will be zero (0).
Disables	Disables the re-sequencing of the H4 byte sequence numbers when a member is added to the VCAT group or removed from the VCAT group. Member #0 will always have a sequence number of zero (0) and member #1 will always have a sequence number of one (1)

Defaults The default setting is Enable.

Command Modes Per POS port configuration

Usage Guidelines The no form of the command will set the mode to the default.

Examples The following example disables the re-sequencing of the H4 byte sequence numbers for POS port 0:

```
Router(config)#int pos 0
Router(config)#pos vcat resequence disable
```

Resolved Software Caveats for Release 4.6.5

The following items are resolved in Release 4.6.5

ML Series Cards

DDTS # CSCef62420

When you provision two circuits on an ML card and then delete the second one provisioned, defects are not detected and alarms are not reported on the POS port. To correct this issue, after deleting the second circuit, change the admin state of the first circuit to OOS and then to IS. Allow a minimum of 5 seconds between the OOS and IS state changes. This issue is resolved in Release 4.6.4.

DDTS # CSCeg11560

As a result of memory loss, the ML card might fail to respond to telnet. When this issue occurs, console login fails with a “low memory” error message, and a possible CONTBUS-IO alarm. Traffic might be affected if spanning-tree is enabled on the ML, as the protocol might stop functioning, resulting in blocked spanning-tree ports without apparent cause.

This issue is most likely to affect service providers or large enterprise customers using static routes. Enterprise customers with routing protocols enabled over an ML network should not be affected. This issue exists in ML software Releases 4.0.x, 4.1.x, and 4.6.x, and is resolved in Release 5.0, and maintenance Release 4.6.4.

To reduce memory loss, increase the MAC aging time, so that short periods of inactivity will not trigger MAC aging. Using a maximum aging time of 1,000,000 seconds (11 days), should prevent nearly all memory loss, ensuring that the issue does not occur. Set aging time to the maximum with the following configuration command (for each bridge group "X"):

```
bridge X aging-time 1000000
```

In very large bridged networks, which might connect directly to thousands of layer-3 devices, Cisco recommends you increase the MAC table limit above the default of 1000 MAC addresses. This is done with the configuration command:

```
bridge X limit dynamic entries 10000
```

If the bridge MAC table is filled (exceeds the bridge dynamic limit), traffic will continue to be forwarded, but will be broadcast, rather than unicast, within the network. If all CPU memory is lost, the only action to restore communication is a reset of the ML card. If a reset via CTC fails, you might need to physically remove and reseat the ML card to initiate the reset. This issue is resolved in Release 4.6.4.

DDTS # CSCed92355

Spanning tree path cost for a POS subinterface is always 3 if there is no STP on the main interface. This issue is resolved in Release 4.6.4.

DDTS # CSCeg36635

With "port based" RPR load-balancing enabled, traffic entering a specific Ethernet port of an ML-100 should all move in one direction around the RPR

ring. (even ports to POS0, and odd ports to POS1). However, Unicast and Multicast traffic types are sent in opposite directions (multicast in even ports is sent out POS1). Routing protocol traffic travels the RPR ring in the opposite direction from that of data traffic. If an unrecovered RPR/ML failure occurs, this might result in down data traffic with no detection of the issue by layer-3 routing protocols, and prevent external layer-3 redundancy from working properly. This issue is resolved in Release 4.6.4.

DDTS # CSCea81249

When accessing an ML-series card via TCC telnet relay (that is, when telnetting to the IP address of the ONS 15454 TCC plus a port number based on the ML-series slot number) a high CPU load (as high as 80%) might result, with tasks "IP Input" and "Virtual Exec" creating the majority of the CPU load. Protocol processing might be disrupted due to this high CPU load. You can view the CPU tasks and their respective resource usage with the "show processes" command. This occurs only when telnetting from the Microsoft Windows operating system environment.

The high CPU load is caused by an endless loop in the telnet negotiation process running in the background while the telnet session remains open. This can be confirmed by entering the exec command, "debug telnet," which shows a rapidly repeating sequence of activity. During normal operation, "debug telnet" would only show activity during the initial telnet connection and disconnection.

The following four methods of connecting to the ML-series command line interface are known workarounds for this issue:

1. Enter by the front serial Console port of the ML-series card.

2. Telnet to an IP address configured on the ML-series card via the POS or
3. front Ethernet interfaces.
4. Connect using the CTC connection window (right-click on ML-series card in CTC and select “Open IOS Connection”).
5. Telnet from UNIX, through TCC telnet relay.

This issue is resolved in Release 4.6.4.

DDTS # CSCef42414

When a card fail alarm is raised due to a microcode failure, you must collect the necessary logs before reloading the system. If the system is reloaded, either by the Cisco TAC or by you, before logs can be collected, you might lose information that could be valuable for debugging the issue. A microcode diagnostics logging feature is committed to Release 4.6.4 that resolves this issue.

DDTS # CSCee16330

A traffic loss can occur when an ML100T or ML1000 board failure occurs. When the board fails RPR does not wrap, and POS and Ethernet ports stay up. To recover from this, shut down the ports through the CLI. This issue is resolved in Release 5.0 and maintenance Release 4.6.4.

DDTS # CSCef77828

Occasionally, when RPR on an ML card unwraps as a result of a POS port that was previously DOWN coming back UP, the convergence time for traffic passing through that ML card is greater than 50 ms. This issue is resolved in Release 4.6.4.

DDTS # CSCee30006

When polling SONET PM statistics in the SONET MIB using SNMP, the TCC might lose connection to the ML Series cards for approximately 5 seconds. An SNMP MIB walk in progress might terminate prematurely. SNMP queries to ML

Series cards can then fail for approximately 5 seconds, and active telnet sessions to ML Series cards via the TCC LAN connection or CTC might become disconnected.

This issue can occur when a circuit is terminated on the ML card, and the community string is not of the format <community_string>@<slot_number>, indicating that the SNMP requests are sent to the SNMP agent on the TCC card. (If using a community string of the format <community_string>@<slot_number>, the SNMP requests are sent to the SNMP agent on the ML card).

If this issue occurs, the ML card status visible in the CTC status display changes to “Failed” for about 5 seconds, and then returns to “Active.” No alarm or condition is raised.

There are two supported workarounds to this issue:

1. Disable NMS from collecting SONET MIBs. Avoid the simple mibwalk on ONS 15454 nodes. Avoid using “getnext” for the SNMP table/object just preceding the SONET MIB.
2. Do not poll SNMP information through the SNMP agent on the TCC card at all. Poll the SNMP information for the ML card through the SNMP agent on the IOS line card instead. In other words, only use community strings of the format <community_string>@<slot_number>.

This issue is resolved in Release 4.6.4.

DDTS # CSCin35960

POS ingress classification based on IP precedence does not match the packets when inbound policy map classifying based on IP precedence is applied to the POS interface, which is configured for HDLC or PPP encapsulation. To avoid this issue, use LEX encapsulation (default) or, at the Ethernet ingress point, mark the COS based on an IP precedence classification, then classify based on the COS during POS ingress. This issue is resolved in Release 4.6.

DDTS # CSCea20962

No warning is displayed when applying OOS to ML drop ports on the circuit provisioning window. This issue is resolved in Release 4.6.

DDTS # CSCea11742

When a circuit between two ML POS ports is provisioned OOS, one of the ports might erroneously report TPTFAIL. This issue exists for both ML100T-12 and ML1000-2 cards. If this occurs, open a console window to each ML card and configure the POS port to shutdown. This issue is resolved in Release 4.6.

DDTS # CSCdy31775

Packets discarded due to output queue congestion are not included in any discard count. This occurs under either of the following conditions:

- Traffic on ML-series cards between Ethernet and SONET ports, with oversubscription of available circuit bandwidth configured, leading to output queue congestion.
- Traffic from SONET to Ethernet, with oversubscription of the available Ethernet bandwidth.

This issue is resolved in Release 4.6.

DDTS # CSCeb24757

Disconnecting a transmit fiber on an ML1000 port causes only the neighboring port to take the link down. Ideally, both ports should identify that the link went down so upper layer protocols can reroute the traffic to a different port. To work around this situation, issue “shutdown” and “no shutdown” to the port that has the disconnected or faulty transmit fiber. This issue is resolved in Release 4.6.

DDTS # CSCeb56287

When an ML-series circuit's state is provisioned from In-Service (IS) to Out-of-Service (OOS), and then back to IS, data traffic does not recover. To avoid this issue, prior to changing the state from IS, set the POS port to shut down on the CLI. After the state is changed back to IS from OOS, set the POS port to “no shutdown.” This issue is resolved in Release 4.6.

DWDM Cards

DDTS # CSCeb49210

A soft reset of the working or protect 2.5g multirate card in a Y-cable protection group clears an existing "Lockout of protection" request. It is not known when or if this issue will be resolved. This issue is resolved in Release 4.6.

DDTS # CSCeb39991

SCHED-PMREPT-CLNT does not generate the automatic report for TXPP cards. If you schedule PM reports on a Client or Trunk port of a TXPP, REPT^PM^EVT is never generated. However, the RTRV-PMSCHED-ALL count shows that the count is decreasing. This issue is resolved in Release 4.6.

DDTS # CSCeb49144

The Lamp Test feature does not display all the LED colors available on the 2.5G Transponder. This issue is resolved in Release 4.6.

DDTS # CSCeb37346

Near end and far end PMs might increment simultaneously on TXPP-2.5G cards. This can occur when two nodes have TXPP-2.5G cards and two nodes have STM16 cards in a four node network, where both TXPP-2.5G cards have STM16 SFPs on them, and are in MS (Line Termination) mode. By default, the TXPP-2.5G cards are in Splitter protection: the first DWDM port is working and the second is protect. If you remove the receive fiber of the first DWDM port on one TXPP-2.5G card, both near and far end counts begin to increment. The far end counts should not increment in this case. This issue is seen only when the Txpd cards have G709 and FEC on. If the cards have G709 and FEC off, only the near end counts will increment, as expected. This issue is resolved in Release 4.6.

G Series Cards

DDTS # CSCed61276

The Apply button on the G1000 Port Provisioning pane is not enabled when the Flow Control column is modified. This can occur when the column TXP Port is not visible. To avoid this issue, ensure that the column TXP Port is visible. Use the scroll bar if necessary. This issue is resolved in Release 4.6.2.

DDTS # CSCec03291

A G1-K traffic loss can occur on a software upgrade from Release 4.0, 4.1, or 4.5 to a later software release in an ONS 15454 node with XC or XCVT cards installed. This issue does not occur if the equipment has XC10G cards installed. This issue is resolved in Release 4.6 and maintenance Release 4.1.3

DDTS # CSCec05896

When a G-series card is used in transponder mode the severity of reported alarms is incorrect in some cases. When using transponder mode on G-series cards, if alarm severity is an issue, use the alarm profile editor to set the severity to the desired values. This issue is resolved in Release 4.6 and maintenance Release 4.1.3.

DDTS # CSCeb80771

An Ethernet traffic hit of 500-600 ms may occur when upgrading to Release 4.1 from a prior release. This can occur if active traffic is running on a G1000-4, G1K-4 or G1000-2 card when upgrading the node to Release 4.1. The hit will occur only the first time that you upgrade to Release 4.1. On subsequent downgrades followed by upgrades there will be no traffic hit and the upgrade will be errorless. There is no workaround; however the issue will not occur when upgrading from Release 4.1 to a later release. This issue is resolved in Releases 4.1.3 and 4.6.

Line Cards

DDTS # CSCed06531

Malformed IP packets can potentially cause the XTC, TCC/TCC+/TCC2 and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to reset at the same time. This issue is resolved in Release 5.0, and maintenance Releases 4.1.4, 2.3.5, 4.0.3, and 4.6.2.

DDTS # CSCed86946

Malformed ICMP packets can potentially cause the XTC, TCC/TCC+/TCC2 and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to reset at the same time. This issue is resolved in Release 5.0, and maintenance Releases 4.1.4, 2.3.5, 4.0.3, and 4.6.2.

DDTS # CSCec88426, CSCec88508, CSCed85088

Malformed TCP packets can potentially cause the XTC, TCC/TCC+/TCC2, and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to reset at the same time. This issue is resolved in Release 5.0, and maintenance Releases 4.1.4, 2.3.5, 4.0.3, and 4.6.2.

DDTS # CSCec59739, CSCed02439, CSCed22547

The XTC, TCC/TCC+/TCC2 and TCCi/TCC2 control cards are susceptible to a TCP-ACK Denial of Service (DoS) attack on open TCP ports. The controller card on the optical device will reset under such an attack.

A TCP-ACK DoS attack is conducted by withholding the required final ACK (acknowledgement) for a 3-way TCP handshake to complete, and instead sending an invalid response to move the connection to an invalid TCP state. This issue is resolved in maintenance Releases 4.1.4, 2.3.5, 4.0.3, and 4.6.2.

DDTS # CSCec88402, CSCed31918, CSCed83309, CSCec85982

Malformed UDP packets can potentially cause the XTC, TCC/TCC+/TCC2, and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to reset at the same time. This issue is resolved in Release 5.0, and maintenance Releases 4.1.4, 2.3.5, 4.0.3, and 4.6.2.

DDTS # CSCea16455, CSCea37089, CSCea37185

Malformed SNMP packets can potentially cause the XTC, TCC/TCC+/TCC2 and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to reset at the same time. This issue is resolved in Release 4.6, and maintenance Releases 4.0.1, 4.0.3, and 4.1.3.

DDTS # CSCed36598

When DHCP forwarding is turned on, and the forwarding to address is set to a cellbus address instead of a DHCP server address, you can lose connection to your nodes. Always set the forwarding address to a DHCP server. This issue is resolved in Release 4.6.2.

DDTS # CSCeb45064

Terminal loopback on DS3XM-6 card may not work properly. AIS-P may be transmitted towards the system (away from the line side) direction. A VT circuit newly created to the DS3XM-6 with no valid input signal to the port can cause this. A terminal loopback will not work because AIS-P is being transmitted towards the system direction. To avoid this issue, apply a valid signal to the input port for the DS3XM card for at least 10 seconds with no terminal or facility loopback applied to that particular port. After receiving a valid signal for this time period, the terminal loopback will function properly even if the input signal is disconnected from the DS3XM port. This issue is resolved in Release 4.6.

DDTS # CSCed05846

In Releases 4.0, 4.0.1, and 4.1 the standby TCC+, TCC2, or XTC card might reset automatically. This can occur at any time, but only rarely. This issue is resolved in Release 4.6, and maintenance releases 4.1.1 and 4.1.3.

Maintenance and Administration

DDTS # CSCed76192

If a host on the same Ethernet as a given NE sends ARP requests to the NE, with a source address that is in a restricted address range (see below), the NE might reboot and other cards in the shelf reset. The NE might become unmanageable under these circumstances. The NE will install an ARP entry for the illegal IP address, with the MAC supplied in the ARP request, thereby misrouting important addresses.

Restricted addresses are those in the loopback network, 127.0.0.0/8, in the multicast networks, 224.0.0.0/4, and in the cell bus network, 192.168.100.0/24.

The workaround is to ensure that no legitimate hosts have addresses in the illegal networks, and that no compromised hosts that might generate ARP attacks are on the Ethernet. This issue is resolved in Releases 4.0.3, 4.6.2, 4.1.5, and 5.0.

DDTS # CSCee35403

When more than one user is logged into an ONS 15454/15327 network, nodes cannot be removed or deleted from the domains at the network view. If a node is moved from a domain to the parent view, the node immediately returns to its original domain. Nodes will also not be deleted. After repeated effort this procedure can work, but results are sporadic and unpredictable. To work around this issue, disable the global update feature that will update every user logged into a network of nodes whenever one1 user makes a change. This can be done by placing an altered CTC.INI file on each user's workstation. The result is that only the user who makes a change will see the change. This issue is resolved in Release 4.6.2.

DDTS # CSCed53035

When you create a LOW (or EOW) circuit between the AIC LOW (or EOW) ports of two nodes, A and B, and then attempt to create a second LOW (or EOW) circuit between two optical ports (or one optical port and one AIC port) of Nodes A and B, you might be unable to create the second local (or express) orderwire circuit between the two nodes, even though the second one does not use any AIC local (or express) orderwire port (so the two circuits will not form a loop among AIC LOW/EOW ports).

Note The software design disallows two types of orderwire circuits that have the same sources and destinations on the same AIC ports of two such nodes, because this would create a loop by the point of the AIC orderwire ports.

If you need to create two of the same type of orderwire circuits between two nodes, you can create intranode (source/drop on the same node) circuits and connect them together to form the path. This issue is resolved in Release 4.6.2

Transmission Control Protocol Specification

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection might be automatically reestablished. In other cases, a user must repeat the action (for example, open a new Telnet or SSH session). Depending on the attacked protocol, a successful attack might have consequences beyond terminated connection that also must be considered. This attack vector is only applicable to those sessions that terminate on a device (such as a router, switch, or computer) and not to those sessions that only pass through the device (for example, transit traffic that is being routed by a router). Also, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products that contain TCP stack are susceptible to this vulnerability.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and describes the vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes the vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

This issue is resolved in Releases 2.3.5, 4.1.4 and 4.6.2.

DDTS # CSCed07126

If you provision a non-existent static route to a node's subnet and then delete it, the node will lose connectivity. If this occurs, remove and replace the Ethernet cable. This issue is resolved in Release 4.6.2.

DDTS # CSCea84427

CTC or Cisco Transport Manager (CTM) communication to a node might be lost while the node is still able to respond to a ping. The CORBA interface on the node can be locked by sending invalid (non-Corba) data to the TCC IIOP listener port. When the CORBA interface is locked, legitimate CORBA communications are lost. To prevent this from occurring, the ONS 15454 should be placed on a secure network or behind a firewall. In the event that this issue arises, CTC/CTM management can be regained by performing a Manual TCC reset using TL1. This issue is resolved in Release 4.6.

DDTS # CSCed58066

If a workstation running CTC has multiple NIC cards installed, and the primary NIC card is not used to connect to the node, and the node is unable to send IP packets to the IP address of the primary NIC card, or if the workstation running CTC is separated from the node by a router that performs NAT translation of the CTC workstation IP address, CTC repeatedly disconnects and reconnects (every two minutes). In either of these cases, CTC registers for alarms and provisioning updates using the IP address of the primary NIC, which the node cannot contact. When the node attempts to contact CTC, the connection fails. This causes the node to remove CTC from its list of registered clients. When CTC subsequently polls the node, CTC determines that it is not registered. CTC resets itself to ensure that it has current alarms and provisioning from the node, causing the disconnect and reconnect.

To avoid this issue, enable the proxy server on all LAN connected nodes with the Proxy-only configuration. This issue is resolved in Release 4.6.1.

DDTS # CSCed60557

Connecting two nodes with the same IP address to the same LAN will result in a broadcast storm. If this occurs, disconnect one of the nodes with the duplicate IP address. This issue is resolved in Release 4.6.1.

DDTS # CSCdw66895

XCVTs (both active and standby) reboot continuously when the K3 byte is mapped to the E2 byte on one side of a WTR span. The rebooting occurs after the WTR timer expires. This has been seen on a two fiber BLSR with OC-48AS. To avoid this issue, if possible, change the K3 mapping on both ends of the span before creating the ring; or, alternatively, you can prevent the ring from reverting during the K3 mapping by setting the Ring Reversion time to “never.” Once you have completed the mapping of the K3 byte to the E2 byte on both sides, return the Ring Reversion to its normal value. This issue is resolved in Release 4.6.

DDTS # CSCdz84149

If a user is logged into CTC as a superuser (or other higher level security type), and then another superuser changes the first user's security level to “retrieve” (or another lower level security type) without first logging the user out, the lower level user is then still able to perform some actions authorized only for the original login security level. For example, a “provisioning” level user demoted

to “retrieve” level in this manner can still provision and edit MS-SPRings (BLSRs) while logged into the current session, though the same user may no longer provision DCCs. To ensure that a user's level is changed completely, the superuser must log the user out prior to changing the security level. This issue is resolved in Release 4.6.

DDTS # CSCdz90753

In the Maintenance > Cross Connect Resource Pane, the VT matrix port detail is inconsistent with the general VT matrix data. This can occur when a 1+1 protection scheme is in place. To avoid confusion, note that the VT matrix data counts the VTs for both the working and protect card, while the detail data counts the VTs only for the working card. This issue is resolved in Release 4.6.

DDTS # CSCdz35479

Rarely, CTC Network view can freeze following the deletion or addition of a node from or to a BLSR/MS-SPRing. This can result in the CTC Network view no longer updating correctly. If this occurs, restart CTC. This issue is resolved in Release 4.6.

DDTS # CSCea92969

The switch indicator does not clear on the Maintenance > Protection tabs when a revertive 1:1 protection group is provisioned to be non-revertive. If this occurs, from the Maintenance > Protection tabs, select the slot with the “Switch” indicator. Click the “Clear” button. This issue is resolved in Release 4.6.

DDTS # CSCea93638

Path level alarms are displayed on the CTC conditions pane for deleted circuits. This issue may occur on any circuit deletion case. The conditions may be cleared by a TCC side switch. This issue is resolved in Release 4.6.

DDTS # CSCea61887

Terminal loopback is provisionable even if the card is in transponder mode.

To see this, in the provisioning tab for a G1000 or G1K-4 card pick a pair of ports and set them to transpond with each other. The condition also holds true by picking one port and setting it to transpond with itself (one-port unidirectional). Once the transponder setting is provisioned, go to the Maintenance tab and attempt to provision terminal loopback on any of the ports that were previously provisioned for transponder functionality. CTC allows terminal loopback to be provisioned even though the setting has no effect due to the fact that the ports are performing transponder functions. If terminal loopback is truly intended, you should remove the transponder settings. A warning stating that terminal loopback has no effect if transponders are present is displayed in Release 4.6.

DDTS # CSCea74000

Rarely, a PLM-P alarm on an OC-12 card might remain after deleting the affected STS-1 circuit. This condition persists even after deleting the affected card. If this occurs, you can reset the TCC2s to remove the stuck alarm. This issue is resolved in Release 4.6.

DDTS # CSCea71675

Rarely, when nodes appear gray in CTC and you view the BLSR tab at the network level, the tab may be blank. When this occurs, all tabs on the same level will also become blank. To avoid this issue, do not enter into the BLSR tab at the network view until all of the nodes are some color other than gray. This issue is resolved in Release 4.6.

DDTS # CSCeb24771

A static route may be lost if SOCKS proxy server mode is turned on and then off on the node. If the workstation was communicating with the NE using static routing it will lose connectivity to the NE. If this happens, re-enter the static route. This issue is resolved in Release 4.6.

DDTS # CSCeb20996

While using the orderwire capability of the AIC-I, you must not input a station number with less than 4 digits. If you enter, for example, 123, CTC will display 0123; however, you will not be able to ring the node by dialing either *123, or *0123. This issue is resolved in Release 4.6.

DDTS # CSCeb63327

The High Temperature Alarm is raised at 50 degrees Celsius. This is, however, not optimal on an Itemp rated system, which can tolerate up to 65 degrees Celsius. To work around this issue, the alarm can be downgraded or suppressed, but note that this will result in no temperature alarm provided at all. Alternatively, Cisco TAC provides a method of retrieving the temperature from the node, which can thus be monitored periodically for temperature-related problems. This issue is resolved in Release 4.6.

DDTS # CSCeb45149

A 1+1 non-revertive system in which the protect card is reseated while the working card is present and active reverts back to working after you clear a Force to Protect or Manual to Protect. Affected cards are OC-3 8 port and OC-12 4 port. To work around this issue, soft-reset the working card with the protect card present and active. This issue is resolved in Release 4.6.

DDTS # CSCec48038

A PCA circuit might be displayed as INCOMPLETE after a span upgrade; for example, when a BLSR span that is carrying PCA traffic is upgraded from OC-48 to OC-192. Although the circuit is reported as INCOMPLETE in CTC, traffic should be unaffected in this instance. To correct the display, restart CTC. This issue is resolved in Release 4.6.

DDTS # CSCec58326

When switching to the protect card in EC1 during 1:1 protection, IPPM goes blank. This is the result of incorrect handling of STS Path PMs (IPPM) in EC1 1:1 protection. This issue is resolved in Release 4.6.

DDTS # CSCec84338

With multiple unnamed circuits (circuit name listed as “Unknown”) on a node, where at least one is a path protection circuit, a cross-connect from one of these unnamed circuits will incorrectly appear on the Circuit Edit > UPSR Selectors, and Circuit Edit > UPSR Switch Counts tabs of the other unnamed circuits. Also, the State tab will show paths in the wrong column (for example, both source and destination in the CRS End B column).

This issue can manifest anytime you create multiple unnamed circuits (via TL1 or from CTC using the TL1-like option) on a node, where at least one is a path protection circuit. This issue is resolved in Release 4.6 and maintenance Releases 4.1.1 and 4.1.3.

DDTS # CSCeb63327

The High Temperature Alarm is raised at 50 degrees Celsius. This is not appropriate on an Itemp rated system, which can handle up to 65 degrees Celsius. The alarm can be downgraded or suppressed to work around the issue, but then no temperature alarm at all is provided. Cisco TAC is providing a method of retrieving the temperature from the node that enables you to periodically monitor temperature related problems. This issue is resolved in Release 4.6 and in maintenance Release 4.1.3.

DDTS # CSCeb34133

When provisioning a circuit as OOS, path level PM collecting is not disabled. To work around this issue, deselect the IPPM for the path. This issue is resolved in Releases 4.1.3 and 4.6.

DDTS # CSCeb34133

When provisioning a circuit as OOS, path level PM collecting is not disabled. To work around this issue, deselect the IPPM for the path. This issue is resolved in Releases 4.1.3 and 4.6.

DDTS # CSCeb84342

Occasionally, after both power sources are removed and plugged in with one power source (Battery A), the node reboots but does not raise PWR-B alarms. To correct this, remove PWR-B and plug it back. This issue is resolved in Releases 4.6 and 4.1.3.

DDTS # CSCec20521

After addition and deletion of a static route that overlaps with the internal IP addresses range, all cards in the shelf reboot. This can also happen after the node learns a similar route through OSPF or RIP updates. This issue is present in all releases through 4.1 and 4.5. To avoid this issue, do not provision static routes with a destination address in the subnet range 192.168.190.x, and avoid overlap between IP addresses in the network and the internal subnet range 192.168.190.x. If the issue does occur, reset your TCCs. This issue is resolved in Release 4.6 and in maintenance Release 4.1.3.

DDTS # CSCec16812

UNEQ-V alarms are incorrectly raised prior to connecting a TAP to a TACC, and also after disconnecting the TAP from the TACC. This issue is resolved in Releases 4.1.1, 4.1.3, and 4.6.

BLSR Functionality

DDTS # CSCdy56668

Ethernet circuits may appear in the CTC circuit table with an INCOMPLETE status after a BLSR/MSSP span is upgraded. The circuits, when this occurs, are not truly incomplete. They are unaffected and continue to carry traffic. To see the circuit status correctly, restart CTC. This issue is resolved in Release 4.6.

DDTS # CSCdy68207

Failing the working and protect spans on a four-fiber BLSR while an extra traffic circuit runs over the span and a lockout is on the span can cause the extra traffic to permanently fail, with no AIS.

The failure scenario is only reproducible by failing and restoring fibers in the following sequence.

Step 1 Create a four-fiber BLSR.

Step 2 Create extra traffic circuits (one or more) over one of the spans, say, from Node A east to Node B west. At Node A, issue a lockout span east. This causes the BLSR to not switch in the event of a span failure.

Step 3 At node A, remove the working transmit fiber east, then remove the protect transmit fiber east. Both protected traffic and extra traffic are down, as expected.

Step 4 Reinsert the protect transmit fiber east, then reinsert the working transmit fiber east. Protected traffic is restored, but extra traffic is not restored.

If this issue occurs, clear the lockout span. All extra traffic is immediately restored. You may then reissue the lockout span. This issue is resolved in Release 4.6.

DDTS # CSCec74273

If a four-fiber BLSR execute MS-R or WTR coexists with SF-P on the same span and FS-R is issued on a different span in the ring, the FS-R preempts the MS-R or WTR, causing a traffic outage. The ring switch is removed, but one side remains in the ring switch state. To recover from this situation, issue a lockout of the protect span on the span that raised the ring switch event. This issue is resolved in Release 4.6.

DDTS # CSCeb24331 and CSCeb40119

If you create a four-fiber BLSR with a VT circuit on it, then delete the circuit and the ring, then created a two-fiber BLSR on the same ports, you may see an unexpected AIS-V on the path, even before any additional circuit is created. A soft switch of the TCC will clear the AIS-V condition. This issue is resolved in Release 4.6.

DDTS # CSCeb40296

IPPM counts for PCA (extra) traffic will not be displayed in CTC if the BLSR switches back to working after a failure recovery. To see this issue, perform the following steps in a two-fiber or four-fiber BLSR configuration.

Step 1 Create a PCA circuit.

Enable IPPM on all OCn cards for this PCA circuit.

Step 2 Issue a Forced Switch Ring (FS-R) in CTC on the add or drop node. The BLSR switches.

Step 3 View the PCA path level counts shown in CTC.

Step 4 Clear the Forced Switch Ring in CTC. The BLSR switches back to working; however, IPPM path level counts for PCA circuits are not shown.

To recover from this situation, lock out the ring by issuing the LockoutOfProtection (LK-S) command on both east and west for all nodes in the ring. Reboot the OCn card that is not showing PCA path level counts. This procedure needs to be performed whenever there is a switch in BLSR configuration. This issue is resolved in Release 4.6.

DDTS # CSCeb40296

IPPM counts for PCA (extra) traffic will not be displayed in CTC if a BLSR ring-switches back to working after a failure recovery. To work around this issue, lockout the ring by issuing a LockoutOfProtection (LK-S) user command on both east and west on all the nodes in the ring. Reboot the OCn card that is not showing PCA path level counts. This procedure needs to be done whenever there is a switch in BLSR configuration. This issue is resolved in Releases 4.1.3 and 4.6.

Performance Monitoring

DDTS # CSCeb40296

IPPM counts for PCA (extra) traffic will not be displayed in CTC if a BLSR switches back to working after a failure recovery. To avoid this issue, lock out the ring by issuing the LockoutOfProtection (LK-S) user command on both east and west on all nodes in the ring. Reboot the OCn card that is not showing PCA path level counts. This procedure needs to be done whenever there is a switch in BLSR configuration. This issue is resolved in Release 4.6.

DDTS # CSCea38791

In the CTC Performance > Statistics tab of the G1000-4 or G1000-2, there are no entries for Rx/Tx Multicast and Broadcast packets. This issue is resolved in Release 4.6.

TL1

DDTS # CSCed18776

Issuing rtrv-pm-stsn and/or rtrv-th-stsn does not return the Pointer Justification (PJ) counts or thresholds respectively. This issue is resolved in Release 4.6.2.

DDTS # CSCed18776

Issuing rtrv-pm-stsn and/or rtrv-th-stsn does not return the Pointer Justification (PJ) counts or thresholds respectively. This issue is resolved in Release 4.6.2.

DDTS # CSCdz86121

In one rare case, the ONS 15454/15327 times out a user session without communicating the timeout to TL1. If this happens, the TL1 user remains logged in, although the session is actually timed out. This can occur when you log into the node with a timeout of X minutes. If the user session sits idle for all but 5 seconds of the X minutes, then you have only 5 seconds to type in a command to notify the node that the session is active. If you try this, you will likely miss the five second window, in which case the node will respond as though the session is inactive and deny access. However, because you have typed a key, irrespective of the five second window, TL1 responds as though the session is active and does not log you out (time out). You will not have access to the node and will receive a "DENY" response to TL1 commands. The error message may vary depending on commands issued. To recover from this situation, log out and log back in to TL1. This issue is resolved in Release 4.6.

DDTS # CSCec10357

Release 4.1 and 4.5 TL1 cannot display/retrieve/delete a DS3Xm VT Non-STS-1 cross-connection/circuit. This applies to ONS 15454s with DS3XM VT cross-connection provisioning via TL1, on any STS or port other than STS-1 or PORT-1, and with the AID format of:

```
VT1-Slot#-Sts#-Group#-Vt#
```

The cross-connection is provisioned as expected; however, the connection STS number in the TL1 VT AID format is always shown as "1" for the RTRV-CRS::ALL command and RTRV-CRS-VT1 with the AID used in the creation command (the non-one STS).

This issue has an impact on any DS3Xm VT connection deletion via TL1 where the STS number is not actually 1. The displayed VT1 AID cannot be used to retrieve the connection, and also cannot be used to delete the created connection. Also, the VT alarms/events/conditions on such a DS3XM VT circuit/connection will have the same AID issue: the StsNumber in the AID is always 1.

To work around this issue, delete the TL1-created DS3XM VT non-STS-1 cross-connection using the provisioned DS3XM VT AID (non-STS-1) or using CTC. There is no workaround for the alarm/event reporting for the non-STS-1 DS3XM VT circuit in the impacted releases (4.1 and 4.5). This issue is resolved in Release 4.6 and in maintenance Release 4.1.3.

New Features and Functionality

This section highlights new features and functionality for Release 4.6.x. For detailed documentation of each of these features, consult the user documentation.

New Hardware

FC_MR-4 Card

The FC_MR-4 (Fibre Channel 4-port) card uses pluggable Gigabit Interface Converters (GBICs) to transport non-SONET/SDH-framed, block-coded protocols over SONET/SDH in virtually concatenated or contiguously concatenated payloads. The FC_MR-4 can transport Fibre Channel over SONET/SDH using Fibre-Channel client interfaces and allows transport of one of the following at a time:

- Two contiguously concatenated (CCAT) STS-24c/VC4-8c circuits
- One STS-48c/VC4-16c CCAT
- Two virtually concatenated (VCAT) circuits (STC3c-8V/VC4-8v) compliant with ITU-T G.7041 GFP-T and Telcordia GR-253-CORE
- One STS-24c/VC4-8c CCAT and one STS-24c/VC4-8c VCAT

In Software Release 4.6.x, only two of the four ports can be active at one time.

For further specifications of this card, consult the *Cisco ONS 15454 Reference Guide, Release 4.6.*

10-Gbps Multirate Transponder Card

The Cisco ONS 15454 Multiservice Provisioning Platform (MSPP) support for a 10-Gbps multirate transponder card simplifies the integration and transport of 10 Gigabit Ethernet, OC-192, and STM-64 interfaces and services into enterprises or metropolitan and regional service provider networks. The 10-Gbps multirate transponder card can transport 10 Gigabit Ethernet, SONET OC-192, and SDH STM-64 services over a 100-GHz spaced, 50GHz stabilized, ITU-compliant wavelength. The transponder card is a plug-in module to the Cisco ONS 15454 MSPP, enabling a cost-effective architecture for delivering high-rate 10-Gbps services as well as low-rate services down to 1.5 Mbps. The 10-Gbps transponder card architecture contains a single client interface that is mapped to a single line interface, without accessing the Cisco ONS 15454 shelf cross-connect fabric.

The client interface supports 10 Gigabit Ethernet LAN physical layer (PHY), 10 Gigabit Ethernet WAN PHY, SONET OC-192, and SDH STM-64 signals. The interface to the client is a short-reach/intra-office, 1310-nm optical interface using LC connectors supporting fiber distances of up to 2 km (with or without the Y-protection option).

The line interface provides one 10-Gbps, long-reach, ITU-compliant, 100-GHz-spaced optical interface using LC connectors supporting OC-192, STM-64, 10 Gigabit Ethernet LAN PHY, or 10 Gigabit Ethernet WAN PHY interfaces. The DWDM output line interface is tunable across two adjacent 100-GHz wavelengths, enabling support for 32 channel DWDM networks via 16 discrete card types. Using amplification and dispersion compensation, the 10-Gbps transponder card is capable of a 300-km reach. When operated within the outlined specifications each card will transport the 10-Gbps signal with a maximum bit error rate (BER) of 10E-15.

The 10-Gbps transponder card incorporates both a client and DWDM line interface on the same card. The 10-Gbps transponder cards are deployable in the 12 multiservice interface card slots of the Cisco ONS 15454 platform, in systems with or without cross-connect cards. The addition of a cross-connect card enables the platform to support hybrid applications, containing transparent 10-Gbps services as well as aggregation of other services supported by the Cisco ONS 15454 platform. The only required common card is the appropriate timing, communications, and control card.

The 10-Gbps transponder card provides many carrier-class features and advanced capabilities necessary to deliver 10-Gbps services, including the protocol transparency, wavelength tunability, flexible protection mechanisms, flow-through timing, management, and performance monitoring capabilities.

For further specifications of this card, consult the *Cisco ONS 15454 Reference Guide, Release 4.6.*

4 x 2.5-Gbps Muxponder Card

The Cisco ONS 15454 Multiservice Provisioning Platform (MSPP) support for a 4x 2.5-Gbps muxponder card expands the Cisco ONS platform's OC-48/STM-16 interface density. The card enables the delivery of transparent 2.5-Gbps-based services for enterprises or metropolitan and regional service provider networks. The Cisco ONS 15454 MSPP 4x 2.5-Gbps muxponder card can transport four OC-48/STM-16 payloads over an OC-192/STM-64-based, 100-GHz spaced, 50GHz stabilized, ITU-compliant wavelength with provisionable digital wrapper (G.709) and selectable forward error correction (FEC). The muxponder card is a plug-in module to the Cisco ONS 15454 MSPP, enabling a high-density, cost-effective solution for OC-48/STM-16 services transport over a platform capable of low-rate services down to 1.5 Mbps. The muxponder card architecture contains four client interfaces that are mapped to a single line interface, without accessing the Cisco ONS 15454 shelf cross-connect fabric.

Each client interface provides a 2.488-Mbps (OC-48/STM-16) SONET/SDH interface via a small-form-factor-pluggable (SFP) optics module with LC connectors, providing the flexibility to support several optical reaches, including short-reach/intra-office, intermediate-reach/short-haul, and long-reach/long-haul, with support for qualified DWDM and DWDM SFP modules. The muxponder card supports any mixture of SFP reach types and also supports in-service insertion or removal without affecting other active ports.

The DWDM line interface provides one 9.95328-Gbps (OC-192/STM-64) or 10.70923-Gbps (OC-192/STM-64 with G.709 digital wrapper enabled), long-reach/long-haul, ITU-compliant, 100-GHz spaced optical interface using LC connectors supporting OC-48/STM-64 interfaces. The DWDM output line interface is tunable across two adjacent 100-GHz wavelengths, reducing inventories for spares. Using amplification and dispersion compensation, the muxponder card is capable of a 300-km reach. When operated within the outlined specifications, each card will transport the 10-Gbps signal with a maximum bit error rate (BER) of 10E-15.

The muxponder card incorporates the four clients and one DWDM line interface on the same card. The muxponder cards are deployable in the 12 multiservice interface card slots of the Cisco ONS 15454 platform, in systems with or without cross-connect cards. The addition of a cross-connect card enables the platform to support hybrid applications, containing transparent 2.5-Gbps services as well as aggregation of the other services supported by the Cisco ONS 15454 platform. The only other common card required for operation is the timing, communications, and control (TCC2) card. The muxponder card provides many carrier-class features and capabilities necessary to deliver 2.5-Gbps services, including selectable protocol transparency, wavelength tunability, flexible protection mechanisms, flexible timing options, and management capabilities.

For further specifications of this card, consult the *Cisco ONS 15454 Reference Manual, Release 4.6.*

New Software Features and Functionality

DWDM and TDM Hybrid Node Support

Hybrid Nodes Overview

A hybrid node running Release 4.6.x allows TDM cards and DWDM cards to be used in the same node, and is limited primarily by the slots available to the node. Hybrid functionality combines the abilities of nodes running software prior to Release 4.5 (in terms of tributary add/drop traffic including SONET,

SDH, and Ethernet incorporated into linear, ring, and PPMN topologies) with the Release 4.5 DWDM functionality, supporting additional hybrid node types, in open ring, closed ring, and linear configurations.

DWDM and TDM Hybrid Node Types

The node type in a network configuration is determined by the type of card that is installed in an ONS 15454 hybrid node. The ONS 15454 supports the following hybrid DWDM and TDM node types.

1+1 Protected Flexible Terminal Node

The 1+1 protected flexible terminal node is a single ONS 15454 node equipped with a series of OADM cards acting as a hub node configuration. This configuration uses a single hub or OADM node connected directly to the far-end hub or OADM node through four fiber links. This node type is used in a ring configured with two point-to-point links. The advantage of the 1+1 protected flexible terminal node configuration is that it provides path redundancy for 1+1 protected TDM networks (two transmit paths and two receive paths) using half of the DWDM equipment that is usually required.

Scalable Terminal Node

The scalable terminal node is a single ONS 15454 node equipped with a series of OADM cards and amplifier cards. This node type is more cost effective if a maximum of 16 channels are used. This node type does not support a terminal configuration exceeding 16 channels because the 32-channel terminal site is more cost effective for 17 channels and beyond.

The OADM cards that can be used in this type of node are: AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, and AD-1B-xx.x. You can also use AD-4B-xx.x and up to four 4MD-xx.x cards. The OPT-PRE and/or OPT-BST amplifiers can be used. The OPT-PRE or OPT-BST configuration depends on the node loss and the span loss. When the OPT-BST is not installed, the OSC-CSM must be used instead of the OSCM card.

Hybrid Terminal Node

A hybrid terminal node is a single ONS 15454 node equipped with at least one 32 MUX-O card, one 32 DMX-O card, two TCC2 cards, and TDM cards. If the node is equipped with OPT-PRE or OPT-BST amplifiers, it is considered an amplified terminal node. The node becomes passive if the amplifiers are removed. The hybrid terminal node type is based on the DWDM terminal node type (see the *Cisco ONS 15454 Reference Manual, R4.6*).

Hybrid OADM Node

A hybrid OADM node is a single ONS 15454 node equipped with at least one AD-xC-xx.x card or one AD-xB-xx.x card, and two TCC2 cards. The hybrid OADM node type is based on the DWDM OADM node type (see the *Cisco ONS 15454 Reference Manual, R4.6*). TDM cards can be installed in any available slot.

Hybrid Line Amplifier Node

A hybrid line amplifier node is a single ONS 15454 node with open slots for both TDM and DWDM cards.

Amplified TDM Node

An amplified TDM node is a single ONS 15454 node that increases the span length between two ONS 15454 nodes that contain TDM cards and optical amplifiers. There are three possible installation configurations for an amplified TDM node. Scenario 1 uses client cards and OPT-BST amplifiers. Scenario 2 uses client cards, OPT-BST amplifiers, OPT-PRE amplifiers, and FlexLayer filters. Scenario 3 uses client cards, OPT-BST amplifiers, OPT-PRE amplifiers, AD-1C-xx.x cards, and OSC-CSM cards.

The client cards that can be used in an amplified TDM node are: TXP_MR_10G, MXP_2.5G_10G, TXP_MR_2.5G, TXPP_MR_2.5G,

OC-192 LR/STM 64 ITU 15xx.xx, and OC-48 ELR/STM 16 EH 100 GHz.

Support for Hybrid Networks

The hybrid network configuration is determined by the type of node that is used in an ONS 15454 network. Along with TDM nodes, the ONS 15454 supports the following hybrid node types: 1+1 protected flexible terminal, scalable terminal, hybrid terminal, hybrid OADM, hybrid line amplifier, and amplified TDM. For examples and details of hybrid network types, see the *Cisco ONS 15454 Reference Manual, R4.6*.

FC_MR-4 Fiber Channel Card Support

The FC_MR-4 card reliably transports carrier-class, private-line Fibre Channel/FICON transport service. Each FC_MR-4 card can support up to two 1-Gbps circuits or a single 2-Gbps circuit. A 1-Gbps circuit is mapped to an STS-24c/VC4-8c (STS-3c-8v) and 2-Gbps circuits are mapped to an STS-48c/VC4-24c. The FC_MR-4 card incorporates features optimized for carrier-class applications such as:

- Carrier-class Fibre Channel/FICON
- 50 ms of failover via SONET/SDH protection as specified in Telcordia GR-253CORE
- Hitless software upgrades
- Remote Fibre Channel/FICON circuit bandwidth upgrades via integrated Cisco Transport Controller (CTC)
- Multiple management options through CTC, Cisco Transport Manager (CTM), TL1 (for SONET only), and Simple Network Management Protocol (SNMP)

The FC_MR-4 payloads can be transported over the following protected circuit types, in addition to unprotected circuits:

- path protection (CCAT circuits only)
- Path-protected mesh network (PPMN)
- BLSR
- Protection channel access (PCA)

The FC_MR-4 card supports high-order virtual concatenation (VCAT).

The FC_MR-4 uses pluggable GBICs for client interfaces and is compatible with the following GBIC types:

- ONS-GX-2FC-SML= (2Gb FC 1310nm Single mode with SC connectors)
- ONS-GX-2FC-MMI= (2Gb FC 850nm Multi mode with SC connectors)

Security Enhancements

The following security enhancements are added or updated in Release 4.6.x. For specific details on these enhancements, consult the *Cisco ONS 15454 SDH Reference Manual, Release 4.6.*

- Prevent password toggling
- Prevent account changes to logged in user

- Forced password change on next login
- Forced password change on first login
- Password aging
- Prevent password flipping
- LAN access security
- Disable inactive user

New Default Superuser Password

As of Release 4.6 the default password for a superuser when you first log onto a new node is changed. The new default is “otbu+1” consistently across all ONS 15454, ONS 15454 SDH, ONS 15600, and ONS 15327 platforms. This change does not affect users upgrading from a previous release, who will continue to use the password they have selected that is stored in their previous release's database.

GNE Load Balancing

Release 4.6.x provides fault tolerant GNE load balancing capability, allowing CTC to reach ENEs over multiple GNEs without the ENEs being advertised by the GNE over OSPF.

Automatic Laser Shutdown

Automatic Laser Shutdown (ALS) is a technique used to automatically shut down the output power of the transmitter in case of fiber break according to ITU-T G.664. If ALS is enabled, after at least 500 ms of continuous presence of an LOS defect, the transmitter is shut down. Once the ALS is engaged, a laser pulse is sent from the transmitter periodically in case of auto mode; or a single pulse is sent in case of manual mode for recovering from the fiber break.

Optical interfaces of ONS 15454 and ONS 15454 SDH support ALS, but due to hardware limitations of current optical cards, only OC192/STM64, OC48/STM16-ELR, and OC3/STM1-8 support the ALS feature.

The pulse recovery interval time for automatic restart is configurable within 60s and 300s. The default is 100s. The laser pulse recovery width is within 2s and 10s. This is to ensure proper operation of the ALS when connecting into long haul WDM systems. In some cases a pulse width of 2s is insufficient to consistently turn on all of the lasers in a given transmission path. In case of “manual restart for test” the pulse recovery width is 100s.

ALS is disabled by default in both the SONET and SDH implementations. The ALS can be disabled on each optical interface individually.

Configuration Management for Automatic Laser Shutdown

Release 4.6.x allows you to configure the following options on ALS for optical cards on a per port basis.

- Disabled
- Auto restart
- Manual restart
- Manual restart for test

Release 4.6.x allows you to configure the pulse recovery width between 2s and 10s, and the pulse recovery interval between 60s and 300s. The default values are set to 2s and 100s correspondingly on a per port basis.

Release 4.6.x allows you to send a restart command when manual restart or manual restart for test is chosen and ALS is engaged on a per optical card port basis.

DCC Capacity, Management, and Tunneling

With Release 4.6.x the TCC2 supports up to 68 SDCC or 28 LDCC terminations. The TCC2 supports mapping of any available SDCC to a GCC, up to the maximum SDCC count supported by the NE.

Note In practice, the maximum number of GCCs supported by the TCC2 is limited by the port density of G.709 cards.

Any optical port can be provisioned to use either SDCC or LDCC termination, with the exception of 4-port OC-3, which only supports SDCC.

SDCC and LDCC termination can coexist on the same fiber, in which case there is only one link created in the topology.

The TCC2 supports 32-bit HDLC CRC for SDCC and 16-bit HDLC CRC for LDCC termination.

The TCC2 supports provisioning of two types of DCC tunnel, hardware transparent and IP encapsulated. IP encapsulated is only supported for SDCC tunnel.

The TCC2 supports up to 68 DCC tunnels to carry foreign DCC traffic.

The TCC2 supports up to 10 IP encapsulated SDCC tunnels.

If an ONS node is acting as a hub node that interconnects with third party nodes in a path protection, and two tunnels are provisioned on the two path protection links, one ONS node can have 10/2 = 5 path protection rings.

Cisco recommends the total number of IP encapsulated tunnels in a DCC network be 64; however, this recommendation is not enforced by the NMS.

The number of path protection configurations supported is the maximum supported DCC terminations, divided by 2.

CTC Support

CTC supports provisioning of up to 68 SDCC terminations and 28 LDCC terminations per node.

CTC defaults the OSPF metric of an SDCC termination link to 100, and LDCC to 33.

CTC allows HDLC CRC provisioning for SDCC/LDCC termination to either 16-bit or 32-bit. For SDCC, the default is 32-bit; for LDCC, the default is 16-bit.

CTC issues a warning if both SDCC and LDCC are provisioned on the same port.

CTC supports provisioning of up to 68 DCC tunnels and 10 IP encapsulated tunnels per node.

CTC supports both transparent and IP encapsulated DCC tunnels. When creating a new tunnel you have the option of selecting whether to create a traditional (transparent) or IP encapsulated tunnel. You are prompted to pick the two end points and then the provisioning will be done on each end point node, and nodes along the path for the transparent tunnel. For the IP encapsulated tunnel, CTC supports provisioning of the throttling threshold, with 100% as the default. It is also possible to provision the maximum bandwidth of the IP encapsulated tunnel.

CTC supports upgrading an existing SDCC tunnel from transparent to IP encapsulated and vice versa.

If you have an SDCC tunnel between Node A and Node B, CTC allows you to select the tunnel and select to upgrade from transparent to IP encapsulated. CTC deletes the existing tunnel and create the terminations at the two end points for the IP encapsulated tunnel. Only tunnels that are in ACTIVE state are upgraded in this way. INCOMPLETE tunnels have the upgrade option disabled. You can also choose to manually delete the existing tunnel and then create an IP-encapsulated tunnel.

Alarms

With Release 4.6.x an LDCC failure alarm is raised when an LDCC termination fails.

Legacy DCC Tunneling Support

With Release 4.6.x you can select either Legacy DCC Tunneling or Encapsulated Tunneling as currently supported by your ONS system.

Go-and-Return Path Protection Routing

The go-and-return path protection routing option allows you to route the path protection working path on one fiber pair and the protect path on a separate fiber pair. The working path will always be the shortest path. If a fault occurs, neither the working nor the protection fibers are affected. This feature only applies to bidirectional path protection circuits. The go-and-return option appears on the Circuit Attributes panel of the Circuit Creation wizard.

BLSR Enhancements

BLSR Maximum Ring Support

Release 4.6.x BLSR supports a maximum of five rings per node, with maximums of five two-fiber, and one four-fiber ring per node.

BLSR 6 Character Ring ID

The name can be from 1 to 6 characters in length. Any alphanumeric string is permissible, and upper and lower case letters can be combined. Do not use the character string “All” in either upper or lower case letters, this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another BLSR.

CTC Enhancements

Performance Monitoring Enhancements for the FC_MR-4 Fiber Channel Card

CTC provides FC_MR-4 performance information, including line-level parameters, port bandwidth consumption, and historical statistics. The FC_MR-4 card performance information is divided into the Statistics, Utilization, and History tabbed windows within the card view Performance tab window.

FC_MR-4 Statistics Window

The statistics window lists parameters at the line level. The Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic

refresh occurs. The Statistics window also has a Clear button. The Clear button sets the values on the card to zero. All counters on the card are cleared. For specific parameters see the *Cisco ONS 15454 Reference Manual, R4.6*.

FC_MR-4 Utilization Window

The Utilization window shows the percentage of Tx and Rx line bandwidth used by the ports during consecutive time segments. The Utilization window provides an Interval menu that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day.

FC_MR-4 History Window

The History window lists past FC_MR-4 statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals.

Alarms Window

Path Width Column

In alarm windows, the display now includes a column called “Path Width”

that indicates how many STSs are contained in the alarmed path.

CTC Enhanced Alarm Severity Profiles

Card and Node View

With Release 4.6.x the profile name is more detailed for inherited profiles. Instead of “Inherited,” the name now offers descriptive information that gives you a better idea of where the severity values are derived from. For example, the name might say “Inherited from Node profile.”

Alarm Profile Editor in Card and Node Views

The “Alarm Profile Editor” tab has been added. You can create, download, clone, or delete alarm severity profiles now from the card view or node view in addition to the traditionally available network view capability.

Alarm Profile Editor, All Levels

The term “UNSET” has been replaced with “Use Default” to clarify where the severity value comes from.

If there is only one profile loaded, the store button is available and will autoselect that profile even if it is not selected.

Buttons have a horizontal layout.

There is a new check box option, “Only Show service-affecting severities.” If checked this box does as the description says. If unchecked, each cell shows the service-affecting/non-service-affecting severities, if applicable. For example, if a cell contains a Major severity, checking the box will show “MJ,” and unchecking the box will show “MJ/MN.”

Permanent profiles (for example, “Default” and “Inherited”) are not editable until the name is changed to a non-permanent-profile name.

Spanning Tree EtherBridge Circuits Window

Release 4.6.x allows you to manage spanning tree information more easily by providing the EtherBridge Circuits window. To see the window, in node view, click the Maintenance > EtherBridge > Circuits tabs.

In the EtherBridge Circuits window you can view the following information:

- Type—Identifies the type of Ethernet circuit mapped to the spanning tree, such as EtherSwitch point-to-point.
- Circuit Name/Port—Identifies the circuit name for the circuit in the spanning tree. This column also lists the Ethernet slots and ports mapped to the spanning tree for the node.
- STP ID—Shows the spanning tree protocol ID number.
- VLANS—Lists the VLANs associated with the circuit or port.

Context-Sensitive Help

With Release 4.6.x you can access context-sensitive help from any CTC window, dialog box, or wizard, affording you “What's this?” level information about CTC fields and table columns at the network, node, and card views.

Configurable Superuser Clear PM

On a configurable basis, where the current system behavior is the default, a superuser can configure the security level required to clear PMs. The ability to baseline PM remains unchanged. You can configure this feature in NE defaults.

PID/VID Visibility

With Release 4.6.x CTC, TL1, SNMP, and the interface to CTM display the PID/VID information programmed into all components with PID/VIDs.

This applies to all platforms where PID/VID is stored on the components.

Release 4.6.x supports setting the PID/VID in the factory.

Proxy ARP Enhancement

Release 4.6.x enhances the ARP proxy function to perform proxy ARP for all target addresses in the system's routing table (not just for the DCC connected devices).

SNMP GNE Proxy

With Release 4.6.x the TCC2 adds SNMP proxy capability for SNMP GET/SET commands and the responses to/from the ENE. The SNMP manager specifies the ENE address in the SNMP PDU, similar to the addressing for a shelf slot (for example, <GNE-community-string>{ENE-Address, ENE-community-string}).

K2 Bits Alarm Notification on 1+1 APS

With Release 4.6.x, K2 bits alarm notification on 1+1 APS supports uniform APS settings across your network. In the case, for example, where one ONS 15454/ONS 15454 SDH node is configured to have 1+1 APS protection on the OC-12 cards in Slots 1 and 2, and Slot 1 is connected to Slot 1 of another node that does not have APS 1+1 configured, an alarm will be raised to alert you to the incomplete provisioning.

Alarming on Duplicate Node IDs

A minor, non-service affecting (MN, NSA) alarm is raised if duplicate node names are detected when two nodes are in the same DCC area. The alarm clears when the duplicate node name is changed or the DCC link is broken.

Alarm on Firewall Turned Off

Release 4.6.x raises a transient condition when the firewall feature (proxy) is disabled after having been enabled.

Rear Panel Ethernet Connection Detach Alarm

The rear panel Ethernet connection detach alarm, when raised, indicates that the backplane LAN connection has been disconnected from a GNE. This allows detection of anyone trying to use the connection to access a corporate DCN.

- The alarm clears under the following conditions:
- The backplane LAN connection is connected or reconnected.
- The node is set to be an ENE

Note This has impacts on proxy/firewall, as well.

The NE default parameter for this option is set to “off” (by a superuser only).

Port Status via Front Panel LCD

Release 4.6.x introduces an enhancement to the fan tray LCD display/controls to increase visibility to the status of various ports on the NE. Prior to Release 4.6.x, a craft person local to the node could not determine which tributary OC-x port card was carrying traffic in a protection group. This enhancement will now allow a craft person determine which OC-x port cards are carrying traffic without having to log into CTC.

With Release 4.6.x, using the fan tray LCD buttons, you can drill down to specific slots and ports to display:

- The working/protect provisioned status of the OC-x port in a 1+1 or a 2F/4F BLSR configuration.
- The current active/standby line status of the OC-x port in a 1+1 or a 2F/4F BLSR configuration.

IP Tunnel Throttle Capability

An IP tunnel that will tunnel traffic from foreign nodes in the form of UDP-i packets can flood the network. With Release 4.6.x you can throttle these tunnels. You can set the throttle bandwidth percentage in a text field labeled Max Bandwidth when you create an IP tunnel using the wizard. Once an IP Tunnel is created you can also edit the tunnel and set the throttle bandwidth. Alternatively, when you are changing an IP Tunnel from SDCC (traditional) to IP Encapsulated, you can set the throttle bandwidth at that time.

ML-Series

VCAT

VCAT significantly improves the efficiency of data transport by grouping the synchronous payload envelopes (SPEs) of SONET/SDH frames in a nonconsecutive manner into VCAT groups. VCAT group circuit bandwidth is divided into smaller circuits called VCAT members. The individual members act as independent circuits. Intermediate nodes treat the VCAT members as normal circuits that are independently routed and protected by the SONET/SDH network. At the terminating nodes, these member circuits are multiplexed into a contiguous stream of data. VCAT avoids the SONET/SDH bandwidth fragmentation problem and allows finer granularity for provisioning of bandwidth services.

Note ML-Series cards purchased prior to Software Release 4.6 need to have the FPGA image upgraded to support the 4.6.x VCAT circuit feature. If a non-upgraded ML-Series card is used with Software Release 4.6.x, non-VCAT features will function normally, but a message will appear in the Cisco IOS CLI warning the user that the VCAT feature will not function with the current FPGA image. An upgraded FPGA image is compatible with all earlier versions of ML-Series card IOS software. Customers should contact TAC for instructions on performing the FPGA image upgrade.

SW-LCAS

LCAS increases VCAT flexibility by allowing the dynamic reconfiguration of VCAT groups without interrupting the operation of non-involved members. SW-LCAS is the software implementation of a LCAS-type feature. SW-LCAS differs from LCAS because it is not errorless and uses a different handshaking mechanism. SW-LCAS on the ML-Series card allows the automatic addition or removal of a VCAT group member in the event of a failure or recovery on two-fiber BLSR. The protection mechanism software operates based on ML-Series card link events. SW-LCAS allows service providers to configure VCAT member circuits on the ML-Series as protection channel access (PCA). This PCA traffic is dropped in the event of a protection switch, but is suitable for excess or noncommitted traffic and can double total available bandwidth on the circuit.

Microcode Image Enhancements

With Release 4.6.x you can choose from three microcode images for the ML-Series card. The default basic image has the same ML-Series base functionality as the Software Release 4.1 IOS image, Cisco IOS Release 12.1(19)EO, plus some additional non-microcode dependant R4.6.x features, such as the ML-Series virtual concatenation (VCAT) circuits. The basic image also allows users to upgrade from Software R4.0 or R4.1 to Software R4.6.x without changing the existing configurations on ML-Series cards.

Enhanced Performance Monitoring

Enhanced performance monitoring displays per-CoS packet statistics on the ML-Series card interfaces when CoS accounting is enabled. Per-CoS packet statistics are only supported for bridged services, not IP routing or MPLS. CoS-based traffic utilization is displayed at the FastEthernet or GigabitEthernet interface or subinterface (VLAN) level or the POS interface level but not at the POS subinterface level. RPR statistics are not available at the SPR interface level, but statistics are available for the individual POS ports that make up the SPR interface. EtherChannel (port-channel) and BVI statistics are available only at the member port level.

Combination VLAN-transparent Services and One or More VLAN-specific Services

In Software Release 4.6 and later, the ML-Series card supports combining VLAN-transparent services and one or more VLAN-specific services on the same port. All of these VLAN-transparent and VLAN-specific services can be point-to-point or multipoint-to-multipoint. This allows a service provider to combine a VLAN-transparent service, such as IEE 802.1Q tunneling (QinQ), with VLAN-specific services, such as bridging specific VLANs, on the same customer port. For example, one customer VLAN can connect to Internet access and the other customer VLANs can be tunneled over a single provider VLAN to another customer site, all over a single port at each site. VLAN-transparent service is also referred to as Ethernet Wire Service (EWS). VLAN-specific service is also referred to as Ethernet Relay Multipoint Service (ERMS).

Ethernet-over-MPLS (EoMPLS) Tunneling

EoMPLS provides Ethernet services across the MPLS backbone and core network. The ML series EoMPLS microcode image supports both VLAN and Port based point to point Ethernet tunnels across the MPLS network. The ML series EoMPLS feature enables Ethernet service delivery on the access SONET/SDH network over the RPR and transport that service across the core MPLS network without the need to create a separate bridged access network.

MST Protocol Tunneling

Release 4.6.x MST Protocol Tunneling allows Multi-Spanning-Tree on an external bridge to be used to enable a redundant pair of ML-series cards without requiring a spanning-tree instance per VLAN.

DS3i-N-12 Card Support for SONET Platforms

Release 4.6.x adds SONET support for the DS3i-N-12 card, as specified herein. For DS3i-N-12 card features and specifications, refer to the *Cisco ONS 15454 Reference Manual*, R4.6.

Compatibility and Interoperability

The DS3i-N-12 card is not compatible with the DS3 or the DS3E card. There is no in-service upgrade path from DS3 or DS3E to DS3i-N-12. Plugging a DS3i-N-12 card into a slot provisioned for DS3 will result in an MEA. Plugging a DS3 card into a slot provisioned for DS3i-N-12 will result in an MEA.

The DS3i-N-12 card operates with either the XC10G or the XCVT card. Future cross connect cards will be supported as they become available.

The DS3i-N-12 card operates with either the TCC+ or the TCC2 as the shelf controller as long as the particular type of TCC card is supported with the particular software release. Future shelf controller cards will be supported as they become available.

Caution Plugging a DS3i-N-12 card into a SONET chassis running a 4.0 or later software release that does not support the DS3i-N-12 will result in an MEA. On software releases prior to 4.0, the DS3i-N-12 card will continuously reboot without raising any alarm.

Circuit Provisioning

The following guidelines apply for circuit provisioning with the DS3i-N-12 card.

- A circuit from a DS3i-N-12 port to a DS3 port cannot be provisioned.

- A circuit from a DS3i-N-12 port on an ONS 15454 (SONET) node to a DS3i-N-12 port on another ONS 15454 node can be made.
- A circuit from a DS3i-N-12 port on an ONS 15454 (SONET) node to a DS3i-N-12 port on an ONS 15454 SDH node can be made, but there will be no end-to-end provisioning. The circuit must be provisioned in a two part process: The DS3i-N-12 to optical card is provisioned on the SONET side and the DS3i-N-12 to the corresponding SDH optical card is provisioned.
- You are only allowed to create STS3C circuits from/to the DS3i-N-12 card.
- There can only be four independent STS3C circuits provisioned from/to the DS3i-N-12 card.
- The ports used in each of the STS3C circuits are 1, 2, and 3; 4, 5, and 6; 7, 8, and 9; 10, 11, and 12.
- Each port on the DS3i-N-12 card can be provisioned independently in or out of service, but if less than three ports are used, the extra bandwidth is underutilized, because the STS3C will still be provisioned across the span cards.
- You cannot add or drop individual DS3 circuits out of the STS3C on intermediate nodes. To maximize bandwidth utilization, you must fill the STS3C at the circuit endpoints on the DS3i-N-12 cards by using the three contiguous DS3i-N-12 ports allocated to the particular STS3C.

Note When provisioning circuits in SDH to interoperate with SONET DS3i-N-12, you must create a VC4 containing VC3s as a payload in the exact order in which they will attach to port groups on the SONET side.

Protection Group Support

For SONET nodes, the DS3i-N-12 card supports 1:1 and 1:N where 1 <= N <= 5. Any DS3i-N-12 card can function as a protect card in a 1:N protection group. The working and protect slots follow the convention for other 1:1 and 1:N electrical protection groups.

For 1:1 protection:

- Slot 1 protects Slot 2
- Slot 3 protects Slot 4
- Slot 5 protects Slot 6
- Slot 13 protects Slot 12
- Slot 15 protects Slot 14
- Slot 17 protects Slot 16

For 1:N protection, the protect Slot 3 can protect Slots 1, 2, 4, 5, and 6; and protect Slot 15 can protect Slots 12, 13, 14, 16, and 17.

Mixed protection groups between DS3 and DS3i-N-12 cards are not supported.

Protection switching for 1:1 and 1:N meets required 60 ms switch times.

Switch times for XCVT or XC10G side switches meet required 60 ms switch times.

The current equipment protection behavior of switch, lock on, and lock out are supported.

Performance Monitoring Support

Release 4.6.x supports the following performance monitoring functions related to the DS3i-N-12.

- Enhanced DS3 PMs for C-bit and M13 framing mode are supported (similar to the DS3E cards).

- Automatic DS3 frame format detection is supported (similar to the DS3E card).
- Path level PMs are supported at the STS level similar to the current DS3 cards.
- Intermediate optical cards only support monitoring path level PMs on the STS3C circuit.
- Far end path PMs are supported at the STS level similar to the current DS3 cards.

Note The default DS3i-N-12 framing type (provisionable from the Maintenance > Provisioning tab) matches the default for SDH (in other words, it is C-bit).

Alarm Support

SD/SF BER calculation is performed at the DS3 line level (similar to the DS3 cards). SD/SF alarming occurs if the BER exceeds the provisioned SD, or SF thresholds, respectively. The SF alarm suppresses the reporting of the SD alarm.

The DS3i-N-12 card supports the standard DS3 alarms, LOS and LOF.

Path Trace Support

The DS3i-N-12 card supports setting and reading of a 16 or 64 byte J1 path trace string.

Intermediate monitoring of the J1 path trace by the optical cards is not supported.

On a path trace mismatch, the TIM-P alarm is raised.

Generation of AIS on TIM-P is user-provisionable as “on” or “off.”

Software Upgrade Support

Software upgrades are errorless for TCC2/XC10G systems.

Note If there is a DS3i-N-12 protection group, the protect card must be in the standby state before the software activation process.

CTC Support

In Release 4.6.x the column “Path Width” has been added to Alarms, Conditions and History panes. The Path Width column provides the width of the STS path on which the alarm is raised or cleared, in units of STS (how many STSs wide the path is). The path width only applies to the “STS-” alarmable object type. For any non-STS object, the column remains blank.

CTC also supports the following functionality for the DS3i-N-12 card for Release 4.6.x.

- Preprovisioning of a slot for DS3i-N-12
- Creating a 1:1 or 1:N protection group with DS3i-N-12, enforcing the limitations specified under the protection section
- Maintenance mode operations (loopbacks, protection switching, ports in and out of service, etc.)
- Shelf view and the card view display of a DS3i-N-12 card
- NE defaults for the DS3i-N-12 card on the SONET platform that match the defaults available on the SDH platform

New TL1 Features

The following TL1 features are new for Release 4.6.x. For detailed instructions on using TL1 commands, consult the *TL1 Command Guide* for Release 4.6.

Functional Differences

FC-MR-4

The FC-MR-4 card is added in Release 4.6.x.

VCAT

VCAT/CCAT circuit provisioning is allowed from Release 4.6.x. Currently it is supported only on ML-series cards.

BLSR

Six character ring IDs are supported in BLSR/MSSP Rings.

Alarms

SF/SD alarms are supported on all electric cards. SFBER and SDBER parameters are introduced in the ED-T1, ED-T3, ED-EC1, and ED-DS3I commands.

Alarm on Fire wall can be turned On/Off using ALW-MSG-ALL/INH-MSG-ALL commands.

STS/VT cross-connections can now be retrieved at NE/Card/Port/Path level using new commands RTRV-STS and RTRV-VT.

TL1 Security Enhancements

The following security enhancements are available in Release 4.6.x

- The RTRV-USER-STATUS command is used to retrieve a list of logged in users.
- The reuse of old passwords is prevented for a specified amount of time. After that time has elapsed the old password can be reused again. A user may retrieve this value with the RTRV-USER-SECU command.
- The SET-ATTR-SECUDFLT command is used to set the POINT (Password Obsolescence Interval) value.
- The REPT^EVT^SESSION is used to indicate that the password needs to be updated.
- User can retrieve password aging interval with the RTRV-USER-SECU command.
- The INH-USER-SECU command is used to disable a userid. The ALW-USER-SECU command enables the userid.
- The REPT^EVT^SECU autonomous message is used to notify a superuser when a user has logged in to the NE.
- The CANC-USER-SECU command is used by a superuser to forcibly logout a user.
- The RTRV-USER-STATUS command is used to determine which userids are locked out.

TL1 Additional Support Added

Optical PMs and ALS support is added in OC3-8 card.

Test Access support is added for SDH cards.

OPR/RLS-PROTNSW-<mod2> and EX-SW commands support <dirn> parameter.

Program ID and Version ID of all components which have PID/VID programmed in them are now displayed in RTRV-INV command's response.

COPY-RFILE is enhanced to perform Database backup and restore.

INIT-REG command can now clear individual montypes.

TL1 Commands Added

The following commands were added in Release 4.6:

- CANC-USER-SECU
- CHG-ACCMD-DS3I
- CONN-TACC-DS3I
- ED-CMD-SECU
- ED-DS3I
- ED-FC
- ED-NE-PATH
- ED-OCN-TYPE
- INIT-REG-DS3I
- INIT-REG-FC
- OPR-LPBK-DS3I
- RLS-LPBK-DS3I
- RLS-LPBK-E43
- RMV-DS3I
- RMV-FC
- RST-DS3I
- RST-FC
- RTRV-ALM-DS3I
- RTRV-ALM-FC
- RTRV-ALMTH-EQPT
- RTRV-ALMTH-OC3
- RTRV-COND-DS3I
- RTRV-COND-FC
- RTRV-DFLT-SECU
- RTRV-DS3I
- RTRV-FC

- RTRV-NE-PATH
- RTRV-PM-DS3I
- RTRV-PMSCHED-DS3I
- RTRV-STS
- RTRV-TH-ALL
- RTRV-TH-DS3I
- RTRV-VT
- SCHED-PMREPT-DS3I
- SET-ALMTH-EQPT
- SET-ALMTH-OC3
- SET-ATTR-SECUDFLT
- SET-TH-DS3I

TL1 Commands Enhanced

ENT-EQPT and ED-EQPT were enhanced to add the CMDMDE name/value parameter

ENUM Differences

ALL_MONTYPE enum items dropped from Release 4.5:

- ALL Montype enum items are now directly fetched from tcadefs.h - refer to Release 4.6_PM_Diff.html document.

ALL_MONTYPE enum items added to Release 4.6:

- ALL_MONTYPE_ALL_PM => “ALL”

ALL_MONTYPE is used in the following commands:

- INIT-REG-MOD2
- RTRV-PM-MOD2
- RTRV-TH-ALL
- RTRV-TH-MOD2
- SET-TH-MOD2

ALL_THR enum items dropped from Release 4.5:

- ALL Threshold enum items are now directly fetched from tcadefs.h from Release 4.6.

ALM_THR enum items added to Release 4.6:

- ALM_THR_BATV_EHIGH => “BATV-EHIGH”
- ALM_THR_BATV_ELOW => “BATV-ELOW”
- ALM_THR_BATV_HIGH => “BATV-HIGH”
- ALM_THR_BATV_LOW => “BATV-LOW”
- ALM_THR_LAT_HIGH => “LAT-HIGH”
- ALM_THR_LAT_LOW => “LAT-LOW”

- ALM_THR_LBCL_LOW => “LBCL-LOW”
- ALM_THR_RXT_HIGH => “RXT-HIGH”
- ALM_THR_RXT_LOW => “RXT-LOW”
- ALM_THR_XCVR_HIGH => “XCVR-HIGH”
- ALM_THR_XCVR_LOW => “XCVR-LOW”

ALM_THR is used in the following commands:

- RTRV-ALMTH-MOD2O
- RTRV-ALMTH-OC3
- RTRV-ALMTH-OTS
- SET-ALMTH-MOD2O

CRS_TYPE enum items added to Release 4.6:

- CRS_TYPE_VT1 => “VT1”

CRS_TYPE is used in the following commands:

- RTRV-CRS

DATARATE enum items added to Release 4.6:

- DATARATE_DR_FC => “FC”
- DATARATE_DR_GIG_E => “GIG_E”
- DATARATE_DR_PASS_THRU => “PASS_THRU”
- DATARATE_DR_TEN_GIG_E => “TEN_GIG_E”

DATARATE is UNUSED in any command.

DS_LINE_TYPE enum items added to Release 4.6:

- DS_LINE_TYPE_LT_AUTO_PROV => “AUTO-PROV”

DS_LINE_TYPE is used in the following commands:

- ED-DS3I
- ED-T3
- RTRV-DS3I
- RTRV-T3

DWDM_RING_TYPE enum items added to Release 4.6:

- DWDM_RING_TYPE_NOT_DWDM => “NOT-DWDM”

DWDM_RING_TYPE is used in the following commands:

- ED-WDMANS
- RTRV-WDMANS

EQPT_TYPE enum items dropped from Release 4.5:

- EQPT_TYPE_EQPT_ID_DS1N_14 => “DS1N-14”
- EQPT_TYPE_EQPT_ID_DS1_14 => “DS1-14”
- EQPT_TYPE_EQPT_ID_DS3ATM_12 => “DS3ATM-12”
- EQPT_TYPE_EQPT_ID_DS3CR_12 => “DS3CR-12”
- EQPT_TYPE_EQPT_ID_DS3E_12 => “DS3E-12”

- EQPT_TYPE_EQPT_ID_DS3NE_12 => “DS3NE-12”
- EQPT_TYPE_EQPT_ID_DS3N_12 => “DS3N-12”
- EQPT_TYPE_EQPT_ID_DS3XM_6 => “DS3XM-6”
- EQPT_TYPE_EQPT_ID_DS3_12 => “DS3-12”
- EQPT_TYPE_EQPT_ID_E1000T_2 => “E1000T-2”
- EQPT_TYPE_EQPT_ID_E100T_12 => “E100T-12”
- EQPT_TYPE_EQPT_ID_E327_4 => “E100T-4”
- EQPT_TYPE_EQPT_ID_EC1N_12 => “EC1N-12”
- EQPT_TYPE_EQPT_ID_EC1_12 => “EC1-12”
- EQPT_TYPE_EQPT_ID_MIC_GEN => “MIC-GEN”
- EQPT_TYPE_EQPT_ID_OC12_327 => “OC12-327”
- EQPT_TYPE_EQPT_ID_OC3ATM_IR_6 => “OC3ATM-IR-6”
- EQPT_TYPE_EQPT_ID_OC3POS_SR_4 => “OC3POS-SR-4”
- EQPT_TYPE_EQPT_ID_OC3_327 => “OC3-327”
- EQPT_TYPE_EQPT_ID_OC48_327 => “OC48-327”
- EQPT_TYPE_EQPT_ID_XC_VT => “XC-VT”

EQPT_TYPE enum items added to Release 4.6:

- EQPT_TYPE_EQPT_ID_DS1N_14 => “DS1N”
- EQPT_TYPE_EQPT_ID_DS1_14 => “DS1”
- EQPT_TYPE_EQPT_ID_DS3E_12 => “DS3E”
- EQPT_TYPE_EQPT_ID_DS3NE_12 => “DS3NE”
- EQPT_TYPE_EQPT_ID_DS3N_12 => “DS3N”
- EQPT_TYPE_EQPT_ID_DS3XM_6 => “DS3XM”
- EQPT_TYPE_EQPT_ID_DS3_12 => “DS3”
- EQPT_TYPE_EQPT_ID_E1000T_2 => “E1000T”
- EQPT_TYPE_EQPT_ID_E100T_12 => “E100T”
- EQPT_TYPE_EQPT_ID_E327_4 => “E100T”
- EQPT_TYPE_EQPT_ID_EC1N_12 => “EC1N”
- EQPT_TYPE_EQPT_ID_EC1_12 => “EC1”
- EQPT_TYPE_EQPT_ID_FCMR => “FC-MR-4”
- EQPT_TYPE_EQPT_ID_MIC_GEN => “MIC”
- EQPT_TYPE_EQPT_ID_OC12_327 => “OC12”
- EQPT_TYPE_EQPT_ID_OC3_327 => “OC3”
- EQPT_TYPE_EQPT_ID_OC48_327 => “OC48”
- EQPT_TYPE_EQPT_ID_TSC => “TSC”
- EQPT_TYPE_EQPT_ID_XC_VT => “XCVT”

EQPT_TYPE is used in the following commands:

- INIT-REG-OTS

EQUIPMENT_TYPE enum items added to Release 4.6:

- EQUIPMENT_TYPE_ET_FC_MR_4 => “FC-MR-4”

EQUIPMENT_TYPE is used in the following commands:

- ENT-EQPT

FC_LINKRATE enum items added to Release 4.6:

- FC_LINKRATE_1GFC => “1GFC”
- FC_LINKRATE_2GFC => “2GFC”
- FC_LINKRATE_UNKNOWN => “UNKNOWN”
- FC_LINKRATE_UNPLUGGED => “UNPLUGGED”

FC_LINKRATE is used in the following commands:

- RTRV-FC

FRAME_FORMAT enum items added to Release 4.6:

- FRAME_FORMAT_LT_BITS_2MHZ => “BITS-2MHZ”
- FRAME_FORMAT_LT_BITS_64K => “BITS-64K”

FRAME_FORMAT is used in the following commands:

- ED-BITS
- ED-T1
- RTRV-BITS
- RTRV-T1

IMPEDANCE enum items added to Release 4.6:

- None

IMPEDANCE is used in the following commands:

- ED-BITS
- RTRV-BITS

LINE_CODE enum items added to Release 4.6:

- LINE_CODE_LC_HDB3 => “HDB3”

LINE_CODE is used in the following commands:

- ED-BITS
- ED-T1
- RTRV-BITS
- RTRV-T1

LPBK_TYPE enum items added to Release 4.6:

- LPBK_TYPE_LINE_LPBK => “LINE”

LPBK_TYPE is used in the following commands:

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

MOD2 enum items added to Release 4.6:

- MOD2_M2_DS3I => “DS3I”

- MOD2_M2_EQPT => “EQPT”
- MOD2_M2_FC => “FC”
- MOD2_M2_STS => “STS”
- MOD2_M2_VT => “VT”

MOD2 is used in the following commands:

- RTRV-LNK-OTS
- RTRV-NE-WDMANS
- RTRV-PMSCHED-ALL
- RTRV-TRC-CLNT
- RTRV-TRC-OCH

MOD2ALM enum items added to Release 4.6:

- MOD2ALM_M2_DS3I => “DS3I”
- MOD2ALM_M2_FC => “FC”

MOD2ALM is used in the following commands:

- RTRV-ALM-WLEN
- RTRV-COND-WLEN

MOD2B enum items added to Release 4.6:

- MOD2B_M2_DS3I => “DS3I”
- MOD2B_M2_FC => “FC”

MOD2B is used in the following commands:

- 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-TH-ALL

MOD2O enum items added to Release 4.6:

- MOD2O_M2_EQPT => “EQPT”
- MOD2O_M2_OC3 => “OC3”

MOD2O is used in the following commands:

- RTRV-ALMTH-OC3
- RTRV-ALMTH-OTS

MOD2_IO enum items added to Release 4.6:

- MOD2_IO_M2_DS3I => “DS3I”
- MOD2_IO_M2_FC => “FC”

MOD2_IO is used in the following commands:

- None

MOD_PATH enum items added to Release 4.6:

- None

MOD_PATH is used in the following commands:

- RTRV-CRS
- RTRV-STS9C
- RTRV-TRC-OC48

MOD_PORT enum items dropped from Release 4.5:

- MOD_PORT_M2_EC1 => “EC1”
- MOD_PORT_M2_G1000 => “G1000”
- MOD_PORT_M2_OC12 => “OC12”
- MOD_PORT_M2_OC192 => “OC192”
- MOD_PORT_M2_OC3 => “OC3”
- MOD_PORT_M2_OC48 => “OC48”
- MOD_PORT_M2_T1 => “T1”
- MOD_PORT_M2_T3 => “T3”

MOD_PORT is used in the following commands:

- None.

OPTICAL_BAND enum items dropped from Release 4.5:

- OPTICAL_BAND_BN_UNKNOWN => “USE-DEFAULT”

OPTICAL_BAND enum items added to Release 4.6:

- OPTICAL_BAND_BN_UNKNOWN => “UNKNOWN”

OPTICAL_BAND is used in the following commands:

- ED-OMS
- RTRV-LNK-OTS
- RTRV-OMS

OPTICAL_LINK_TYPE enum items added to Release 4.6:

- OPTICAL_LINK_TYPE_OL_HITLESS_OCH => “HITLESS-OCH”
- OPTICAL_LINK_TYPE_OL_HITLESS_OMS => “HITLESS-OMS”
- OPTICAL_LINK_TYPE_OL_OCH => “OCH”
- OPTICAL_LINK_TYPE_OL_OMS => “OMS”

OPTICAL_LINK_TYPE is used in the following commands:

- RTRV-LNK-MOD2LNK
- RTRV-LNK-OTS

REVERTIVE_TIME enum items added to Release 4.6:

- REVERTIVE_TIME_RT_0 => “0.0”

REVERTIVE_TIME is used in the following commands:

- ED-BLSR
- ED-EQPT
- ED-FFP-CLNT
- ED-FFP-OCH
- ED-FFP-OCN-TYPE
- ED-NE-SYNCN
- ED-STS-PATH
- ED-VT-PATH
- ED-VT1
- ENT-BLSR
- ENT-EQPT
- ENT-FFP-CLNT
- ENT-FFP-OCN-TYPE
- RTRV-BLSR
- RTRV-EQPT
- RTRV-FFP-CLNT
- RTRV-FFP-OC48
- RTRV-FFP-OCH
- RTRV-NE-SYNCN
- RTRV-STS9C
- RTRV-VT1

SA_BIT enum items added to Release 4.6:

- SA_BIT_SA_BYTE_4 => “BYTE-4”
- SA_BIT_SA_BYTE_5 => “BYTE-5”
- SA_BIT_SA_BYTE_6 => “BYTE-6”
- SA_BIT_SA_BYTE_7 => “BYTE-7”
- SA_BIT_SA_BYTE_8 => “BYTE-8”

SA_BIT is used in the following commands:

- ED-BITS
- RTRV-BITS

SST enum items added to Release 4.6:

- SST_SS_UNKNOWN => “UNKNOWN”

SST is used in Most ED/RTRV commands.

STS_PATH enum items dropped from Release 4.5:

- STS_PATH_STS1 => “STS1”
- STS_PATH_STS12C => “STS12C”
- STS_PATH_STS192C => “STS192C”
- STS_PATH_STS24C => “STS24C”

- STS_PATH_STS3C => “STS3C”
- STS_PATH_STS48C => “STS48C”
- STS_PATH_STS6C => “STS6C”
- STS_PATH_STS9C => “STS9C”

STS_PATH is used in the following commands:

- RTRV-CRS-STS9C
- RTRV-STS9C
- RTRV-TRC-OC48

TACC_MODE enum items added to Release 4.6:

- TACC_MODE_SPLTAB => “SPLTAB”

TACC_MODE is used in the following commands:

- CHG-ACCMD-MOD-TACC
- CONN-TACC-MOD-TACC
- RTRV-TACC

TAPTYPE enum items added to Release 4.6:

- TAPTYPE_DUAL => “DUAL”
- TAPTYPE_SINGLE => “SINGLE”

TAPTYPE is used in the following commands:

- ED-DS1
- ED-DS3I
- ED-STS-PATH
- ED-T1
- ED-T3
- ED-VT-PATH
- RTRV-DS1
- RTRV-DS3I
- RTRV-STS9C
- RTRV-T1
- RTRV-T3

TRCMODE enum items added to Release 4.6:

- TRCFORMAT_16_BYTE => “16-BYTE”
- TRCFORMAT_1_BYTE => “1-BYTE”
- TRCFORMAT_64_BYTE => “64-BYTE”

TRCMODE is used in the following commands:

- ED-STS-PATH
- ED-TRC-CLNT
- ED-TRC-OCH
- RTRV-STS9C

- RTRV-TRC-CLNT
- RTRV-TRC-OC48
- RTRV-TRC-OCH

USER_LOGINS enum items added to Release 4.6:

- USER_LOGINS_MULTIPLE => “MULTIPLE”
- USER_LOGINS_SINGLE => “SINGLE”

USER_LOGINS is used in the following commands:

- SET-ATTR-SECUDFLT

WDM enum items dropped from Release 4.5:

- TRCFORMAT_16_BYTE => “16-BYTE”
- TRCFORMAT_1_BYTE => “1-BYTE”
- TRCFORMAT_64_BYTE => “64-BYTE”
- WDM_WDM_CLNT => “CLNT”
- WDM_WDM_OCH => “OCH”
- WDM_WDM_OMS => “OMS”
- WDM_WDM_OTS => “OTS”

WDM is UNUSED in any command.

COMMAND Syntax Changes

The syntax of the following commands was changed from Release 4.5 to Release 4.6:

CONN-TACC-DS1 syntax changed:

CONN-TACC-DS1[:<TID>]:<aid>:<CTAG>[::<tap>]:MD=<md>;

CONN-TACC-DS1[:<TID>]:<aid>:<CTAG>::<tap>:MD=<md>;

CONN-TACC-STS1 syntax changed:

CONN-TACC-STS1[:<TID>]:<aid>:<CTAG>[::<tap>]:MD=<md>;

CONN-TACC-STS1[:<TID>]:<aid>:<CTAG>::<tap>:MD=<md>;

CONN-TACC-STS12C syntax changed:

CONN-TACC-STS12C[:<TID>]:<aid>:<CTAG>[::<tap>]:MD=<md>;

CONN-TACC-STS12C[:<TID>]:<aid>:<CTAG>::<tap>:MD=<md>;

CONN-TACC-STS192C syntax changed:

CONN-TACC-STS192C[:<TID>]:<aid>:<CTAG>[::<tap>]:MD=<md>;

CONN-TACC-STS192C[:<TID>]:<aid>:<CTAG>::<tap>:MD=<md>;

CONN-TACC-STS24C syntax changed:

CONN-TACC-STS24C[:<TID>]:<aid>:<CTAG>[::<tap>]:MD=<md>;

CONN-TACC-STS24C[:<TID>]:<aid>:<CTAG>::<tap>:MD=<md>;

CONN-TACC-STS3C syntax changed:

CONN-TACC-STS3C[:<TID>]:<aid>:<CTAG>[::<tap>]:MD=<md>;

CONN-TACC-STS3C[:<TID>]:<aid>:<CTAG>::<tap>:MD=<md>;

CONN-TACC-STS48C syntax changed:

CONN-TACC-STS48C[:<TID>]:<aid>:<CTAG>[::<tap>]:MD=<md>;

CONN-TACC-STS48C[:<TID>]:<aid>:<CTAG>::<tap>:MD=<md>;

CONN-TACC-STS6C syntax changed:

CONN-TACC-STS6C[:<TID>]:<aid>:<CTAG>[::<tap>]:MD=<md>;

CONN-TACC-STS6C[:<TID>]:<aid>:<CTAG>::<tap>:MD=<md>;

CONN-TACC-STS9C syntax changed:

CONN-TACC-STS9C[:<TID>]:<aid>:<CTAG>[::<tap>]:MD=<md>;

CONN-TACC-STS9C[:<TID>]:<aid>:<CTAG>::<tap>:MD=<md>;

CONN-TACC-T1 syntax changed:

CONN-TACC-T1[:<TID>]:<aid>:<CTAG>[::<tap>]:MD=<md>;

CONN-TACC-T1[:<TID>]:<aid>:<CTAG>::<tap>:MD=<md>;

CONN-TACC-T3 syntax changed:

CONN-TACC-T3[:<TID>]:<aid>:<CTAG>[::<tap>]:MD=<md>;

CONN-TACC-T3[:<TID>]:<aid>:<CTAG>::<tap>:MD=<md>;

CONN-TACC-VT1 syntax changed:

CONN-TACC-VT1[:<TID>]:<aid>:<CTAG>[::<tap>]:MD=<md>;

CONN-TACC-VT1[:<TID>]:<aid>:<CTAG>::<tap>:MD=<md>;

COPY-IOSCFG syntax changed:

COPY-IOSCFG[:<TID>]:<src>:<CTAG>::SRC=<src1>,DEST=<dest>;

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

COPY-RFILE syntax changed:

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

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

DLT-EQPT syntax changed:

DLT-EQPT[:<TID>]:<aid>:<CTAG>[:::];

DLT-EQPT[:<TID>]:<tap>:<CTAG>;

DLT-UCP-CC syntax changed:

DLT-UCP-CC[:<TID>]:<aid >:<CTAG>[::::];

DLT-UCP-CC[:<TID>]:<aid>:<CTAG>[::::];

ED-BITS syntax changed:

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

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

ED-CLNT syntax changed:

ED-CLNT[:<TID>]:<aid>:<CTAG>[:::NAME=<portname>,][SFBER=<sfber>,][SDBER=<sdber>,][ALSMODE=<alsmode>,][ALSRCINT=<alsrcint>,][ALSRCPW=<alsrcpw>,][COMM=<comm>,][MACADDR=<macaddr>,][SYNCMSG=<syncmsg>,][SENDDUS=<senddus>,][RLASER=<rlaser>,][SOAK=<soak>][:<pst>,][<sst>];

ED-CLNT[:<TID>]:<aid>:<CTAG>[:::NAME=<portname>,][SFBER=<sfber>,][SDBER=<sdber>,][ALSMODE=<alsmode>,][ALSRCINT=<alsrcint>,][ALSRCPW=<alsrcpw>,][COMM=<comm>,][MACADDR=<macaddr>,][SYNCMSG=<syncmsg>,][SENDDUS=<senddus>,][RLASER=<rlaser>,][SOAK=<soak>,][OSPF=<ospf>][:<pst>,][<sst>];

ED-DS1 syntax changed:

ED-DS1[:<TID>]:<aid>:<CTAG>[:::TACC=<tacc>];

ED-DS1[:<TID>]:<aid>:<CTAG>[:::TACC=<tacc>,][TAPTYPE=<taptype>];

ED-EQPT syntax changed:

ED-EQPT:[<TID>]:<aid>:<CTAG>:::[PROTID=<protid>,][PRTYPE=<prtype>,][RVRTV=<rvrtv>,][RVTM=<rvtm>][:];

ED-EQPT:[<TID>]:<aid>:<CTAG>:::[PROTID=<protid>,][PRTYPE=<prtype>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][CMDMDE=<cmdmde>][:];

ED-NE-SYNCN syntax changed:

ED-NE-SYNCN[:<TID>]::<CTAG>[:::TMMD=<tmmd>,][SSMGEN=<ssmgen>,][QRES=<qres>,][RVRTV=<rvrtv>,][RVTM=<rvtm>];

ED-NE-SYNCN[:<TID>]::<CTAG>;

ED-OCH syntax changed:

ED-OCH[:<TID>]:<aid>:<CTAG>[:::RDIRN=<rdirn>,][EXPWLEN=<expwlen>,][VOAATTN=<voaattn>,][VOAPWR=<voapwr>,][CALOPWR=<calopwr>,][CHPOWER=<chpower>,][NAME=<portname>,][SFBER=<sfber>,][SDBER=<sdber>,][ALSMODE=<alsmode>,][ALSRCINT=<alsrcint>,][ALSRCPW=<alsrcpw>,][COMM=<comm>,][GCCRATE=<gccrate>,][OSFBER=<sfber>,][OSDBER=<sdber>,][DWRAP=<drwap>,][FEC=<fec>,][MACADDR=<macaddr>,][SYNCMSG=<syncmsg>,][SENDDUS=<senddus>,][RLASER=<rlaser>,][SOAK=<soak>][:<pst>,][<sst>];

ED-OCH[:<TID>]:<aid>:<CTAG>[:::RDIRN=<rdirn>,][EXPWLEN=<expwlen>,][VOAATTN=<voaattn>,][VOAPWR=<voapwr>,][CALOPWR=<calopwr>,][CHPOWER=<chpower>,][NAME=<portname>,][SFBER=<sfber>,][SDBER=<sdber>,][OSDBER=<sdber>,][ALSMODE=<alsmode>,][ALSRCINT=<alsrcint>,][ALSRCPW=<alsrcpw>,][COMM=<comm>,][GCCRATE=<gccrate>,][DWRAP=<drwap>,][FEC=<fec>,][MACADDR=<macaddr>,][SYNCMSG=<syncmsg>,][SENDDUS=<senddus>,][RLASER=<rlaser>,][SOAK=<soak>,][OSPF=<ospf>][:<pst>,][<sst>];

ED-OTS syntax changed:

ED-OTS[:<TID>]:<aid>:<CTAG>[:::RDIRN=<rdirn>,][VOAATTN=<voaattn>,][VOAPWR=<voapwr>,][CALOPWR=<calopwr>,][CALTILT=<caltilt>,][OSRI=<osri>,][EXPGAIN=<gain>][:<pst>,][<sst>];

ED-OTS[:<TID>]:<aid>:<CTAG>[:::RDIRN=<rdirn>,][VOAATTN=<voaattn>,][VOAPWR=<voapwr>,][CALOPWR=<calopwr>,][CALTILT=<caltilt>,][OSRI=<osri>,][ALSMODE=<alsmode>,][ALSRCINT=<alsrcint>,][ALSRCPW=<alsrcpw>,][EXPGAIN=<gain>][:<pst>,][<sst>];

ED-T1 syntax changed:

ED-T1[:<TID>]:<aid>:<CTAG>[:::LINECDE=<linecde>,][FMT=<fmt>,][LBO=<lbo>,][TACC=<tacc>,][SOAK=<soak>,][SFBER=<sfber>,][SDBER=<sdber>][:<pst>,][<sst>];

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

ED-T3 syntax changed:

ED-T3[:<TID>]:<aid>:<CTAG>[:::FMT=<fmt>,][LINECDE=<linecde>,][LBO=<lbo>,][TACC=<tacc>,][SOAK=<soak>,][SFBER=<sfber>,][SDBER=<sdber>][:<pst>,][<sst>];

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

ED-VT1 syntax changed:

ED-VT1[:<TID>]:<aid>:<CTAG>[:::RVRTV=<rvrtv>,][RVTM=<rvtm>,][HOLDOFFTIMER=<holdofftimer>,][TACC=<tacc>][:<pst>,][<sst>];

ED-VT1[:<TID>]:<aid>:<CTAG>[:::RVRTV=<rvrtv>,][RVTM=<rvtm>,][HOLDOFFTIMER=<holdofftimer>,][TACC=<tacc>,][TAPTYPE=<taptype>][:<pst>,][<sst>];

ED-WDMANS syntax changed:

ED-WDMANS[:<TID>]:<aid>:<CTAG>[:::POWER-IN=<powerIn>,][POWER-OUT=<powerOut>,][POWER-EXP=<powerExp>,][POWER-DROP=<powerDrop>,][SYS-TYPE=<sysType>,][RING-TYPE=<ringType>];

ED-WDMANS[:<TID>]:<aid>:<CTAG>[:::POWER-IN=<powerIn>,][POWER-OUT=<powerOut>,][POWER-EXP=<powerExp>,][POWER-DROP=<powerDrop>,][SYS-TYPE=<sysType>,][NTW-TYPE=<ringType>];

ENT-EQPT syntax changed:

ENT-EQPT:[<TID>]:<aid>:<CTAG>::<aidtype>:[PROTID=<protid>,][PRTYPE=<prtype>,][RVRTV=<rvrtv>,][RVTM=<rvtm>][:];

ENT-EQPT:[<TID>]:<aid>:<CTAG>::<aidtype>:[PROTID=<protid>,][PRTYPE=<prtype>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][CMDMDE=<cmdmde>][:];

ENT-UCP-CC syntax changed:

ENT-UCP-CC[:<TID>][:<aid>]:<CTAG>[:::NBRIX=<nbrix>,][CCTYPE=<cctype>,][PORT=<port>,][LOCALCCID=<localccid>,][LOCALIPCC=<localipcc>,][REMOTCCID=<remoteccid>,][REMOTEIPCC=<remoteipcc>,][LMPHELLOINT=<lmphelloint>,][LMPHELLODEADINT=<lmphellodeadint>,][MTU=<mtu>,][CRCMD=<crcmd>,][TUNMD=<tunmd>][:];

ENT-UCP-CC[:<TID>][:<aid>]:<CTAG>:::NBRIX=<nbrix>,CCTYPE=<cctype>,[PORT=<port>,][LOCALCCID=<localccid>,][LOCALIPCC=<localipcc>,][REMOTCCID=<remoteccid>,][REMOTEIPCC=<remoteipcc>,][LMPHELLOINT=<lmphelloint>,][LMPHELLODEADINT=<lmphellodeadint>,][MTU=<mtu>,][CRCMD=<crcmd>,][TUNMD=<tunmd>][:];

ENT-UCP-IF syntax changed:

ENT-UCP-IF[:<TID>]:<aid>:<CTAG>[:::NBRIX=<nbrix>,][CCID=<ccid>,][LOCALIFID=<localifid>,][REMOTEIFID=<remoteifid>,][TNATYPE=<tnatype>,][TNAADDR=<tnaaddr>,][CORENETWORKID=<corenetworkid>][:];

ENT-UCP-IF[:<TID>]:<aid>:<CTAG>:::NBRIX=<nbrix>,[CCID=<ccid>,][LOCALIFID=<localifid>,][REMOTEIFID=<remoteifid>,][TNATYPE=<tnatype>,][TNAADDR=<tnaaddr>,][CORENETWORKID=<corenetworkid>][:];

EX-SW-OC12 syntax changed:

EX-SW-OC12[:<TID>]:<aid>:<CTAG>[::<st>];

EX-SW-OC12[:<TID>]:<aid>:<CTAG>[::,<st>][,<dirn>];

EX-SW-OC192 syntax changed:

EX-SW-OC192[:<TID>]:<aid>:<CTAG>[::<st>];

EX-SW-OC192[:<TID>]:<aid>:<CTAG>[::,<st>][,<dirn>];

EX-SW-OC48 syntax changed:

EX-SW-OC48[:<TID>]:<aid>:<CTAG>[::<st>];

EX-SW-OC48[:<TID>]:<aid>:<CTAG>[::,<st>][,<dirn>];

INIT-REG-CLNT syntax changed:

INIT-REG-CLNT[:<TID>]:<src>:<CTAG>::,,[<location>,][<direction>,][<tmper>][,,];

INIT-REG-CLNT[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-DS1 syntax changed:

INIT-REG-DS1[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-DS1[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-EC1 syntax changed:

INIT-REG-EC1[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-EC1[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-G1000 syntax changed:

INIT-REG-G1000[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-G1000[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-OC12 syntax changed:

INIT-REG-OC12[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-OC12[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-OC192 syntax changed:

INIT-REG-OC192[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-OC192[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-OC3 syntax changed:

INIT-REG-OC3[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-OC3[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-OC48 syntax changed:

INIT-REG-OC48[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-OC48[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-OCH syntax changed:

INIT-REG-OCH[:<TID>]:<src>:<CTAG>::,,[<location>,][<direction>,][<tmper>][,,];

INIT-REG-OCH[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-OMS syntax changed:

INIT-REG-OMS[:<TID>]:<src>:<CTAG>::,,[<location>,][<direction>,][<tmper>][,,];

INIT-REG-OMS[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-OTS syntax changed:

INIT-REG-OTS[:<TID>]:<src>:<CTAG>::,,[<location>,][<direction>,][<tmper>][,,];

INIT-REG-OTS[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-STS1 syntax changed:

INIT-REG-STS1[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-STS1[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-STS12C syntax changed:

INIT-REG-STS12C[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-STS12C[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-STS192C syntax changed:

INIT-REG-STS192C[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-STS192C[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-STS24C syntax changed:

INIT-REG-STS24C[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-STS24C[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-STS3C syntax changed:

INIT-REG-STS3C[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-STS3C[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-STS48C syntax changed:

INIT-REG-STS48C[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-STS48C[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-STS6C syntax changed:

INIT-REG-STS6C[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-STS6C[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-STS9C syntax changed:

INIT-REG-STS9C[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-STS9C[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-T1 syntax changed:

INIT-REG-T1[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-T1[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-T3 syntax changed:

INIT-REG-T3[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-T3[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-VT1 syntax changed:

INIT-REG-VT1[:<TID>]:<aid>:<CTAG>::,,[<locn>,][<dirn>,][<tmper>][,,];

INIT-REG-VT1[:<TID>]:<aid>:<CTAG>::<montype>,,[<locn>,][<dirn>,][<tmper>][,,];

OPR-PROTNSW-OC12 syntax changed:

OPR-PROTNSW-OC12[:<TID>]:<aid>:<CTAG>::<sc>,[<switchType>][:];

OPR-PROTNSW-OC12[:<TID>]:<aid>:<CTAG>::<sc>[,<switchType>][:<dirn>];

OPR-PROTNSW-OC192 syntax changed:

OPR-PROTNSW-OC192[:<TID>]:<aid>:<CTAG>::<sc>,[<switchType>][:];

OPR-PROTNSW-OC192[:<TID>]:<aid>:<CTAG>::<sc>[,<switchType>][:<dirn>];

OPR-PROTNSW-OC3 syntax changed:

OPR-PROTNSW-OC3[:<TID>]:<aid>:<CTAG>::<sc>,[<switchType>][:];

OPR-PROTNSW-OC3[:<TID>]:<aid>:<CTAG>::<sc>[,<switchType>][:<dirn>];

OPR-PROTNSW-OC48 syntax changed:

OPR-PROTNSW-OC48[:<TID>]:<aid>:<CTAG>::<sc>,[<switchType>][:];

OPR-PROTNSW-OC48[:<TID>]:<aid>:<CTAG>::<sc>[,<switchType>][:<dirn>];

OPR-SYNCNSW syntax changed:

OPR-SYNCNSW[:<TID>][:<aid>]:<CTAG>::<switchto>,[<sc>];

OPR-SYNCNSW[:<TID>]::<CTAG>;

RLS-EXT-CONT syntax changed:

RLS-EXT-CONT[:<TID>]:<aid>:<CTAG>[::,];

RLS-EXT-CONT[:<TID>][:<aid>]:<CTAG>;

RLS-PROTNSW-OC12 syntax changed:

RLS-PROTNSW-OC12[:<TID>]:<aid>:<CTAG>[::];

RLS-PROTNSW-OC12[:<TID>]:<aid>:<CTAG>[::<dirn>];

RLS-PROTNSW-OC192 syntax changed:

RLS-PROTNSW-OC192[:<TID>]:<aid>:<CTAG>[::];

RLS-PROTNSW-OC192[:<TID>]:<aid>:<CTAG>[::<dirn>];

RLS-PROTNSW-OC3 syntax changed:

RLS-PROTNSW-OC3[:<TID>]:<aid>:<CTAG>[::];

RLS-PROTNSW-OC3[:<TID>]:<aid>:<CTAG>[::<dirn>];

RLS-PROTNSW-OC48 syntax changed:

RLS-PROTNSW-OC48[:<TID>]:<aid>:<CTAG>[::];

RLS-PROTNSW-OC48[:<TID>]:<aid>:<CTAG>[::<dirn>];

RTRV-ALM-ENV syntax changed:

RTRV-ALM-ENV[:<TID>]:<aid>:<CTAG>[::<ntfcncde>,][<almtype>];

RTRV-ALM-ENV[:<TID>]:<aid>:<CTAG>[::<ntfcncde>][,<almtype>];

RTRV-BITS response changes:

<aid>::[<linecde>],[<fmt>],[<lbo>],[<syncmsg>],[<aisthrshld>]:[<pst>]

<aid>::[<linecde>],[<fmt>],[<lbo>],[<syncmsg>],[<aisthrshld>],<saBit>:[<pst>]

RTRV-CLNT response changes:

<aid>:,,[<role>],[<status>]:[<plgtype>],[<serialnum>],[<partnum>],[<vendor>],[<vendorrev>],[<vendorid>],[<clei>],[<portname>],[<sfber>],[<sdber>],[<alsmode>],[<alsrcint>],[<alsrcpw>],[<comm>],[<macaddr>],[<syncmsg>],[<senddus>],[<lsrstat>],[<soak>],[<soakleft>]:<pst>,[<sst>]

<aid>:,,[<role>],[<status>]:[<plgtype>],[<serialnum>],[<vendorrev>],[<clei>],[<portname>],[<sfber>],[<sdber>],[<alsmode>],[<alsrcint>],[<alsrcpw>],[<comm>],[<partnum>],[<vendor>],[<vendorid>],[<macaddr>],[<syncmsg>],[<senddus>],[<lsrstat>],[<soak>],[<soakleft>],[<ospf>]:<pst>,[<sst>]

COMMAND Response Changes:

RTRV-DS1 response changes:

<aid>::[<tacc>]

<aid>::[<tacc>],[<taptype>]

RTRV-G1000 response changes:

<aid>::[<mfs>],[<flow>],[<lan>],[<optics>],[<soak>],[<als>],[<trans>],[<tport>],<lwmrk>,<hiwmrk>,[<buff>],[<soakleft>]:<pst>,[<sst>]

<aid>::[<mfs>],[<flow>],[<lan>],[<optics>],[<soak>],[<als>],[<trans>],[<tport>],<lwmrk>,<hiwmrk>,[<buff>]:[<soakleft>]:<pst>,[<sst>]

RTRV-INV response changes:

<aid>,<aidtype>::[<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>]

<aid>,<aidtype>::[<plugtype>],[<vendor>],[<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>]

RTRV-OCH response changes:

<aid>:,,[<role>],[<status>]:[<rdirn>],[<opticalPortType>],[<power>],[<expWlen>],[<actWlen>],[<iloss>],[<voamode>],[<voaattn>],[<voapwr>],[<voarefattn>],[<voarefpwr>],[<refopwr>],[<calopwr>],[<chpower>],[<portname>],[<sfber>],[<sdber>],[<alsmode>],[<alsrcint>],[<alsrcpw>],[<comm>],[<gccrate>],[<dwrap>],[<fec>],[<osfber>],[<osdber>],[<macaddr>],[<syncmsg>],[<senddus>],[<lsrstat>],[<soak>],[<soakleft>]:<pst>,[<sst>]

<aid>:,,[<role>],[<status>]:[<rdirn>],[<opticalPortType>],[<power>],[<expWlen>],[<actWlen>],[<iloss>],[<voamode>],[<voaattn>],[<voapwr>],[<voarefattn>],[<voarefpwr>],[<refopwr>],[<calopwr>],[<chpower>],[<portname>],[<sfber>],[<sdber>],[<alsmode>],[<alsrcint>],[<alsrcpw>],[<comm>],[<gccrate>],[<dwrap>],[<fec>],[<osfber>],[<osdber>],[<macaddr>],[<syncmsg>],[<senddus>],[<lsrstat>],[<soak>],[<soakleft>],[<ospf>]:<pst>,[<sst>]

RTRV-OTS response changes:

<aid>::<rdirn>,<opticalPortType>,[<power>],[<iloss>],[<voamode>],[<voaattn>],[<voapwr>],[<voarefattn>],[<voarefpwr>],[<laserst>],[<osri>],[<amplmode>],[<gain>],[<expgain>],[<refopwr>],[<calopwr>],[<reftilt>],[<caltilt>],[<dculoss>],[<awgst>],[<heatst>]:<pst>,[<sst>]

<aid>::<rdirn>,<opticalPortType>,[<power>],[<iloss>],[<voamode>],[<voaattn>],[<voapwr>],[<voarefattn>],[<voarefpwr>],[<laserst>],[<osri>],[<alsmode>],[<alsrcint>],[<alsrcpw>],[<amplmode>],[<gain>],[<expgain>],[<refopwr>],[<calopwr>],[<reftilt>],[<caltilt>],[<dculoss>],[<awgst>],[<heatst>]:<pst>,[<sst>]

RTRV-STS9C response changes:

<aid>::[<level>],[<sfber>],[<sdber>],[<rvrtv>],[<rvtm>],[<swpdip>],[<holdofftimer>],[<exptrc>],[<trc>],[<inctrc>],[<trcmode>],[<tacc>],[<upsrpthstate>],[<c2>],[<blsrpthstate>]:[<pst>],[<sst>]

<aid>::[<level>],[<sfber>],[<sdber>],[<rvrtv>],[<rvtm>],[<swpdip>],[<holdofftimer>],[<exptrc>],[<trc>],[<inctrc>],[<trcmode>],[<tacc>],[<taptype>],[<upsrpthstate>],[<c2>],[<blsrpthstate>]:[<pst>],[<sst>]

RTRV-T1 response changes:

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

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

RTRV-T3 response changes:

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

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

RTRV-TRC-CLNT response changes:

<aid>,<aidtype>::[<trclevel>],[<exptrc>],[<trc>],[<inctrc>],[<trcmode>],[<trcformat>]

[<trclevel>],[<exptrc>],[<trc>],[<inctrc>],[<trcmode>],[<trcformat>]

RTRV-WLEN response changes:

<aid>::[<size>]:[<pst>],[<sst>]

<aid>::[<mode>],[<size>]:[<pst>],[<sst>]

SET-TOD syntax changed:

SET-TOD[:<TID>]::<CTAG>::<year>,<month>,<day>,<hour>,<minute>,<second>,[<difference>][:DST=<dst>];

SET-TOD[:<TID>]::<CTAG>;

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15454, Release 4.6.4*
- *Release Notes for the Cisco ONS 15327, Release 4.6.4*
- *Cisco ONS 15454 Software Upgrade Guide, Release 4.6*

Platform-Specific Documents

- *Cisco ONS 15454 Procedure Guide, Release 4.6*
- *Cisco ONS 15454 Reference Guide, Release 4.6*
- *Cisco ONS 15454 Troubleshooting Guide, Release 4.6*
- *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide, Release 4.6*
- *Cisco ONS 15454 Product Overview, Release 4.6*

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

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