Release Notes for Cisco ONS 15454 SDH Release 4.6.1

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

August, 2007

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15454 SDH multiplexer. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to the "Release 4.6" version of the of the *Cisco ONS 15454 SDH Installation and Operations Guide, and Cisco ONS 15454 SDH Troubleshooting and Reference Guide.* For the most current version of the *Release Notes for Cisco ONS 15454 SDH Release 4.6.1*, visit the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/ong/15454sdh/sdhrelnt/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

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

Obtaining Technical Assistance, page 44

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15454 SDH Release 4.6.1* since the production of the Cisco ONS 15454 SDH System Software CD for Release 4.6.1.

The following changes have been added to the release notes for Release 4.6.1.

Changes to Caveats

The following caveat has been added.

Transmission Control Protocol Specification, page 15

Caveats

Review the notes listed below before deploying the ONS 15454 SDH. 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 # CSCec33248

Pulling the active XCVXL card might result in a traffic outage lasting for greater than 2 seconds. It is possible to see this approximately 1 out of every 7 active XCVXL card pulls. Excessive traffic outage from this issue will not occur after a software-induced XCVXL side switch. In this case, you can expect a traffic hit of less than 60 ms, and traffic will resume normally.

DDTS # CSCdw92634

SDH DS3-i and E3 electrical cards only support a VC4 J1 trace string setting for all VC4s together. You cannot set the J1 byte for individual VC4s. This issue is a limitation of hardware.

Note VC3 J1 strings can be set individually, but the optical cards cannot monitor the VC3 J1 string.

DDTS # CSCdw14501

Interconnection Equipment failure alarms may be generated at 55 degrees C, and 72 volts. When the operating environment is at 55 degrees C and 72 volts, interconnection equipment failure alarms for the following cards can occur:

- STM16SH

- STM64LH
- STM16LH
- XC10G

The alarms could potentially occur on any of these boards, as well: OC48AS, GigE, OC192 or OC192LR. This issue will be resolved in a future release.

DDTS # CSCdw50903

E1-14 boards with second source components can incur bit errors under extreme environmental conditions. When these boards operate under voltage and temperature stress conditions and a temperature ramp rate of 1 degree per minute, the boards could exhibit dribbling bit errors at high temperatures: BER = 5.5e-6. To avoid this, you must apply the temperature ramp rate at 0.5 degree per minute. This ramp rate complies with the NEBS standard; however, this issue will be revisited in a future release.

Upgrades

DDTS # CSCec42769 Database Corruption with ONS 15454 SDH Release 4.0, 4.0.1, 4.1

Caution Before you upgrade to Release 4.6.1 from Release 4.0, 4.0.1, or 4.1, you must read this caveat and run the SDH Circuit Repair Utility (VcCheck) provided on the software CD (also available on CCO).

The XCVXL card on the ONS 15454 SDH allows the intermixing of VC12 and VC3 payloads within a single VC4. When a VC4 contains only one VC12 tributary and at least one VC3 tributary and the VC12 is deleted, the database becomes corrupt.

The database load process on the ONS 15454 SDH occurs during a TCC2 reboot, TCC2 protection switch, software activation, or database restore. When the database is loaded containing this corruption the load process fails, causing the corrupt database to be deleted from the TCC2 flash memory. The previous saved database is then loaded instead. When all saved databases on a TCC2 contain the corruption, the TCC2 will load with the default provisioning, and all existing provisioning will be lost.

If this issue occurs you will see a loss of either some or all provisioning after a TCC2 switch or reset.

To ensure that your network is not vulnerable to this issue, you must first determine if the issue already exists within your network, and if so, correct it. You can detect the issue by using the SDH Circuit Repair Utility (VcCheck) provided on the ONS 15454 SDH Release 4.1.3 and 4.6.1 software CDs. The VcCheck tool is also available for download from CCO. Once you have alleviated immediate risk from the issue, you must upgrade to Release 4.6.1, or maintenance Release 4.1.3 (or any later release) to avoid further risk.

The VcCheck utility and its associated README file (in the same directory with the tool) provide details on how to temporarily alleviate this issue before upgrading to a release in which the issue is resolved.

This issue is resolved in Release 4.6 and maintenance Release 4.1.3 (caveated herein because of the upgrade issue).

Line Cards

J1 and J2 Path Trace with E1-42 Cards

On E1-42 cards, do not enable J1 or J2 monitoring in Release 4.6.1. To do so can result in a loss of traffic. If you do have J1 or J2 path trace turned on, and you upgrade to Release 4.6.1, turn those features off prior to the upgrade in order to avoid possible traffic loss. This issue will be resolved in a future release.

DDTS # CSCed30150

When the E1-42 card is fully loaded, J2 path trace cannot be retrieved on VC12 circuits. This issue will be resolved in a future release.

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 will be resolved in a future release.

DDTS # CSCec83712

Avoid pulling the active cross connect when the standby is locked out. If the standby cross connect card is locked out and the active cross connect card is pulled, the E1-42 card switches to protect. This switch should not occur. After the active cross connect card reboots and traffic is restored, the reverting E1-42 card takes a hit of +/- 1 second. This issue will be resolved in a future release.

DDTS # CSCed14006

Rarely, after you power cycle a node, an installed E1-14 card might report LOF on various ports. Provisioning will clear the LOF. This issue will be resolved in a future release.

DDTS # CSCed27998

Rarely, a traffic hit can occur during the TCC2 switch that occurs as a part of the upgrade procedure. Traffic hits are only expected on E1-42 traffic; all other E3 & DS3 traffic should remain errorless during the upgrade's TCC2 switch portion. Hits to the E1-42 traffic occur 90% of the time during the upgrade if all 42 circuits are provisioned on the card. This issue will be resolved in a future release.

DDTS # CSCed15073

Rarely, a WKSWPR condition resulting from loss and recovery of power to the node can become stuck when there are multiple 1+1 protection groups provisioned on a single OC3-8 card. This issue will be resolved in a future release.

DDTS # CSCec30792

On a small percentage of active XCVXL card pulls, the E1-42 card can lose traffic for more than 2 seconds. To avoid this issue, do not pull active XCVXL card. First, switch to the protect XCVXL, wait for the switchover, then, pull the XCVXL in question. This will be resolved with the E1-63 card.

DDTS # CSCed29086

Resetting both TCC2s occasionally causes the IO cards to send and/or receive corrupt K bytes. If this occurs, it might cause a ring to unswitch at the passthrough node. If you cause a force switch and then clear the force switch, traffic will recover. This issue will be resolved in Release 5.0.

DDTS # CSCec82148

Rarely, traffic hits can occur on TCC2 card removal. To avoid this issue, remove the card quickly. To recover from this issue, soft reset the TCC2 card. This issue will be resolved in Release 5.0.

DDTS # CSCed31270

Rarely, E1-42 traffic might fail to recover after active XC boot up following a lockon and removal of the active XC. To work around this, induce the software to perform a “chipInitSequence.” This issue will be resolved in a future release.

DDTS # CSCed26246

Rarely, an STM1-8 card reports MEA after an NE power cycle. This can occur when a power cycle is induced by quickly removing and reinserting a fuse, or when the fuse is removed for several minutes and then replaced. Cycle power again to recover STM1-8 operation. This issue is under investigation.

DDTS # CSCed25636

Occasionally, a 1:N soft switch command can take approximately 20 seconds to take effect on E1-42 after a software upgrade when several circuits are provisioned. If this occurs, soft reset the card, or reprovision all the circuits. This issue will be resolved in a future release.

DDTS # CSCec82450

When the Active TCC2's power supply fails (using a failure insertion test card) and the Standby TCC2 takes over; the circuits on the DS3I and E1-42 cards in that node might incur a traffic hit. This issue will be resolved in a future release.

Interoperability with SONET DS3i-N-12

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.

DDTS # CSCea52722

With DS3-I cards in a 1:2 protection group, when the protect card is active and in the WTR condition, removing another working card from the protection group clears the WTR condition. To work around this issue, remove the working card from the protection group when the protect card is in the standby state. This issue will be resolved in a future release.

Ethernet Polarity Detection

The TCC2 does not support Ethernet polarity detection. The TCC+ and TCCI both support this feature. If your Ethernet connection has the incorrect polarity (this can only occur with cables that have the receive wire pairs flipped), the TCC+/I will work, but the TCC2 will not. In this event, a standing condition, "LAN Connection Polarity Reverse Detected" (COND-LAN-POL-REV), will be raised (a notification will appear on the LCD, and there will be an alarm raised). This issue will most likely be seen during an upgrade or initial node deployment. To correct the situation, ensure that your Ethernet cable has the correct mapping of the wire wrap pins. For Ethernet pin mappings, consult the "DLP-A 21 Install LAN Wires on the Backplane" procedure in the user documentation.

Active Cross Connect or TCC2 Card Removal

Active cross connect or TCC2 cards should not be removed. If the active cross connect or TCC2 card must be removed, to minimize network interruption you can first perform an XC10G (or XCVXL) side switch 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).

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

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
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, 22Ý/55.9cm long, SONET/ANSI system
15454E-CONSOLE-02	Cable, console, ML-Series, RJ-11 plug to RJ-45 jack, 22Ý/55.9cm long, SDH/ETSI system

DDTS # CSCdw44431

Cisco ONS 15454 optical cards are not provisioned for particular path labels (C2 bytes). Consequently, they cannot raise a PLM condition. However, the ONS 15454 electrical card that terminates traffic ensures that the C2 byte is correct for the type of traffic carried. If the C2 byte is incorrect, this card raises a PLM condition that is reported against the optical port of ingress. An optical card will not raise a PLM against traffic that passes through a node, though it will appear to raise a PLM against traffic with the wrong C2 byte that is terminated on an electrical card within the node. It is not known at this time when or if this issue will be resolved.

Note Optical cards do ensure that the C2 byte is nonzero (Equipped), and will raise a UNEQ condition if the C2 byte is 0 (Unequipped).

DDTS # CSCdw80652

When one traffic card in a DS3i 1:N protection group is reset, and then another card is reset, there will be a loss of traffic on the second card, after the first card completes its reset, lasting until the second card completes its reset. This only occurs when the protect card tries to handle the traffic of a card that is resetting, and that card is carrying traffic because when it reset the protect card was carrying traffic for another card. This loss of traffic occurs because the protect card attempts to set its relays to handle the traffic of the working card, but the relays on the working card are also set to carry the traffic, and since the card is resetting, no software is running to switch its relays. This issue most frequently presents itself when testing a double-failure scenario: resetting two cards in a protection group. Wait until the first card completes its reset sequence before resetting the second card to prevent this problem. Configuring cards in 1:1 instead of 1:N protection should also avoid the problem. This issue will not be resolved.

DDTS # CSCdw57215

In a configuration with STM16 Any Slot cards and an VC4-8c circuit, provisioned between G1000-4 cards with traffic going over the STM16 span, extracting the G1000-4 card at one end of the VC4-8c circuit before deleting the circuit can result in a traffic hit on all existing SDH circuits defined over that same span. There are no issues if the circuit is deleted prior to the removing the G1000-4 card.

XC10G Boot Process

If you install a new XC10G card to the node and it fails to boot, remove the card and reinsert it. If the card still fails to boot, return it using the RMA procedure. This issue will be resolved in future hardware.

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 subsequent version of the XC10G cross connect card. DDTS numbers related to this issue include CSCdv50357, CSCdv63567, CSCdv68418, CSCdv68441, CSCdv68389, CSCdv59621, and CSCdv73402.

DWDM Cards

DDTS # CSCed18225

When the trunk ports for two back-to-back connected MXPs or TXPs have different ALS modes enabled (such as if one of them is ALS-Manual, and other is ALS-Auto), or have the same ALS mode for both sides (with ALS-Manual or ALS-Auto enabled), MXP or TXP might enter a state in which there are oscillating LOS-P, ALS, and Client Squelch alarms. If this occurs, either choose ALS-Disable on MXP/TXP, or remove the trunk transmit fiber on either end for 15-20 seconds and then reinsert it. It has not been determined when or if this issue will be resolved.

DDTS # CSCed21403

Occasionally, in a node with MXP-2.5G-10G cards, when you hard reset the active TCC2, the MXP-2.5G-10G traffic can take a hit of 1-4 ms. It has not been determined when or if this issue will be resolved.

DDTS # CSCed01940

The TXPP card does not squelch the near end client on putting trunk ports OOS. This can occur where two TXPP cards are connected via trunks. Each TXPP card is in transparent mode with GCC enabled. Testsets are connected to each client port. On the near end, place both trunk ports OOS. The far end client squelches because of LOS-P. The near end client, however, does not squelch. The near client should also squelch. To work around this, place the client port OOS, or place the far-end trunk port OOS. This issue will be resolved in a future release.

DDTS # CSCeb25490

Occasionally CTC 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 # 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.

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.

DDTS # CSCeb32065

Once engaged, the 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. 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 # CSCeb24815

With TXP-MR-2.5G cards, ratios are calculated incorrectly after clearing statistics. This is because after you clear statistics the entire time period becomes invalid. Once the time period rolls over again, values will be reliable for the new period.

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

E1000-2/E100T

Do not use the repair circuit option with provisioned stitched Ethernet circuits. It is not known at this time when or if this issue will be resolved.

Single-card EtherSwitch

Each E100/E1000 card can be configured as a single-card EtherSwitch configuration to allow VC4-4c of bandwidth to be dropped at each card. The following scenarios for provisioning are available:

VC4-4c

VC4-2c, VC4-2c

VC4-2c, VC4, VC4

VC4, VC4, VC4, VC4

When configuring scenario 3, the VC4-2c must be provisioned before either of the VC4 circuits.

Multicard EtherSwitch

When deleting and recreating Ethernet circuits that have different sizes, you must delete all VC4 circuits provisioned to the EtherSwitch before you create the new circuit scenario. (See the preceding "Single-card EtherSwitch" section on page 6 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.

ML Series Cards

DDTS # CSCec52443

On an ML-series RPR ring circuit deletion or creation causes an approximately 200 ms traffic loss. Traffic loss is expected to be less than 50 ms for RPR. 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, traffic loss is greater than 50 ms. When a maintenance action is taken, 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 # CSCed06286

If you create several bridgegroups before provisioning POS circuits, POS stays in the BLK state. If this issue occurs, perform a shut/no shut on POS interface that is stuck in the BLK state. This issue will be resolved in a future release.

DDTS # CSCeb25778

When a MAC-SA is seen for the first time, it is learned, but may age out in less than 5 minutes. If the same MAC-SA is seen again before the first ages out, the entry will age out after 5 minutes, as expected. This issue will not be resolved.

DDTS # CSCin43669

Timer expiration can cause a system crash when you attempt to remove 250 Shared Packet Ring (SPR) subinterfaces using the “no int spr1” command, while Cisco Discovery Protocol (CDP) is also enabled. To avoid this issue, either turn off CDP, issue the command, and then turn CDP back on; or remove the SPR subinterfaces explicitly. This issue will not be resolved.

DDTS # CSCea36829

The broadcast packet count is always 0 for the SPR interface. The ML100 and ML1000 hardware does not support counting broadcast packets. This issue will not be resolved.

DDTS # CSCeb21996

When the POS interface is removed from SPR due to a defect, while SPR is configured in immediate mode, the defect type may not be reported. This only occurs if the defect is set and clears in less then 50 ms.

DDTS # CSCdz49700

ML-series cards do not appear in the Cisco Discovery Protocol (CDP) adjacencies and do not participate in the Spanning-Tree Protocol. All packets are counted as multicast.

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 # CSCea01675

Packets without an 802.1q VLAN tag are classified as COS 0. This issue will not be resolved.

DDTS # CSCea20962

No warning is displayed when applying OOS to ML drop ports on the circuit provisioning window. This issue will be resolved in Release 5.0.

DDTS # CSCea26847

An unexpected card reload can occur when a card is configured to route IP-Multicast traffic and subsequently sends IP-Multicast frames larger than 1649 bytes. To prevent this, avoid routing IP-Multicast frames larger than 1649 bytes. This issue is under investigation.

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.

DDTS # CSCdy55437

The maximum MAC Address Learn Rate for the ML-Series cards is 1300 MAC addresses per second. This number varies based on the ML-Series control and forwarding plane loads. If the forwarding and control planes are heavily loaded, the maximum MAC Address Learn Rate could be as low as 100 MAC addresses per second. To correct a situation where an ML-Series card has stopped learning MAC addresses, reduce the load on these cards. This load limit is by design.

DDTS # CSCdy47284

Oversize frames are not supported on ML100 Fast Ethernet ports. Oversize frames cause egress traffic to incur CRC, line, and fragment errors on these ports. To avoid this issue, do not send jumbo packets to ML far end ports. This is as designed.

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 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).

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 will be resolved in Release 5.0.

DDTS # CSCed27389

Under certain conditions, you cannot unlock a cross-connect from CTC and TL1. If you lock a cross-connect, then quickly click the SWITCH button, the Clear is sent only to the protect XC side. This causes the Unlock command to fail. This issue is resolved in Release 5.0.

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 SNCP and MS-SPRing 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 MS-SPRing 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 # CSCec48979

With STM1_E12 E4 traffic, when you inject BPV errors at 10E-3 rate to the E4 traffic port, sometimes SF will not be reported. This issue will be resolved in a future release.

DDTS # CSCec21668

Do not create more than three VC3 or VC12 circuits in auto-range mode. The VC3 or VC12 circuits can be created in batches of three, or manually. When you create more than three VC3 or VC12 circuits in auto-range mode, CTC creates the first three circuits and then issues the error message:

"Exception: Source is not fully specified"

This can occur with an SDH node when you wish to create more than three VC3 or VC12 circuits in auto-range mode. This issue will be resolved in a future release.

DDTS # CSCed27389

In some instances, you might not be able to unlock a cross-connect from both CTC and TL1. After locking the cross-connects, if you quickly click the SWITCH button, the unlock command might fail. This issue is resolved in Release 5.0.

DDTS # CSCeb39359

When changing NE timing from extern/mix to Line timing, a Transient IEF alarm may be reported against the standby XC10G. This issue will be resolved in a future release.

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 # 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 # CSCdz62367

When replacing a failed working E1-42 card in a 1:1 or 1:N protection configuration with the protect card carrying the switched traffic, bit errors, less than 50ms in duration, are possible on the activated protection card. This issue will not be resolved.

DDTS # CSCdy10030

CVs are not positively adjusted after exiting a UAS state. When a transition has been made from counting UAS, at least 10 seconds of non-SES must be counted to exit UAS. This issue will not be resolved.

DDTS # CSCdx35561

CTC is unable to communicate with an ONS 15454 SDH that is connected via an Ethernet craft port. CTC does, however, communicate over an SDCC link with an ONS 15454 SDH that is Ethernet connected, yielding a slow connection. This situation occurs when multiple nodes 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 SDH 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 15454 SDHs.

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 SDH 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 # CSCdy11012

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

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

To work around this issue, if no firewall enabled, then the network configuration of the CTC host can be changed to allow CTC to see all nodes in the network. The launch node must be on its own subnet to prevent network partitioning, and craft access must not be enabled. The CTC host must be provisioned

with an address on the same subnet as the initial node (but this address must not conflict with any other node in the network), and with the default gateway of the initial node. CTC will now be able to contact all nodes in the network.

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

DDTS # CSCdy57891

An LOP-P alarm can be inadvertently cleared by an LOS that is raised and cleared. On STM-N cards, when an LOP condition and an LOS condition are both present on the input, an LOS will be raised. However, upon clearing the LOS with the LOP still present, the LOP alarm is not raised. An AIS-P condition will be visible. This issue will not be resolved.

DDTS # CSCdw38283

If a node has one good BITS reference and is running in a normal state, and you configure a second BITS reference, then reconfigure the second reference within 30 seconds of applying the first configuration, the node will enter FAST START SYNC mode. To avoid this problem, wait a minute before configuring the second reference a second time. This issue is a hardware limitation, and there are no current plans to resolve it.

DDTS # CSCdw23208

The following table summarizes B1, B2, and B3 error count reporting for SDH optical cards. Note that not all reporting is done according to ITU specifications. In particular, ITU specifies error counts for B1 and B3 as the number of blocks with errors (refer to ITU-T G.826 for paths and ITU-T G.829 for RS and MS).

Table 0-5 Error Count Reporting

	B1	B2	B3
ITU Specification	block	bit	block
STM1	block	bit	block
STM4	bit	bit	bit
STM16 trunk	bit	bit	bit
STM16 AS	block	bit	bit
STM64	block	bit	bit
STM1-8	bit	bit	bit
STM4-4	bit	bit	bit

DDTS # CSCdw82689

After creating 509 VLANs and provisioning many Ethernet circuits, Ethernet circuit provisioning can become very slow, or possibly fail. Ethernet traffic may also incur an outage of a few minutes. To avoid this problem, delete any VLANs that are created but not used, and do not recreate them. There is no resolution planned for this issue.

DDTS # CSCdv10824: Netscape Plugins Directory

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

"Are you sure" Prompts

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

MS-SPRing Functionality

DDTS # CSCed28018

If at least one drop of the circuits created on an MS-SPRing is an electrical card circuit, an active XCVXL hard reset can cause a high traffic hit on VC12, VC3 (DS3), VC3 STM1E to E3. This issue will be resolved in a future release.

DDTS # CSCec34856

When you create a circuit over MS-SPRing or DRI, the resource usage in the Maintenance > Cross-Connect > Resource Usage tab will display the incorrect VC# for the circuit you created. Use the Circuit Edit > Monitors window to view the correct VC#. This issue will be resolved in a future release.

DDTS # CSCea81000

In a two-fiber or four-fiber MS-SPRing, 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 6.0.

DDTS # CSCeb09217

Circuit states are not updated after a span update. If you update a four node OC-12 two-fiber MS-SPRing to a four node OC-192 two-fiber BLSR, the previous PCA circuits should be shown as two-fiber MS-SPRing 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 # CSCdz66275

When creating a MS-SPRing from the network view, the node default values for reversion are not initially used. To see this, starting with no preferences file, log into a node with CTC, and set the node default values for MS-SPRing reversion. Now, in Network view, use the MS-SPRing wizard to create a MS-SPRing. The node level default values are initially ignored while the wizard is still in operation. If you encounter this issue, you may need to change values as appropriate for your network while you are still using the MS-SPRing wizard. Once the wizard is finished, these values are saved to a preferences file and will be used henceforth. This issue will not be resolved.

DDTS # CSCdw53481

Two MS-Rs are not allowed to coexist. If you execute a manual ring switch command on one side of an MS-SPRing node and apply another manual ring switch command on other side of the node, the second manual ring switch command is rejected. This works as designed. The implementation complies with Telcordia GR-1230, R6-102.

DDTS # CSCdx45851

On a four fiber MS-SPRing, restoring the database for all nodes at the same time could cause VC4-16c traffic to fail to switch. Do not restore the database for multiple nodes simultaneously. The proper procedure for restoring the database for multiple nodes is to restore one node at a time. This procedure is documented in the user documentation.

DDTS # CSCdx19598

A rare hardware failure on an STM16AS card transmitter can trigger SEF on the receiving STM16AS card in a four fiber MS-SPRing (or BLSR) configuration. The BER calculations are suspended when SEF is detected, so SD or SF is never raised. Likewise SEF is not considered a signal failure condition like LOS or LOF, so a protection switch will not occur. If this occurs, use the CTC GUI to force a protection switch on the MS-SPRing (or BLSR). This issue will not be resolved.

DDTS # CSCdv53427

In a two ring, two fiber MS-SPRing (or BLSR) configuration (or a two ring MS-SPRing or 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. There are two possible workarounds for this issue:

1. Manually route the circuit to avoid the “one circuit over two ring” routing scenario.
2. When routing the circuit automatically, select the Using Required Nodes/Spans option in the Circuit Routing Preference screen, then select the appropriate spans to avoid the “one circuit over two ring” routing scenario.

This issue will be resolved in a future release.

Database Restore on an MS-SPRing (or BLSR)

When restoring the database on an MS-SPRing (or 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 TCCi has reset and booted up, release the force switch from each node.

SNCP Functionality

DDTS # CSCeb37707

With a VT SNCP 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.

Active Cross Connect or TCC2 Card Removal

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

Active cross connect cards should not be removed. If the active cross connect or TCC2 card must be removed, to minimize network interruption you can first perform an XC10G (or XCVXL) side switch 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).

SNMP

DDTS # CSCec75857

There is no SNMP return value for dsx1TotalTable when you configure an ONS 15454 with DSX 1 day stats, then query the node. This issue will be resolved in Release 5.0.

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 # CSCec63978

The clear button on the PM pane in CTC does not clear PJ detected seconds, PJ generated seconds, or PJ diff. Clearing PMs should result in the associated cell being marked yellow (INVALID) and zero; however, for PJ detected seconds, PJ generated seconds, and PJ diff, the cells remain unchanged.

There is no workaround for PJ seconds. These will continue to accumulate where they left off and not be marked invalid. PJ diff should be marked invalid, but is recalculated to the correct value, and is displayed as such. This issue will be resolved in Release 5.0.

Resolved Caveats for Release 4.6.1

The following items are resolved in Release 4.6.1

Line Cards

DDTS # CSCdy65482

On the AIC-i card, a volume adjustment on the receive value of a four-wire orderwire circuit will be displayed as the negative of its actual value. To work around this issue, enter the negative of the value you actually want for the receive value. For example, adjust the receive value on CTC to -2 dbm for a gain of 2 dbm. This issue is resolved in Release 4.6.

DDTS # CSCeb43397 and CSCeb42187

Rarely, E1-42 cards may incur a greater than 60 ms traffic disruption during protection switches. This can occur when you pull the active working E1-42 card. This issue is resolved in Release 4.6.

DDTS # CSCeb34655 and CSCeb39337

Very rarely, E1-42 takes greater than 2 second hits on an active XCVXL pull. To avoid this issue, side switch the XCVXL cards. This issue is resolved in Release 4.6.

DDTS # CSCeb39337

Very rarely, DS3i can lose traffic on an active XC-VXL pull. To avoid this issue, side switch the XC-VXL cards. This issue is resolved in Release 4.6.

DDTS # CSCea60715

In a 1+1 configuration, traffic may be lost upon reset of both working and protect STM64 cards. If you reset the protect card and then, before the protect card completes rebooting, reset the working card, the traffic does not switch to protect but remains on working. If the working card is removed during the time the protect is still coming up, the traffic does not switch to working and is lost. To avoid this issue, wait for the protect to fully come up before pulling the work card. This issue is resolved in Release 4.6.

DDTS # CSCeb19055

On the subsequent 3 slots occupied by the protect FMEC, MEA is not set when a mismatched IO card is inserted. This issue is resolved in Release 4.6.

DDTS # CSCec46228

Rarely, traffic on the DS3i-N-12 card might incur a hit when the active TCC2 is pulled. Removing the active TCC2 can cause timing hits and disrupt communication between cards, causing protection switches. To avoid this issue, instead of pulling the active TCC2, issue a manual switch, then pull the TCC2 once it has become standby. This issue is resolved in Release 4.6; however, you should still always switch traffic away from any TCC2 you intend to remove.

DDTS # CSCec49231

In an LMSP 1+1 configuration, following an XCVXL reset, The HP-PLM alarm might become stuck. The following steps will reproduce this issue.

Step 1 Create a circuit from and to DS3i-N-12 cards through an STM16 LMSP (1+1) in a two-node configuration.

Step 2 Perform a LOCKOUT on the cross connect cards (XCVXL).

Step 3 Perform a hard reset on the active XCVXL cards.

Traffic goes down, then returns after the XCVXLs finish booting. The false HP-PLM alarms are now present on the STM16 span card. Once the false HP-PLM alarms are detected; to remove the false alarms, perform a TCC side switch. 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.

DDTS # CSCeb34326

Rarely, an E1-42 card can go into continual autoreset. This can occur after the E1-42 card is inserted, or following a node power cycle. Hard reset the E1-42 by removing and re-inserting it into the chassis to stop this cycle. This issue is resolved in a Release 4.6.

DDTS # CSCec13638

Rarely, a greater than 2 second traffic hit can occur when the active XC is pulled, then you switch the IO from active (Working) to standby (protect). This issue is resolved in Release 4.6.

DDTS # CSCeb42187

Occasionally, if you remove the active working E1-42 card, the card takes a greater than 60 ms hit. This issue is resolved in Release 4.6.

DDTS # CSCeb41057

On an E1-42, the LOSS-L parameter appears as random values. For example, sometimes it appears as -269,488,145. This makes the count unavailable from the card. This issue is resolved in Releases 4.6 and 4.1.3.

DDTS # CSCeb49051

If you configure 1:N or 1:1 protection for DS1, DS3, E1, or E3, then lock the XC and soft reset the active XC, after the XC finishes resetting, the protection for the electrical cards switches. This issue is resolved in Releases 4.1.3 and 4.6.

DWDM Cards

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.

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 # 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. This issue is resolved in Release 4.6.

ML Series

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 # 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 SDH ports, with oversubscription of available circuit bandwidth configured, leading to output queue congestion.
- Traffic from SDH to Ethernet, with oversubscription of the available Ethernet bandwidth.

This issue is resolved in Release 4.6 by performance monitoring enhancements.

DDTS # CSCeb11930

The POS shutdown command will raise PLM-P on the far end for a VC3 circuit in an SDH node. This occurs on all ML-series cards in nodes running Release 4.0 or 4.1. 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.

G Series Cards

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.

Maintenance and Administration

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 # 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 # CSCdz90733

PCA traffic can remain down after restoring the incorrect database and then restoring the correct database to the node. To avoid this issue, exercise care in database restoration. If you accidentally restore the wrong database, first restore the correct database and check to see if all traffic has returned. If PCA traffic is still down, you may need to remove and reinsert a fiber or perform a cross connect card reset. This issue is resolved in Release 4.6.

DDTS # CSCea13593

DRI configuration rules require limits on multiple drops. However, in an ONS 15454 SDH DRI topology, a unidirectional circuit can be created from one ring to another with two drops at the destination node. 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 # 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 # 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 # 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 # CSCeb09356

The CTC card level provisioning pane allows a different range of values for the PSC-W, PSC-S, and PSC-R thresholds from the range allowed in the defaults provisioning window. At the CTC card view for an OC-192 card, CTC will allow any values for the PSC-W, PSC-S, and PSC-R. When provisioning these same values using the CTC node view defaults pane, the range is restricted from 0 to 600. This issue is resolved in Release 4.6.

DDTS # CSCeb35648

A circuit in the AINS state on STM1-8/OC3-8 may transition to IS state even when signals in both directions have alarms. 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, and in maintenance Release 4.1.3.

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 4.1.3 and 4.6.

MS-SPRing Functionality

DDTS # CSCdy56668 and CSCdy26822

Ethernet circuits may appear in the CTC circuit table with an INCOMPLETE status after an MS-SPRing 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 # CSCdy63060

In a 4 node, two-fiber MS-SPRing configuration, the E100 unstitched circuit state can become stuck at OOS-AINS-PARTIAL, even if there are no alarms and conditions raised.

This issue has been seen under the following conditions:

Step 1 Set up a 4 node, two-fiber MS-SPRing.

Step 2 Provision an E100 point to point circuit starting with the OOS-AINS state and the longer

Step 3 path as the working path. The working path should have at least one pass-through node.

Step 4 Ensure that Ethernet ports and STM-N ports are all in service, no alarms or conditions are raised, and traffic is running clear.

If the state does not change automatically, use the Circuit Edit Window to explicitly set the circuit state to IS. 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 # CSCea02986

In MS-SPRing configurations multiple node deletions and additions on a ring in quick succession can cause PCA traffic to go down. If this occurs, apply a Force Ring switch on the effected nodes. This issue is resolved in Release 4.6.

DDTS # CSCeb40296

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

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

Step 4 Clear the Forced Switch Ring in CTC. The MS-SPRing 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 MS-SPRing configuration. This issue is resolved in Release 4.6.

SNCP Functionality

DDTS # CSCea23732

If you try to manually create a VC4 circuit over a three node, STM4 SNCP using automatic routing and a required node, but there is no protected path from the source to the destination excluding the required node, automatic routing will fail to find a path and will raise a "ComputeRouteInMixedDomains: No Route Found" exception. To avoid this issue, you can avoid selecting required nodes, or use manual routing. This issue is resolved in Release 4.6.

DDTS # CSCec04550

In a SNCP configuration, upon detecting a double-path failure with UNEQ-P, the UNEQ-P on the protect path is not reported. This issue is resolved in Release 4.6.

Performance Monitoring

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.

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 SDH Reference Guide, Release 4.6.*

10-Gbps Multirate Transponder Card

The Cisco ONS 15454 SDH 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 SDH 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 SDH 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 SDH 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 SDH 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 SDH Reference Guide, Release 4.6.*

4 x 2.5-Gbps Muxponder Card

The Cisco ONS 15454 SDH 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 SDH 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 SDH 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 SDH 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 SDH 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 SDH 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 SDH 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 SDH hybrid node. The ONS 15454 SDH 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 SDH 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 SDH 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 SDH 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 SDH Reference Manual, R4.6*).

Hybrid OADM Node

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

Amplified TDM Node

An amplified TDM node is a single ONS 15454 SDH node that increases the span length between two ONS 15454 SDH 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 SDH network. Along with TDM nodes, the ONS 15454 SDH 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 SDH 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:

- SNCP (CCAT circuits only)
- Path-protected mesh network (PPMN)
- MS-SPRing
- 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 SNCP Routing

The go-and-return SNCP routing option allows you to route the SNCP 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 SNCP circuits. The go-and-return option appears on the Circuit Attributes panel of the Circuit Creation wizard.

MS-SPRing Enhancements

MS-SPRing Maximum Ring Support

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

MS-SPRing 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 MS-SPRing.

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 SDH 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, 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 MS-SPRing configuration.
- The current active/standby line status of the OC-x port in a 1+1 or a 2F/4F MS-SPRing 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 MS-SPRing. 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.

TL1 Test Access

With Release 4.6.x SDH supports TL1 test access. For details, see the *Cisco ONS 15454 SDH TL1 Test Access Quick Start Guide*.

Related Documentation

Release-Specific Documents

- *Release Notes for Cisco ONS 15454 SDH Release 4.6*
- *Release Notes for Cisco ONS 15454 Release 4.6.1*
- *Release Notes for Cisco ONS 15327 Release 4.6.1*

Platform-Specific Documents

- *Cisco ONS 15454 SDH Reference Manual, Release 4.6*
- *Cisco ONS 15454 SDH Procedure Guide, Release 4.6*
- *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide, Release 4.6*

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

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

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

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