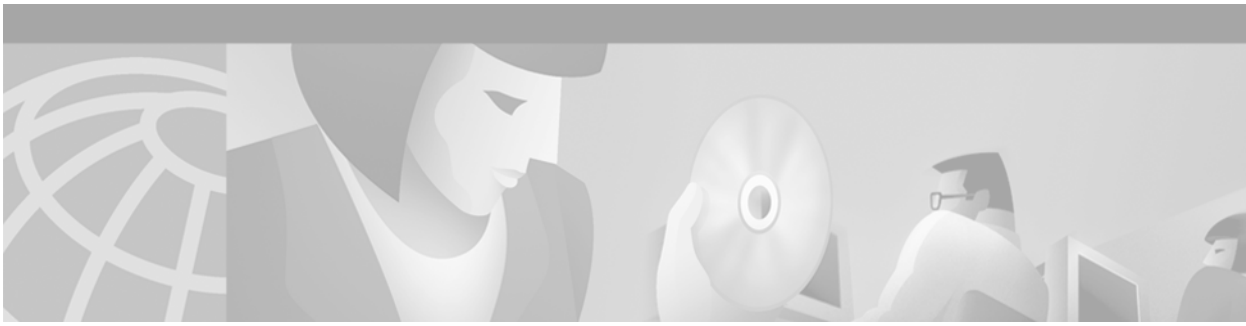

Release Notes for Cisco ONS 15454 SDH Release 4.1.2

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

November, 2003

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 4.1 and 4.5" 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 4.1.2, 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

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15454 SDH Release 4.1.2* since the production of the Cisco ONS 15454 SDH System Software CD for Release 4.1.2.

There are no changes to the release notes for Release 4.1.2.

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.

CWDM and DWDM GBIC Compatibility with G1000-4 Cards and G1K-4 Cards

Existing G1000-4 cards are expected to support CWDM and DWDM GBICs, but final qualification testing was not complete at press time. The online version of the 4.1 user documentation and release notes will be updated to reflect the final qualification status of CWDM and DWDM GBICs on the G1000-4 card, when this information is available.

Existing G1K-4 cards do not support CWDM or DWDM GBICs.

G1K-4 cards with the CLEI code of WM5IRWPCAA (manufactured after August 2003) are expected to support CWDM and DWDM GBICs, but final qualification testing was not complete at press time. The online version of the 4.1 user documentation and release notes will be updated to reflect the final qualification status of CWDM and DWDM GBICs on the G1K-4 card with the CLEI code of WM5IRWPCAA, when this information is available.

Note Operating temperature of the DWDM GBICs is -5 degrees C to 40 degrees C.

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 # CSCdy00622

Very rarely, an Equipment Failure Alarm can occur on an externally timed TCC+ or TCC-I card after a reset. If this occurs, BITS will be displayed as good for one TCC, but bad for the other. If the issue occurs on the standby TCC, a second reset could clear the problem. If the issue occurs on the active TCC, the card must be replaced. This issue is closed, as it does not occur with TCC2, and is otherwise very rare.

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.

Line Cards

DDTS # CSCec49231

In an LMSP 1+1 configuration, followint 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 will be resolved in a future release.

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 will be resolved in Release 4.6.

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 # CSCeb19055

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

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.

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 will be resolved in a future release.

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 will be resolved in a future release.

DDTS # CSCeb34655

Very rarely, E1-42 takes greater than 2 second hits on an active XC-VXL pull. To avoid this issue, side switch the XC-VXL cards. This issue will be resolved in a future release.

DDTS # CSCeb43397

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 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 TCCi/2 Card Removal

Active cross connect or TCCi/2 cards should not be removed. If the active cross connect or TCCi/2 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 TCCi/2 will be removed (performing a lockout on all spans will also accomplish the same goal). No lockout is necessary for switches initiated through CTC.

Caution If you mistakenly remove an active cross connect or TCCi/2 card and you subsequently lose traffic on some interface cards, you may need to physically reset these cards if they fail to regain traffic.

DDTS # CSCdz21738

A cross connect card switch can result in double traffic hits or a long hit for a E1-VC12 circuit. This issue is under investigation.

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 will be resolved in a future release.

SONET and SDH Card Compatibility

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

Table 1 SDH Data Cards that are SONET Compatible

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

Table 1 SDH Data Cards that are SONET Compatible

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

Table 2 SONET Data Cards that are SDH Compatible

Product Name	Description
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.

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

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 will be resolved in Release 4.6.

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 # 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 will be resolved in Release 4.6.

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 # 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 will be resolved in a future release.

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 be resolved in a future release.

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 # CSCdz87944

Error messages indicating “Stuck Ucode” and “MDA_INTERNAL_ERROR” occur when routing 64-byte VLAN tagged frames at line rate. For VLANs, use bridging instead of routing. This issue will be resolved in a future release.

DDTS # CSCea01675

Packets without an 802.1q VLAN tag are classified as COS 0. This issue will be resolved in a future release.

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 will be resolved in Release 5.0.

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 # 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 will be resolved in a future release.

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.

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 will be resolved in Release 4.6, and in a future maintenance release of Release 4.1.

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 # 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 will be resolved in a future release.

DDTS # CSCeb12032

When upgrading the software from Release 4.0 to Release 4.1, a TU-AIS will be reported on the span card for a one way VC12 E1-42 circuit. The alarm cannot be cleared once it is detected. This issue will be resolved in a future release.

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 will be 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 will be resolved in Release 6.0.

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 will be resolved in Release 5.0.

Changed Default Alarm Severities

The following alarm severities have changed for Release 4.1.x.

Table 4 Changed Alarm Severities

Alarm	New Severity
VT-MON::AUTOSW-LOP	NSA-Minor
VT-MON::AUTOSW-UNEQ	NSA-Minor
VT-TERM::PLM-V	SA-Major
VT-TERM::LP-TIM	SA-Major

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 # 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 will be displayed 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 will be 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 will be resolved in Release 5.0.

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 will be resolved in Release 5.0.

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 under investigation.

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 under investigation.

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 is currently under investigation.

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. There are no plans to resolve this issue at this time.

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 be resolved in a future release.

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 # CSCec32195

Rarely, in a two fiber MS-SPRing with STM64 span cards and a VC3 circuit running across DS3I drop cards, if you upgrade to Release 4.1.2 the TU-LOP alarm might be falsely reported against the STM64 trunk card even though traffic is passing fine. It is not known when or when this issue will be resolved.

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 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 BLSR configuration. This issue will be resolved in Release 4.6.

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 # 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 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 be resolved in a future release.

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 will be resolved in Release 5.0.

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 will be resolved in a future release.

DDTS # CSCdy56668

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 under investigation.

DDTS # CSCdy48872

Issuing a lockout span in one direction while a ring switch (SF-R) is active in the other direction may result in a failure to restore PCA circuits on the ring.

To see this issue, on a node participating in a two fiber MS-SPRing with PCA circuits terminating at the node over the two fiber MS-SPRing, cause an SF-R by failing the receive fiber in one direction (say, west). Then issue a lockout span in the other direction (in our example, east). Since the lockout span has higher priority than the SF-R, the ring switch should clear and PCA traffic should be restored on spans without a fiber fault. The ring switch does clear, but PCA traffic does not restore. To correct this issue, clear the fiber fault. All traffic restores properly. This issue will be resolved in a future release.

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.

DDTS # CSCea23862

After you perform a force switch on one of the spans of a DRI or IDRI topology with SNCP DRI circuits present, if you then apply a clear on the same span, the state will not show up immediately in CTC. This issue is under investigation.

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 will be resolved in Release 5.0.

Active Cross Connect or TCCi/2 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 TCCi (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 TCCi/2 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 TCCi/2 will be removed (performing a lockout on all spans will also accomplish the same goal). No lockout is necessary for switches initiated through CTC.

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 will be resolved in a future release.

Documentation

The following two notes on page 5-30 of the Cisco ONS 15454 Reference Manual, R4.1 and R4.5 should be replaced.

Note G-Series cards manufactured before August 2003 do not support DWDM GBICs. G1000-4 cards compatible with DWDM GBICs have a CLEI code of SNP8KW0KAB. Compatible G1K-4 cards have a CLEI code of WM5IRWPCAA.

Note All versions of G1000-4 and G1K-4 cards support CWDM GBICs.

The replacement information is contained in CWDM and DWDM GBIC Compatibility with G1000-4 Cards and G1K-4 Cards, page 3.

Resolved Caveats for Release 4.1.2

The following items are resolved in Release 4.1.2

Line Cards

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 4.1.2.

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 4.1.2.

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 4.1.2.

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 4.1.2.

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 4.1.2 and 4.6.

ML Series

DDTS # CSCin25238

If you configure Fast EtherChannel and POS-channel in the same bridge group, during system boot, the Fast EtherChannel or POS-channel configuration may be lost and following error message displayed:

```
Interface FastEthernet1 is attempting to join Port-channel1. But Port-channel1
belongs to bridge-group 1 which has another FE(C) member in it. FEC + FE(C) is not
allowed in the same bridge group. Please change your configuration and retry.
```

This issue is resolved in Release 4.1.

DDTS # CSCea18623

To avoid possible ML-series card resets when adding interfaces to a bridge group, always configure the Spanning-Tree Protocol for the bridge group (using the **bridge** *number* **protocol** command) before performing any other configuration on the bridge group.

If you want to use a bridge group that does not run the Spanning-Tree Protocol, you must first configure the bridge group with the Spanning-Tree Protocol, and then disable the Spanning-Tree Protocol for that bridge group on every interface where it is used (using the **bridge-group** *number* **spanning-disabled** interface configuration command). This issue is resolved in Release 4.1.

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 4.1.2.

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 4.1.2 and 4.6.

Maintenance and Administration

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 4.1.2.

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 4.1.2.

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 4.1.2 and 4.6.

DDTS # CSCea19297

For any STS or VT circuit that terminates on a node, an AIS (path level) that raises and clears on that circuit's path may result in an inability of other path alarms to be cleared. This can also occur when a line-level alarm occurs on the circuit path's line, causing the OC-N to send AIS-path downstream on each path within the line. This issue is resolved in Release 4.1.

DDTS # CSCea21686

Retrieving a diagnostic file may cause a Standby or Active TCC2 reset. This is not traffic affecting. This issue is resolved in Release 4.1.

MS-SPRing Functionality

DDTS # CSCdy65890

If you have PCA circuits over two-fiber or four-fiber MS-SPRing protect channels, an incorrect auto-inservice transition occurs after traffic preemption. You may place the circuit back into the OOS-AINS state after the BLSR has returned to the unswitched mode, using the Circuit Editing pane of the CTC. This issue is resolved in Release 4.1.

SNCP Functionality

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 4.1.2.

DDTS # CSCec14995

In a non-revertive SNCP configuration, when a double failure is detected on both paths with UNEQ-P or AIS-P, upon clearing the protect path defect, the UNEQ-P or AIS-P alarm may remain stuck on the working path for the node. The most reliable way to remove the alarm is a TCC2 side switch. This issue is resolved in Release 4.1.2.

New Features and Functionality

This section highlights new features and functionality for Release 4.1.x. For detailed documentation of each of these features, consult the user documentation.

New Software Features and Functionality

CTC Additional Support for DS3i-N-12

As of Release 4.1.2 the column “Path Width” has been added to Alarms, Conditions and History panes. The Path Width column provides the width of the VC4 path on which the alarm is raised or cleared, in units of VC4 (how many VC4s wide the path is). The path width only applies to the “VC4-” alarmable object type. For any non-VC4 object, the column remains blank.

ML-Series Resilient Packet Ring

RPR (Resilient Packet Ring) is a new protocol available on the ML-Series cards enabling you to use SDH bandwidth more efficiently, with 50 ms recovery times.

Basic Feature Description

RPR for the ML-Series line cards provides a set of enhancements to the performance of any such card running the Release 4.1.x. These improvements include:

RPR for the ML-Series line cards allows new deployment applications for all cards running Release 4.1.x. These improvements include:

- Better SDH bandwidth utilization compared to an STP controlled ring topology.
- Non-SDH fail-over mechanism with sub 50-millisecond convergence for fiber cuts, restores, node failures and inserting new nodes.
- Ability to perform ML-Series QOS (quality of service) features on all SDH traffic (pass-through, drop, and add).
- No hardware changes: Only requires ONS 15454 Release 4.1.x, which includes the new IOS configuration.
- Increased number of supportable VLANs and MAC addresses on the ring.
- A scalable, inter-ring protection mechanism for increased network resiliency.
- The addition of RPR does not remove any Release 4.0 functionality. RPR features are enabled via a new set of configuration commands.

For further details of RPR uses and features, consult the user documentation for Release 4.1.

Open Ended SNCP

In previous releases, you could create an end-to-end SNCP circuit on any Cisco ONS 15XXX network using A-Z provisioning of CTC/CTM. This feature requires you to specify one source node and one destination node of a SNCP circuit. CTC/CTM requires these nodes to be part of the network that is discovered by CTC/CTM.

With Release 4.1.x you can create an open ended SNCP circuit in addition to a regular SNCP. An open ended SNCP circuit is a partial SNCP circuit. This feature helps you create end-to-end SNCP circuits where a part of the given SNCP circuit is on a Cisco 15XXX network, while the other part of the circuit is on another vendor's equipment. The circuit may consist of one source point and two end points. There are two paths from the source; one path is from the source to one end point and the other path is from the source to the other end point. The source has a bridge that sends the traffic on both paths. The end points do not have any selectors and may hand off the traffic to another vendor's equipment. For bidirectional circuits, the source also contains a selector for the reverse traffic from end points to source.

Alternatively, open ended SNCP can be used to create a circuit with two sources and one destination. In the unidirectional case, the destination node has a selector, and the source nodes have one-way connections.

NE Defaults

The NE defaults pane user interface is changed in Release 4.1.x as follows:

- The NE defaults pane now has a highlighted title at the top of the pane, indicating the last action taken by the user.
- If you import or export a file, the title shows the file name and the time of the action.
- If you load or apply a file to the node, the changes and the time of the action will be displayed.

User Privileges

As of Release 4.1.x, The following user privileges have changed:

- A Maintenance level user can back up the database and transfer a software package to the node.
- A Provisioning level user can delete and reset cards.

Protect Threshold Crossing Alarms

As of Release 4.1.x, BLSR/MS-SPR and path protection/SNCP protect thresholds at both the card and port level are inherited from the working card/port.

Gigabit Ethernet Transponder

The Gigabit Ethernet Transponder is a software enhancement to existing G-series Ethernet cards that allows these cards to support transponder functionality.

The following features support Gigabit Ethernet Transponder functionality for Release 4.1.x.

Note In this section, unless otherwise mentioned, all items apply equally to both G1000-4 cards and G1K-4 cards. Some capabilities also apply to G1000-2 cards for the ONS 15327.

CWDM GBICs

Note This applies only to the ONS 15454-based G-series cards (G1000-4 and G1K-4).

CWDM GBICs correspond to the eight wavelengths supported by the Cisco CWDM GBIC solution on the ONS 15454: CWDM-GBIC-1470, CWDM-GBIC-1490, CWDM-GBIC-1510, CWDM-GBIC-1530, CWDM-GBIC-1550, CWDM-GBIC-1550, CWDM-GBIC-1570, CWDM-GBIC-1590.

DWDM GBICs

This applies only to the latest revision of the ONS 15454-based G-series cards (G1000-4 and G1K-4).

DWDM GBICs correspond to the 32 different ITU-100GHz wavelengths supported on the ONS 15454: 1530.33, 1531.12, 1531.90, 1532.68, 1534.25, 1535.04, 1535.82, 1536.61, 1538.19, 1538.98, 1539.77, 1540.56, 1542.14, 1542.94, 1543.73, 1544.53, 1546.12, 1546.92, 1547.72, 1548.51, 1550.12, 1550.92, 1551.72, 1552.52, 1554.13, 1554.94, 1555.75, 1556.55, 1558.17, 1558.98, 1559.79, and 1560.61. The ONS 15454 version DWDM GBICs are the only officially supported DWDM GBICs for the G-Series Ethernet cards. These GBICs have wideband reception capability and can receive with adequate sensitivity across the 1260-1620 nm range (refer to GBIC specs in the user documentation for details). This capability can be exploited in some of the transponder applications.

GBIC Notes

New GBICs are supported for only those vendors/brands that are officially certified for use on the ONS 15454.

GBIC inventorying functions are not currently supported. However, the type of GBIC plugged in and the wavelength used are displayed to CTC and TL1 users (as well as CTM users when CTM support is added).

Performance monitoring of optical parameters such as DWDM power levels per wavelength are not supported in Release 4.1.x.

The GBIC security feature is not supported in Release 4.1.x.

Three Transponder Modes of Operation

Release 4.1.x supports three transponder modes of operation:

Bidirectional 2-port transponder

Bidirectional 1-port transponder

Unidirectional 2-port transponder

This applies only to the ONS 15454-based G-series cards (G1000-4 and G1K-4). This feature also includes the ability of the cards to operate (when in transponder mode) independent of the cross connect cards and even operate without any cross connect cards in the shelf.

When at least one port is provisioned in a transponder mode, the entire card will be in transponder mode. When SONET/SDH circuits are provisioned on a card, the card is said to be in normal/SONET/SDH mode.

Hybrid mode of operation is not supported in Release 4.1.x. At any given time, a card can be either in transponder mode (with one or more ports being provisioned to provide transponder capabilities) or in normal SONET/SDH mode. A mixed or hybrid mode (in which only some ports are performing transponder functions while others are switching traffic into the SONET/SDH network) is not supported and you will be prevented from provisioning such a combination. In order to move a card from SONET/SDH mode to transponder mode you must first delete all SONET/SDH circuits terminating on the card, after which ports will become provisionable as transponders. Similarly you must first turn off transponder mode on all ports before a card can become eligible for SONET/SDH circuits again.

Facility Loopback

Facility Loopback is supported for Release 4.1.x transponder functionality.

This applies to all G-series cards (G1000-4 and G1K-4 on the ONS 15454 and G1000-2 on the ONS 15327).

Provisionable Flow Control Watermarks

Provisionable flow control watermarks are supported for Release 4.1.x. This capability enables the user to tune the flow control mechanism on the G-Series cards for some network applications.

This applies to all G-series cards (G1000-4 and G1K-4 on the ONS 15454 and G1000-2 on the ONS 15327).

Changed Alarms

The following alarms have changed as of Release 4.1.x.

SDH CRITICAL Alarms

LOC is added in Release 4.1.x.

SDH MAJOR Alarms

SQUELCHED is MJ in Release 4.0 but changed to NA in Release 4.1.x.

FEC-MISM is added in Release 4.1.x.

SDH MINOR Alarms

LP-PLM is MN in Release 4.0 but changed to MJ in Release 4.1.x.

LP-TIM is MN in Release 4.0 but changed to MJ in Release 4.1.x.

SDH Conditions

BAT-A-HGH-VLT is in Release 4.0 and Release 4.1.x but unused.

BAT-A-LOW-VLT is in Release 4.0 and Release 4.1.x but unused.

BAT-B-HGH-VLT is in Release 4.0 and Release 4.1.x but unused.

BAT-B-LOW-VLT is in Release 4.0 and Release 4.1.x but unused.

INTRUSION-PSWD is added in Release 4.1.x.

LPBKFACILITY (G-Series) is added in Release 4.1.x.

Related Documentation

Release-Specific Documents

- *Release Notes for Cisco ONS 15454 SDH Release 4.1.1*
- *Release Notes for Cisco ONS 15454 Release 4.1.2*
- *Release Notes for Cisco ONS 15327 Release 4.1.2*

Platform-Specific Documents

- *Cisco ONS 15454 SDH Installation and Operations Guide, Release 4.1 and 4.5*
- *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide, Release 4.1 and 4.5*
- *Cisco ONS 15454 SDH Product Overview, Release 4.1 and 4.5*

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.