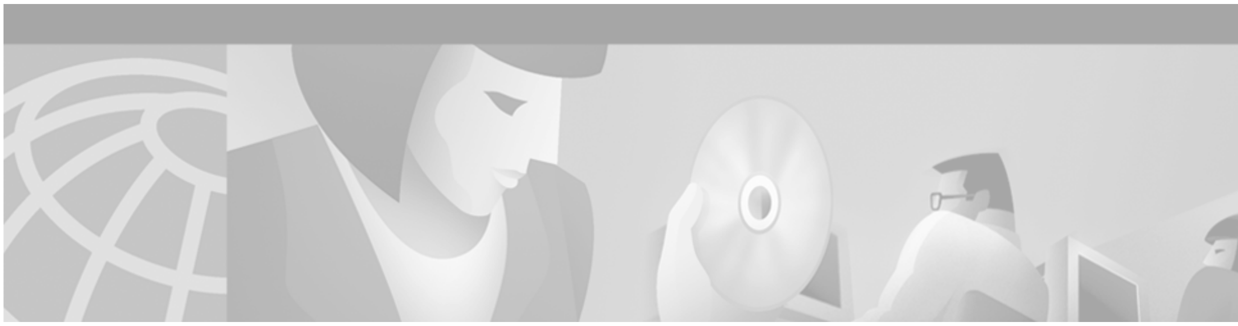

Release Notes for Cisco ONS 15454 Release 3.2.1

July, 2002

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15454 SONET multiplexer. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to Release 3.2. of the *Cisco ONS 15454 Installation and Operations Guide*, *Cisco ONS 15454 Troubleshooting and Reference Guide*, and *Cisco ONS 15454 TL1 Command Guide.* For the most current version of the Release Notes for Cisco ONS 15454 Release 3.2.1, visit the following URL:

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

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

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

Contents

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 Release 3.2.1* since the production of the Cisco ONS 15454 System Software CD for Release 3.2.1.

The following changes have been added to the release notes for Release 3.2.1.

Changes to Caveats

The following caveats have been added.

- JRE Updates, page 7
- DDTS # CSCdy29683, page 8
- DDTS # CSCdy66962, page 8
- Pointer Justification Thresholds, page 8
- DDTS # CSCdw45877, page 8

Caveats

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

Line Cards

DDTS # CSCdx83373

DS1 traffic might remain down after removing and reinserting a locked XCVT. The DS1 traffic in this case can be recovered by either soft resetting the DS1 card or causing an XCVT switch. This issue is rare and will be resolved in a future release.

DDTS # CSCdx89498

If you remove and replace both XC10G cards, AIS-V and LOP-V alarms may appear and become stuck. To clear these alarms, reset the active TCC. This issue will be resolved in a future release.

DDTS # CSCdx95242

During an XC to XC10G upgrade, while switching from XC to XC10G, a switch time of up to 120 ms can occur. This can occur when using OC-48AS cards as source/destination cards, or as span cards. This issue will be resolved in Release 3.4, and is rare.

DDTS # CSCdx92109

Under very rare circumstances, you may not be able to provision a DS3 card after removal of previous DS3E card which was in protection group before. This will require an active TCC switch to provision the DS3 card. This issue is under investigation for resolution in a future release.

DDTS # CSCdw59020

CTNEQPT_PB alarms may be raised during a hardware upgrade from XC or XCVT cards to XC10G cards. The alarm will be raised if one of the following actions is performed during the XC or XCVT upgrade to XC10G, while the XC10G is active and the XC or XCVT is standby:

- resetting the standby XC or XCVT
- resetting an OC48AS in a trunk slot
- inserting a new OC48AS in a trunk slot
- switching from XC10G to XC or XCVT

If this issue occurs, switch from the XC10G back to the XC or XCVT, soft reset the OC48ASs in the trunk slots, and restart the upgrade process. This issue will be resolved in a future release.

DDTS # CSCdw66444

When an SDH signal is sent into an ONS 15454 BTC-48 based OC-12 or OC-48 port which has been configured to support SDH, an SD-P (Signal Degrade) alarm will appear as soon as the circuit is created. This alarm will continue to exist until the circuit is deleted.

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

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

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

DDTS # CSCdw57215

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

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.

DDTS # CSCdw09604

After an upgrade from XCVT to XC10G, nodes with older OC-48 cards (revision number 005D) can be subject to jitter problems on the transmit line, possibly causing B3 errors on the far end receiver.

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.

DDTS # CSCdv81011, CSCdu15203

When performing an XC/XCVT to XC10G upgrade on a two fiber BLSR configuration, Ethernet traffic disruptions can exceed seven minutes. This issue will be resolved in a future release.

DDTS # CSCdv80971

A service disruption of greater than 50 ms can occur on a working OC-3 card removal. This extended traffic disruption can occur on an OC-3 1+1 span on ports 3 or 4, with STS-3C traffic, when OC-3 cards are provisioned to have four OC-3 1+1 protection groups, and when all four ports are in service. This issue will be resolved in a future release.

DDTS # CSCdv80935

A DS-1 can raise an equipment fail alarm if there have never been any circuits provisioned on the card since the card was inserted in its slot. To correct this issue when it occurs, provision a circuit on the card. This issue will be resolved in a future release.

DDTS # CSCdv49271

In a network with a 1:1 protection group where Slot 1 has the protect card and Slot 2 has the working card, and where there is a VT circuit between the two cards, it is possible to create a situation wherein both cards are temporarily in the active state. This can occur if you switch traffic on the Slot 1 card, lock on the Slot 1 card, reseat the Slot 2 card, and then soft reset the Slot 1 card. Both cards will reboot simultaneously and both with come up active, and traffic may be lost. To avoid this problem, always wait for the working card to finish rebooting and go into standby before you reset the protect card. This issue will be resolved in a future release.

Active Cross Connect or TCC+ Card Removal

In BLSR, UPSR, and 1+1, you must perform a lockout before physically removing an active cross connect or TCC+ card. The following rules apply.

Active cross connect cards should not generally be physically removed. If the active cross connect or TCC+ card must be removed, you can first perform an XC/XCVT 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 TCC+ will be removed (performing a lockout on all spans will also accomplish the same goal). No lockout is necessary for switches initiated through CTC or through TL1.

DDTS # CSCdv62565, CSCdv62573

In a 1:N protection group, do not pre-provision a DS-N card and then add it to the group while an actual traffic-carrying card in the group is removed from its slot. This issue will be resolved in a future release.

DDTS # CSCdu71847: DS3 Equipment Protection

DS3N-12E and DS3N-12 cards can be provisioned in the same 1:1 or 1:N protection group only if a DS3N-12E card is the protect member. If a DS3N-12 card is chosen as the protect member, only the DS3-12 cards will be available to be the working members of that protection group. This applies to both the 1:1 and 1:N protection schemes. This functionality is as designed.

E Series and G Series Cards

Note When using ONS 15327s as passthrough nodes with Release 3.2.1, you cannot create 9c or 24c gigabit Ethernet circuits through any 15327.

Throughput/Latency Testing

When testing the G1000-4 for latency/throughput at, near, or above the maximum allowable line rate per the guiding specifications, IEEE 802.3 and 802.3z. Customers testing for Throughput or Latency may see throughput calculations that can vary from 100% to 99.98% throughput, depending on the accuracy of the test set clock and the variability of the clock on the G1000-4. As described in the text below, the G1000-4 is fully compliant with the specification for line rate gigabit Ethernet. However, during testing in the lab environment, technicians need to be cognizant of the throughput settings and accuracy of the clock on the test set to ensure that the variances in throughput seen on the G1000-4 are not mistakenly perceived as being out of specification. Further, it needs to be understood that such testing is not reflective of traffic conditions that would be experienced in real world networks.

IEEE 802.3 allows for a variation in the clock rate of +/- 100 parts per million (ppm), allowing a range of speeds to be considered conforming to the specification.

The legal range of for Gigabit Ethernet is an follows:

- Minimum Speed—1,487,946 Frames Per Second
- Nominal Speed—1,488,095 Frames Per Second
- Maximum Speed—1,488,244 Frames Per Second

Conforming devices may not vary the preamble size, start frame delimiter size, or reduce the inter packet gap. The G1000-4 is fully compliant with these parameters.

During lab testing with a throughput testing device (Spirent Smartbits, Ixia test devices, etc.), because of a speed variance between the ingress packets from the external device and the egress speed from the G1000-4, throughput can vary from 100 percent to 99.98%, depending on the difference in clock speeds between the devices. Due to the allowable variation of clock tolerance, Some G1000 cards transmit below the nominal clock speed for Gigabit Ethernet, but well within the IEEE specification. In fact, although the specification allows for +/- 100ppm of tolerance, the oscillator on the G1000-4 has been found to vary only between +/- 40ppm on average (G1000-4 clock never runs below the minimum speed of 1,487,946 frames per second outlined in the IEEE specification). We guarantee the +/- 100ppm per the specification.

Short duration traffic bursts that are above the nominal rate are buffered, thus traffic isn't dropped for bursty traffic above the nominal rate. However, sustained traffic that is above wirespeed will be buffered and at some point the buffers will overflow can result in a nominal amount of dropped packets. The G1000 card will never drop a single frame with test equipment that is running at -100 ppm of line rate.

This issue can only be witnessed in a lab environment, as it would require all of the following conditions to occur simultaneously in a real network in order to cause frame loss.

1. Sustained traffic that is above the minimum clock speed possible. For example, if the clock on the G1000 was running -100 ppm or 1,487,946 frames per second, the sustained traffic would have to last 53.69 seconds in order to cause frame loss. This is because there is a 149 frame per second mismatch and we can buffer 8,000 64 byte frames.
2. Traffic patterns that are fixed frame sizes with a constant minimum Inter frame Gap. This is not real world traffic and can only be produced by high end test equipment.

DDTS # CSCdw43919

When running traffic at 100% line rate with a repetitive data pattern, frame corruption and loss may occur for approximately one to three percent of the frames. This issue can occur when all of the following conditions are present:

- 100% line rate traffic.
- Attached device clock rate is greater than the G1000-4 clock rate (even if within the 100 ppm tolerance range of IEEE 802.3).
- Repetitive data patterns—this issue is not seen with random data patterns, even if the other conditions are met.

There are two ways to avoid this issue:

1. Use varying or random data frames for line rate performance measurements.
2. If fixed repetitive data patterns must be used for testing, use an “all zeros” data pattern in the frame, including all-zero source and destination MAC addresses. This pattern is known to not exhibit the problem. You can also experiment with varying the data patterns one bit at a time in order to determine other fixed patterns that will not exhibit the problem.

In summary, this problem will only be exhibited in test scenarios, for which the above workarounds can be used, and the probability of occurrence is extremely remote.

The resolution for this issue will be released with a PCN, which improves the tolerance of the transmit clock.

DDTS # CSCdv76022

In a network running multicard Etherswitch over BLSR, an Ethernet traffic loss can occur after a power cycle. To correct this issue when it occurs, wait until the Ethernet cards are in the active state, then reset the standby cross connect card, and finally, reset the active cross connect. This issue will be resolved in a future release.

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

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

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

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

Multicard EtherSwitch

When deleting and recreating Ethernet circuits that have different sizes, you must delete all STS circuits provisioned to the EtherSwitch before you create the new circuit scenario. (See the preceding "Single-card EtherSwitch" section on page 7 for details on the proper order of circuit creation.) Enable front ports so that the VLANs for the ports are carried by the largest circuit first. A safe approach is to enable the front port before you create any circuits and then retain the front port VLAN assignment afterwards. If you break the rules when creating a circuit, or if you have to delete circuits and recreate them again, delete all circuits and start over with the largest first.

DDTS # CSCds02031 E1000-2/E100

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

Maintenance and Administration

JRE Updates

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

DDTS # CSCdy29683

For some combinations of concatenations that include STS-24C along with STS-1 and/or STS-3C, some circuits become blocked from provisioning (typically the STS-24C). When using CTC/CTM the G1000 card is not listed as a possible candidate for the circuit. If you are creating all circuits from the beginning, Cisco recommends you create the STS-1 and STS-3C circuits to be dropped on a card first and the remaining circuits afterwards. Alternately, if some circuits have already been created and you find you need to work around this issue, you can delete some or all circuits and retry the combination by creating all 1s and 3Cs first. This issue will require a future revision of hardware before it can be resolved.

DDTS # CSCdy66962

Creating circuit at the card level view can cause CTC to lock up. To avoid this issue do not create circuits at the card level view. This issue is resolved in software Release 3.3.

Pointer Justification Thresholds

CTC displays four Pointer Justification (PJ) thresholds. Only the first value is used as a threshold for all PJ counts. The second value is changeable but ignored. The 3rd and 4th are not changeable. TCAs are generated for PPJC-PDet, NPJC-PDet, PPJC-PGen, and NPJC-PGen using the one threshold (PPJC-PDet).

DDTS # CSCdw45877

In releases prior to 3.4, the ONS 15454 software restricts STS starting positions for 6C and 9C paths on OC-N cards to those that are even multiples of the path width. For instance, a 9C, may only start on STSs 1, 10, 19, 28, and so on. So, for example, if you first configure a 12C across a 2-fiber OC-48 BLSR such that it starts on STS 1, you will not be able to configure a 9C on the remaining 12 working STSs (recall that there are only 24 working STSs on a 2-fiber OC-48 BLSR). If, on the other hand, you first create the 9C to use STS 1, then the 12C may still use STS 13. Cisco suggests that you plan your 9C circuits with this limitation in mind.

Keep these starting STS rules in mind in any case where circuit is not provisionable on a card, even when there is enough bandwidth to support the circuit, regardless of whether BLSR is being used or not.

This issue is resolved in Release 3.4.

DDTS # CSCdy03991

The maximum number of bidirectional VT circuits allowable on an XCVT card is 224. In a UPSR, when using the CTC autorange function to create 224 VT circuits where either the source or destination card is a DS3, DS3XM, or EC1 card, the circuit creation will complete successfully but the last 28 circuits will not carry traffic. If this issue arises, reset the active XCVT card. This issue will be resolved in a future release.

DDTS # CSCdx96160

When there are two CTC sessions open at the same time, and you perform an operation in one CTC session, very rarely, status information is not updated for the other concurrently running CTC session. When this occurs, exceptions will be visible in the CTC Debug Window (<Ctrl>-<Shift> and then Help/About). To recover from this situation, restart the CTC session that is not being updated. This issue will be resolved in a future release.

DDTS # CSCdy03597

If you enter an invalid subnet mask, IP address, or other parameter through the LCD panel, you will receive a message stating that the changes were not saved, and in fact, the changes will not be applied, but the value you entered might become stuck in the display. To correct this, you must reset the TCC. This issue will be resolved in a future release.

ONS 15454 Conducted Emissions Kit

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

Upgrading to Use the G1000-4 Ethernet Card

Before installing or seating the G1000-4 Ethernet card on node running Release 3.1 or prior, you must upgrade the software on that node to Release 3.2.1. This is as designed.

DDTS # CSCdw64191

When testing throughput and latency of STS-24c circuits on the G1000-4 card, Gigabit Ethernet utilization must be no more than 99.98%. If utilization exceeds this rate, an increase in latency will result. This is an unlikely scenario in a production network, considering dynamic frame sizes, patterns, utilization rates, and interframe gaps. This issue will be resolved in a future release.

DDTS # CSCdw61550

When upgrading the software from Release 3.1 to Release 3.2.1 and subsequently reverting back to Release 3.1, a one-way Ethernet traffic loss may occur after the revert. This issue has been seen after a multicard STS-6c circuit is created. The traffic loss will show LOP-P on OC-192 and AIS-P on E1000 cards. To revive traffic, perform a cross connect switch. This is a Release 3.1 issue that is resolved with Release 3.2.

SNMP Payload Visibility

Release 3.1 SNMP reports path/payload level alarm traps (such as AIS-P, PDI-P, etc.) against line0 without payload information. Release 3.2.1 provides payload visibility into SNMP traps for path/payload level alarm traps).

DDTS # CSCdw59020

Cisco does not support downgrades from XC10G to XC or XCVT cards. In a future release Cisco will, however, support downgrades that occur during the upgrade process, in the event that circumstances make this necessary. There are no plans to implement further downgrade support.

DDTS # CSCdw58071

Users of both CTC and TL1 are able to specify a G1000 card as a secondary source or destination as if it were an OC-N trunk card.

When you create a circuit in CTC and select the G1000 card, the Secondary Source/Destination checkbox is not grayed out. Checking this box allows the selection of another G1000 port as a secondary drop.

Similarly, in TL1 the following command creates a UPSR cross-connect with primary and secondary drops on the G1000 card (in slot 4 in the example):

Example 1 ent-crs-sts3c::fac-4-1&fac-4-2,sts-2-1:1;

Neither of these procedures is supported. To avoid possible problems, do not execute either of the two procedures described above.

This issue will be resolved in Release 3.30.

DDTS # CSCdw47506

A CTC communications failure on the network during circuit creation can cause a “Circuit Provisioning Error” exception. An attempt to continue with the errored circuit creation results in other exceptions that occur repeatedly on each attempt to continue. This issue has been seen infrequently, and only on large networks. To correct the problem, abandon the attempted circuit creation and start over. This issue will be resolved in a future release.

DDTS # CSCdw03281

Under certain conditions, the CTC GUI freezes. To recover from this condition, you must restart CTC. This behavior has only been seen when all of the following conditions are met:

- 2 sets of 6 nodes, each node connected to 4 of the other nodes in its set
- Circuits total at least 850
- Several operations occur over a short period
- JRE 1.2.2 is running on the workstation running CTC

Upgrade to JRE 1.3.1 to resolve this issue.

DDTS # CSCct03396 Ring Map Change Dialog Box

In Releases 2.0-2.2.2 and 3.0-3.1, when you add a node to a BLSR, CTC displays a Ring Map Change dialog box asking you to accept the change. If you browse away from the node view before this dialog box has appeared, the dialog box may fail to appear, or may come up behind another window. This issue will be resolved in a future release.

DDTS # CSCdv72344

Provisioning multiple VT 1.5 circuits using auto-ranging can put a strain on the node, causing some other nodes to temporarily appear as grayed-out in the network view. To prevent excess stress on the node, reduce the number of auto-ranged circuits created per batch. This issue will be resolved in a future release.

DDTS # CSCdv81633

In Release 3.1, TL1 and CTC report the equipment type for an XC10G card as “XC192.” This can be seen in the alarm messages generated after an XC10G card is removed from its slot. Also, SNMP reports a “powerFailRestart” when an XC10G card is removed. These issues will be resolved in a future release.

DDTS # CSCdv62990

Telcordia GR-815 requires that a new password must have at least 1 numeric character (0 to 9) and at least one special character from the character set {plus-sign (+), pound-sign (#), percent-sign (%)}. CTC normally issues a warning if the password is non-compliant, but allows you to create the password. However, CTC does not issue a warning when a new password is requested that has two special characters, but no numeric component. Thus, for example, there is no warning in CTC for the password aaaa++, which lacks the numeric character and is non-compliant.

DDTS # CSCdt94185

CTC can fail to drop user initiated switch requests (Manual or Force) when a higher priority request is initiated. This issue can arise when a switch request is made by the user and then another, higher priority request is made. CTC should preempt the user request with the higher priority request. If CTC fails to clear the request, manually clear the request. This issue will be resolved in a future release.

DDTS # CSCdv10824: Netscape Plugins Directory

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

DDTS # CSCdu82934

When you auto-route a VT circuit on an ONS 15454 node, a path is computed based on the availability of STSs on the nodes involved. This selection process, when combined with a lack of VT matrix (or STS-VT connections) on an auto-route selected node, can result in the VT circuit creation failing with the message “unable to create connection object at node.” To correct this situation, manually route VT circuits in cases when auto-routing fails. The error message will indicate which node is at issue.

OSPF Virtual Links

When ONS 15327s are DCC-connected you cannot use OSPF virtual links. This issue will be resolved in a future release.

DDTS # CSCdu19246: CTC Protection Pane Displays Protect/Standby on Pulled Card

The CTC Protection pane that displays the status of protection groups might not refresh to reflect that a protect card has been removed. The Improper Removal alarm is raised, however.

DDTS # CSCdt88289: Processing of FEAC Loopback Commands

FEAC loopback commands issued in specific scenarios may not be processed appropriately unless a deactivate FEAC loopback command is sent first. To clear the FEAC loopback, put the port Out of Service, perform a manual loopback, or change the framing mode to a mode other than C-Bit. The FEAC loopback state is cleared correctly in CTC and the DS3E card, but currently, a loop down command (for example, deactivate FEAC loopback) needs to be sent before the DS3E will process loop up commands. This issue will be resolved in Release 3.3.

"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.

Interoperability

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

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

BLSR Functionality

DDTS # CSCdy06778

In a 2 fiber BLSR you can isolate a node using LOS on one span and Force Ring Switch on the other span. In this scenario clearing the LOS will result in a traffic hit of more than 60 ms for the traffic that switches back to the working path. This issue will be resolved in a future release.

DDTS # CSCdy03629

Under rare circumstances, you may be unable to create a VT tunnel on a BLSR span. This issue has occurred only once, with a 4 node, 2 fiber OC-192 BLSR, in combination with two other ring types, and some provisioning in place. If this occurs, it can be corrected by resetting the TCC cards on the affected nodes. This issue will be resolved in a future release.

DDTS # CSCdw79328

Traffic with bit errors can fail to switch when a unidirectional signal degrade occurs on the working span and a unidirectional signal fail occurs on the protect span between the same two nodes, where one condition is detected by each node. To correct this problem when the protect span is still failed, issue a Force switch-ring on the working span that detected SD. To correct this problem when the protect has been restored and the working still detects SD, issue a Force switch-span on the protect span that detected SF. Before clearing the issued force command (either "force-ring" or "force-span") make sure that at least one of the line conditions has been cleared properly. It is critical that you do not clear the force command until one of the failures has been cleared. This issue will be resolved in Release 3.3.

DDTS # CSCdv70175

Release 3.1 introduced the support of up to two BLSRs per node; this includes support for one 4 Fiber BLSR and one 2 Fiber BLSR on the same node. When configuring a node with one 4 Fiber BLSR and one 2 Fiber BLSR, an issue was found related to the version of XC deployed. Revision 004H and earlier revisions of the XC do not support this configuration. All later revisions of the XC and all versions of the XCVT and XC10G cross connects support all permutations of two BLSRs per node.

DDTS # CSCdw57215

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

DDTS # CSCdw45196

In a BLSR configuration with a node isolated from the ring, the span cards on the nodes connected to the isolated node normally send out AIS-P. However, if the span cards receive any new provisioning messages while in squelch mode, the squelch AIS-P is mistakenly cleared. To avoid this problem, do not perform any provisioning while a node is isolated. This issue will be resolved in Release 3.3.

DDTS # CSCdw48849

Some difficulty can be encountered on creating 336 VT 1.5 circuits over a four fiber BLSR. This has only been seen after creating 300 or more such circuits, in a ring where there may have been a communication problem with one of the nodes in the ring. This issue will be resolved in a future release.

DDTS # CSCdv80859

Using the span upgrade procedure to perform a two fiber to four fiber BLSR upgrade, or performing the upgrade while the BLSR is in any switching state, can cause traffic disruption. This issue is more likely to arise in a non-revertive ring. To avoid traffic loss, force a lockout over the entire ring (as you would before a software activation) to prevent the ring from switching during the upgrade. If for some reason you are unable to perform the lockout beforehand, and you experience a traffic disruption, traffic can only be recovered by a soft reset both active and standby cross connect cards. This issue will be resolved in a future release.

> **Note** BLSR protection is not functional during this upgrade, so locking out the ring does no harm.

DDTS # CSCdv74761

An EC1 card on a BLSR node that is squelching traffic generates a UNEQ-P alarm. This occurs because BLSR does not send out AIS-P to the drop EC1 card (this only occurs with EC1), when the node squelches traffic. This issue will be resolved in a future release.

DDTS # CSCdv63336

On a Release 3.1 BLSR, when conducting a span upgrade to XC10G, watch for any rebooting of the active cross connect. This condition is rare; however, if the active cross connect does reboot, you must reboot it again after the span upgrade is complete. This issue will be resolved in a future release.

DDTS # CSCdv53427

In a two ring, two fiber BLSR configuration (or a two ring BLSR configuration with one two fiber and one four fiber ring) it is possible to provision a circuit that begins on one ring, crosses to a second ring, and returns to the original ring. Such a circuit can have protection vulnerabilities if one of the common nodes is isolated, or if a ring is segmented in such a way that two non-contiguous segments of the circuit on the same ring are each broken. This issue will be resolved in a future release.

DDTS # CSCct03919

VT1.5 BLSR squelching in BLSRs is not supported.

Database Restore on a BLSR

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

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

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

Step 3 After the TCC+ has reset and booted up, release the force switch from each node.

UPSR Functionality

Active Cross Connect or TCC+ Card Removal

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

Active cross connect cards should not generally be removed. If the active cross connect or TCC+ card must be removed, you can first perform an XC/XCVT 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 TCC+ will be removed (performing a lockout on all spans will also accomplish the same goal). No lockout is necessary for switches initiated through CTC or through TL1.

Documentation

AIP Card Replacement

When replacing an AIP card, you must record the old MAC address from the card before replacing it, as you will need the MAC address in the Circuit Repair procedure that follows the card replacement. The MAC address must be recorded before the TCC reset that follows the card replacement, or it will be lost. This issue will be resolved in Release 3.3. The documentation for Release 3.3 clarifies the need to record the MAC address.

TL1

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

DDTS # CSCdu53509

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

DDTS # CSCdw42351

On a DS3XM card, the DS1 AISP/ESP/SESP threshold crossing alerts list the facility and the VT that crossed the threshold. In Release 3.2.1, the positions of the facility and VT numbers may be transposed (swapped). To use the data effectively, record the VT and facility numbers elsewhere, in their correct (transposed) positions. This issue will be resolved in a future release.

Commands not Supported as of Release 3.0

The following Cross Connect commands are not supported as of Release 3.0:

ED-CRS-<STS_PATH>

ED-CRS-VT1

The following Equipment commands are not supported as of Release 3.0:

OPR-UPGRADE

Resolved Software Caveats for Release *3.2.1*

The following items are resolved in Release 3.2.1.

Line Cards

DDTS # CSCdx55434

In a 1+1 OC-48 configuration with a UNEQ-P condition on the working OC-48, the severity of the UNEQ-P is displayed as critical on the first working STS, but minor on others. This issue is resolved in Release 3.2.1

DDTS # CSCdx64148

Under very specific conditions, the TCC can reboot continuously after a software upgrade. Although very specific timing and memory allocation can trigger this issue, occurrence under actual operating conditions is exceedingly rare. In most cases, there is no workaround. In some circumstances, however, inserting a second XTC can alter internal timing in the offending XTC such that the issue may be avoided. This issue is resolved in Release 3.2.1.

DDTS # CSCdv83422

Removing or resetting the active cross connect on a node can cause a traffic disruption on an OC-12 or DS-3E card in that node. To avoid this issue, perform a side switch on the cross connect before resetting. This issue is resolved in Release 3.2.1.

DDTS # CSCdv76800

An OC-3 1+1 span carrying SDH traffic might experience a traffic disruption greater than 50 ms during a cross connect switch. This issue is resolved in Release 3.2.

DDTS # CSCdv74258

When an OC-192 or OC-48AS card is configured as the protect card in a 1+1 protection group, and is provisioned to operate in SDH mode, it may fail to transmit the expected zero value in bits 6 through 8 of a K2 byte. Other optical cards will report the zero value for K2 bytes as expected (for SDH). This issue is not traffic affecting.

In an all-Cisco network, this will pose no problems; however, if Cisco nodes inter-operate with a third party node, this could be an issue, depending on how that node responds to non-zero values in those bits. This issue is resolved in Release 3.2.

DDTS # CSCdv44837, CSCdv22992

When you perform an XC/XCVT to XC10G card upgrade following the procedure in *Cisco ONS 15454 Troubleshooting and Maintenance Guide*, Release 3.1, you may encounter a traffic disruption for a duration greater than 50 ms after you have switched to the XC10G. This issue is resolved in Release 3.2.

DDTS # CSCdv28419

E1000 cards with the part number (PN) 800-06746-03 do not fully meet the IEEE 802.3 specification for pulse mask. Multiple mask hits occur in region 1 of the mask. These cards may generate 8b/10b coding violations. Greater than 10% of sample cards with this part number have been observed to generate mask violations. Such mask violations are not expected to cause bit errors. The issue is addressed with Engineering Change Order E031468, implemented on September 20, 2001. Cards with a new PN, 800-06746-04, were issued. Mask violations from the 800-06746-04 cards are significantly less than 5% in samples tested. This issue is resolved entirely with ECO # E038294.

E Series and G Series

DDTS # CSCdx53004

An STS1 or STS3C circuit is sometimes not allowed to be provisioned on a G1000-4 card if there are certain other circuits already existing on the same card. This can happen under one of two scenarios:

If a G1000 card already has some circuits which have been provisioned via a Release 3.2 image with some large circuits (such as STS-24C, STS-12C or STS-9C) then, if new STS-1 or STS-3C circuits are attempted with a Release 3.3 image, these circuits may be disallowed.

Also, occasionally even if all circuits were provisioned by a Release 3.3 image but a few large circuits (like those above) were provisioned first then STS-1 or STS-3c circuits may be prevented from being provisioned.

In some cases similar symptoms may appear if the problem is due to a known initial hardware limitation (refer to the G1000-4 section of the user reference guide for details). The way to distinguish the two cases is that with the known hardware limitation the total sum of the circuit sizes of existing circuits and the new circuit has to be STS-36C or greater. If the total is less than STS-36C then you have this problem.

If, using the above test, you can determine with certainty that you have this problem, you can recover from it by deleting all the existing circuits on the affected card and then re-provisioning all of them, as well as the new circuit,

in the order of smallest circuit size first. However, deletion of all existing circuits may not be necessary if you can delete existing circuits until the total provisioned bandwidth is STS-24C or less and then start re-provisioning

circuits in order of smallest through largest. This issue will be resolved in Release 3.4, and is resolved in maintenance Release 3.2.1.

DDTS # CSCdx58347

When two circuits of width STS-24C and STS-9C are dropped on a G1000-4 card, and subsequently you attempt to drop an STS-1 or STS-3C on the same card, the card does not show up as a candidate card. To correct this issue, delete one or both circuits (24C and 9C), create all the STS-1 and STS-3C circuits needed, and then add back the STS-24C or STS-9c. This issue is resolved in Release 3.2.1.

DDTS # CSCdw61278

When running STS1 or STS3c circuits with G1000 traffic and executing an XC switch, a hit of 500 ms to 1.2 seconds is possible in the G1000 traffic. Before removing an XC card, make it the standby card (by switching from the management interface). This issue is resolved in Release 3.2.1.

DDTS # CSCdw69347

When sending frames greater than 16384 bytes that also have a valid and matching Ethernet CRC over the G1000-4, the link between the ports can sometimes toggle up and down. The receiving port should discard oversized packets, rather than bringing the link down. In practice, no real-world device is expected to generate frames that are both greater than 16384 bytes and also have a correct Ethernet CRC. This issue is most likely to be seen when using test equipment in the lab (which can be set up to generate frames which are both greater than 16384 bytes and have a correct CRC), rather than with real world Ethernet switches or routers. This issue is resolved in Release 3.3.

DDTS # CSCdw69347

When sending frames greater than 16384 bytes that also have a valid and matching Ethernet CRC over the G1000-4, the link between the ports can sometimes toggle up and down. The receiving port should discard oversized packets, rather than bringing the link down. In practice, no real-world device is expected to generate frames that are both greater than 16384 bytes and also have a correct Ethernet CRC. This issue is most likely to be seen when using test equipment in the lab (which can be set up to generate frames which are both greater than 16384 bytes and have a correct CRC), rather than with real world Ethernet switches or routers. This issue is resolved in Release 3.2.1.

DDTS # CSCdx05444

If a circuit already exists on a G1000-4 card, the provisioning of any subsequent circuit can cause bit errors up to 1 ms on the existing circuit(s). The only affected circuit size found in testing is 24c. This issue is resolved with Release 3.2.1.

Maintenance and Administration

DDTS # CSCdx69931

The Conditions tab does not show a timestamp on each fault condition to show when it was raised. This is not a bug, but rather, an unsupported feature. Timestamps were added in maintenance Release 3.2.1, and will be added to all products thereafter.

DDTS # CSCdx48853

The Cisco ONS 15454 optical transport platform is vulnerable when IP packets with the Type Of Service (TOS) bit enabled are sent to the Timing Control Card (TCC) LAN interface. Cisco ONS software Releases 3.1. and 3.2 are vulnerable. The following advisory offers workarounds to mitigate the effects of this vulnerability.

http://www.cisco.com/warp/public/707/ons-tos-vuln-pub.shtml

DDTS # CSCdx04313

Some (unknown) superuser and password combinations may fail when you attempt to FTP to a node. To work around this issue, you must create another superuser and try again. This issue is resolved in Release 3.2.1.

DDTS # CSCdx27495 SNMP Traps

When SNMP traps 3580 & 3590 are received from a Cisco ONS 15454 node, the NMS does not display the associated cerent454ObjectName varbind (the rest of the varbinds are displayed correctly). This problem occurs only if the NMS uses the trap definitions from the MIB file to build a display template to display all the Cisco 15454 proprietary traps. To work around this issue, manually add additional varbind display information to the trap display template in the NMS for these traps. This issue is resolved in Release 3.2.

DDTS # CSCdw16886

Under some circumstances, CTC enters a condition whereby the CPU remains at 100% utilization for the platform on which it is running (it is normal for the CPU to undergo brief periods of 100% utilization). For a network to be vulnerable to this issue, the network must contain ONS 15327s, must have at least 8 nodes (the problem is more likely to occur with 12 or more nodes), and the node acting as CTC host (GNE) must be one of the following:

ONS 15327 Release 1.0

ONS 15327 Release 1.0.1

ONS 15454 Release 3.0

ONS 15454 Release 3.0.1

ONS 15454 Release 3.0.2

ONS 15454 Release 3.0.3

ONS 15454 Release 3.1

To avoid this problem, networks with 8 or more nodes and

1. Only ONS 15327s should ensure that all host nodes are running ONS 15327 Release 1.0.2.
2. Mixed 15327 and 15454 networks should ensure that either:

    a) All host nodes are running ONS 15327 Release 1.0.2 and all 15454s are running Release 2.2.x or 3.2, or

    b) All host nodes are running ONS 15454 Release 3.2.

If this issue occurs in a network running all ONS 15327s, point to a different node with CTC or utilize TL1, or SNMP for monitoring, then call the Technical Assistance Center (TAC) at 1 877 323-7368.

If this issue occurs in a mixed ONS 15454 and 15327 network, terminate the CTC process, then call the Technical Assistance Center (TAC) at 1 877 323-7368.

This issue is resolved in ONS 15454 Release 3.2 and ONS 15327 Release 1.0.2, with exceptions as noted above.

DDTS # CSCdv91318, CSCdv82311

Upon completion of a software download of Release 3.1 to a node running Release 3.0.x, you may see an “aborted” message in the status window. This message does not necessarily mean that the software failed to download successfully. To check the status of the software download, from the CTC node view, click the Maintenance > Software tabs, then verify that the protect version is 3.1. This issue is resolved in Release 3.2.

DDTS # CSCdv76104

After performing a span upgrade on a 1+1 network with Ethernet traffic, you might experience an optical card reboot. This has been seen with OC-48 cards. This issue is resolved in Release 3.2.

DDTS # CSCdv82500

When you perform a span upgrade where a one way UPSR circuit exists, the circuit may undergo traffic outage on the alternate span after the upgrade. This occurs when the circuit is incorrectly cross-connected after the particular card is upgraded. To correct this issue when it occurs, in the node view, Maintenance tab, switch the cross connect cards in both nodes connected to the upgraded span. Alternatively, you can perform the following steps to restore traffic for each one way UPSR circuit:

Step 1 Clear the Force (which was placed prior to the span upgrade).

Step 2 Force the circuit to the upgrade span.

Step 3 Clear the Force.

Step 4 Force the circuit away from the upgrade span.

This issue is resolved in Release 3.2.

DDTS # CSCdv76699

After a span upgrade, you might experience a TCC+ reset. This reset should not affect traffic. A TCC+ reset after a span upgrade can lead to one or more MEA alarms in response to new card types present in the node. If you experience an MEA alarm, change the affected card type to reflect the type of the new card by right-clicking on the card, selecting Change Card, and changing the card type to match that of the new card in the given slot. This issue is resolved in Release 3.2.

DDTS # CSCdv89038

You must reset the active TCC+ on any node for which the MEM-LOW or MEM-GONE alarm is raised. This issue is resolved in Release 3.2.

DDTS # CSCdv63386

When using Release 3.1 TL1, a manual switch to an internal (ST3) clock might be allowed when the active source is of better quality. Specifically, issuing the OPR-SYNCSW command to switch to the internal source will succeed when it should not. If this occurs, use the RLS-SYNCSW command to reinstate the higher quality timing source. This issue is resolved in Release 3.2.

DDTS # CSCdv25954

In networks supporting Release 3.1 and Release 2.2.1 nodes concurrently, do not choose “Exclude dynamically discovered nodes” at CTC login. To do so can impair visibility of some nodes from your CTC session. This issue is resolved in Release 3.2.

SNMP

DDTS # CSCdw75755

Malformed SNMP traps can cause TCC resets. Use firewalling or access control lists to prevent SNMP traps from being sent into an ONS 15454 from any external system. For more information, consult the PSIRT notification on SNMP vulnerabilities. This issue is resolved in Releases 3.2.1 and 3.3.

DDTS # CSCdv78610

When creating an SNMP trap destination, do not enter a Community Name with a length of more than 32 characters. This issue is resolved in Release 3.2.

DDTS # CSCdv36186

The cerent454LineNumber is always zero in the trap varbind list. This varbind should carry the payload information regarding the interface. That is, if a trap is raised by an object in the system, this newly added varbind should indicate which object raised this trap. This issue is resolved in Release 3.2.

BLSR Functionality

DDTS # CSCdw52669

After a power failure, when the node reboots, a BLSR might switch back early to the working cards and cause a traffic outage on the passthrough circuits. This occurs only in 4 fiber BLSR (Release 3.1 and later only). This issue is resolved in Release 3.2 to traffic hits less than 200 ms, and resolved in Release 3.2.1 to within specification (less than 100 ms). Note, however, that 4 fiber OC-192 may still see up to a 200 ms traffic hit on a node power cycle. The 4 fiber OC-192 case has been resolved in software Release 3.3.

DDTS # CSCdw58919

Symptom: After a power cycle on a traffic-carrying passthrough node in a BLSR, while the node is rebooting, sometimes a long or double traffic hit can occur. If you know you are going to power cycle the node, apply a Lockout-Span on both sides of the node first. This issue is resolved in Release 3.3 and 3.2.1.

DDTS # CSCdw85221

Symptom: In a 4 fiber BLSR, traffic may be lost when issuing FS-R and MS-R on two adjacent nodes and releasing the FS-R very quickly. To avoid this issue, allow some time between each user command. This issue is resolved in Release 3.2.1.

DDTS # CSCdw86238

During a node isolation caused by a Force Ring on one side and a signal failure on the other side of the node, when the signal failure on the other side clears, you can lose passthrough traffic. If the node isolation was caused by a Force Ring on one side and signal failure on the other side, issue a Force Ring on the side with signal failure to avoid traffic loss. Do not repair the signal condition before issuing the second Force Ring. This issue is resolved in Release 3.2.1.

DDTS # CSCdw52669

After a power failure, when the node reboots, BLSR might switch back early to the working cards and cause a traffic outage on the passthrough circuits. This occurs only in 4 fiber BLSR (Release 3.1 only). This issue is resolved in Release 3.2.

DDTS # CSCdv78467

In a BLSR running Release 3.1, if you plan to perform a side switch on a node that has a cross connect already in the wait to restore (WTR) state (from a previous side switch), to ensure continuous traffic, you must first lock out both spans to adjacent nodes (as you would if you were performing an active cross connect removal). This issue is resolved in Release 3.2.

TL1

DDTS # CSCdx40587

Symptom: In TL1, pressing the Ctrl X key combination when connected to serial port causes a TCC reset. This does not impact traffic. Note that Ctrl X is not a supported TL1 command and should not be used. This issue is resolved in Release 3.2.1.

DDTS # CSCdw04303 TL1 RTRV-CRS-VT1 Command

In Release 3.1, do not use the TL1 RTRV-CRS-VT1 command with the AID value, “ALL.” To do so will cause the TCC+ to reset. If you accidentally issue the RTRV-CRS-VT1 command with the AID value and experience the TCC+ reset, follow these instructions to re-establish your TL1 session:

Step 1 If the RTRV-CRS-VT1 command caused the TCC+ to reset on the Gateway Network Element (GNE), all TL1 sessions will be disconnected, including all TL1 sessions to any End Network Elements (ENEs) and all other user TL1 sessions (including OSS sessions). To re-establish OSS sessions, reissue the telnet command. To re-establish the ENE TL1 sessions, reissue the ACT-USER to each individual ENE from the GNE. For example,

```
GNENode> ACT-USER:ENENode:UserId:Ctag::Password;
```

Step 2 If the RTRV-CRS-VT1 command caused the TCC+ to reset on an ENE node, the TL1 session between the GNE and ENE will be disconnected. To re-establish this connection, issue the ACT-USER command to the ENE node (after it comes back up) from the GNE. For example,

```
GNENode> ACT-USER:ENENode:UserId:Ctag::Password;
```

This issue is resolved in Release 3.2.

New Features and Functionality

This section documents new features and functionality as of Release 3.2. It is included in the Release 3.2.1 release notes for reference.

Hardware

G1000-4 Card

Release 3.2 introduces the G1000-4 card. The G1000-4 card provides four line-rate gigabit (STS-24c) Ethernet ports. The card supports the following circuit sizes under any SONET protection configuration:

- STS-1
- STS-3c
- STS-6c
- STS-9c
- STS-12c
- STS-24c
- STS-48c

The G1000-4 supports up to 48c maximum aggregate bandwidth per board. The G1000-4 transports up to one 48c, two 24c, or four 12c circuits per board.

The following specifications are defined for the G1000-4 card:

- Part Name: 15454-G1000-4
- Part Number: 800-08578-01
- CLEI Code: SNP8KW0KAA

G1000-4 cards are equipped with four GBIC connectors used for optical cable termination. GBICs must be ordered separately. The G1000-4 cards are rated at 62 watts per card and operate at ambient temperatures ranging from -5 degrees Celsius to +55 degrees Celsius.

Before you install the G1000-4 card to an ONS 15454 node, the node must be running Release 3.2 software or greater, must be provisioned with TCC+ cards, and must be provisioned with the XC10G card in the new (Release 3.1) ANSI shelf. If a G1000-4 card is inserted into a node that is provisioned with either XC or XCVT cards, the new card will not be recognized. Both high-speed slots and low-speed slots support the G1000-4 card. The high-speed slots are 5, 6, 12, and 13. The low-speed slots are 1–4 and 14–17.

Software

G1000-4 Path Trace Mode Support

Release 3.2 provides support for transmitting or receiving J1 byte information in the Trace Path Mode of the G1000-4 card. Only Path Terminate Equipment (PTE) can transmit and receive consecutive 64-J1 byte information. The trunk card can only receive (monitor) J1 byte information.

802.3 Flow Control and Frame Buffering

The G1000-4 supports 802.3x flow control and frame buffering to reduce data traffic congestion. To buffer over-subscription, 512 K bytes of buffer memory are available for the receive and transmit channels on each port (2 M bytes per board). When the buffer memory on the Ethernet sides nears capacity, the ONS 15454 uses 802.3x flow control to send back a frame called a "pause frame" to the source at the opposite end of the Gigabit Ethernet connection.

The pause frame instructs that station to stop sending packets for a specific period of time. The sending station waits the requested time before sending more data. The G1000-4 card does not respond to pause frames received from client devices.

This flow-control mechanism matches the sending and receiving device throughput to that of the bandwidth of the STS circuit. For example, two GSR 12000 series routers may transmit 1000 Mbps data through the 12c circuit on the G1000-4. This particular data rate between GSRs may occasionally exceed 622 Megabits per second (STS-12c). In this example, the G1000-4 sends out a pause frame and requests that the GSR12000 series delay transmission for a certain period of time.

Ethernet Link Integrity and SONET PDI-P Support

The G1000-4 supports end-to-end Ethernet link integrity. This capability is integral to providing an Ethernet private line service as well as for correct operation of layer 2 and layer 3 protocols on the attached Ethernet devices at each end. End-to-end Ethernet link integrity essentially means that if any part of the end-to-end path has a failure then the entire path is brought down. This is done by turning off the transmit lasers at each end, which will be detected by the attached Ethernet devices as a loss of carrier and consequently an inactive link. An Ethernet interface is expected to detect a loss of carrier as an indication of an inactive link.

When a local side of the link fails with a CARLOSS (Carrier Loss on LAN) alarm, the local G1000-4 card will send a PDI-P indication (C2-byte) to the remote G1000-4 through the trunk. The far-end G1000-4 receiving the PDI-P will indicate that the link is down with a TPTFAIL (Transport Layer Failure) alarm and turn off its associate port transmitter. The far-end Ethernet device will then detect the Carrier Loss on the associate network interface. The PDI-P condition is raised on the far-end trunk card and G1000-4, as well as all trunk cards (if any) of the transport nodes.

Note that even if one of the Ethernet ports is administratively disabled or set in loopback mode, this is considered a "failure" for the purposes of end-to-end link integrity, since the end-to-end Ethernet path is not available. These conditions also cause both ends of the path to be brought down. This feature is also an integral part of the support for Gigabit EtherChannel.

Terminal Loopback and Hairpin Circuit Support

G1000-4 supports terminal loopback from the Maintenance tab of the CTC card view. You can configure a port for a Terminal (Inward) loopback or clear the loopback (none). Release 3.2 supports hairpin (port-to-port) circuits on the G1000-4.

G1000-4 Ethernet Port Media Type Display Support

The G1000-4 can display the Media (GBIC) type (SX, LX or ZX). From the CTC card view, select Provisioning > Port to view the media type.

Support for New Ethernet Performance Statistics

Clear Button

Release 3.2 adds a Clear button to the Performance > Statistics tabs in the card view for the G1000-4. This button resets the actual counters on the card to zero. All management clients see the change. Note that the Clear button does not cause the G1000-4 card to reset.

New Statistics for the G1000-4 Card

Release 3.2 supports the following new Ethernet performance statistics for the G1000-4 card.

Receive Pause Frames—Number of received Ethernet 802.3x pause frames

Transmit Pause Frames—Number of transmitted 802.3x pause frames

Receive Packets Dropped Internal Congestion—Number of received packets dropped due to overflow in G1000-4 frame buffer

Transmit Packets Dropped Internal Congestion—Number of transmit queue drops due to drops in G1000-4 frame buffer

A new "HDLC errors" counter has been added. This counter internally monitors the corruption of data on the SONET path between 2 G1000-4 cards.

K3 Byte Transparency for the OC-48AS

K3 byte transparency provides networking flexibility for mixed vendor BLSR networks. The K3 byte, required for BLSR functionality on the ONS 15454, is carried in the K2 byte of the second STS. Since the K3 byte is a non-standard feature of ONS 15454 SONET overhead, some third party muxponder topologies have, in the past, been unable to transport them seamlessly. With Release 3.2, the ONS 15454 OC-48AS card allows users to re-map the K3 byte to an alternative byte (Z2, F1, or E2) supported by third party vendor equipment. For information on remapping the K3 byte, see *Cisco ONS 15454 Installation and Operations Guide, Release 3.2*.

SNMP Enhancements

RMON Support

The ONS 15454 features Remote Monitoring (RMON), allowing network operators to monitor the health of the network with a Network Management System (NMS).

New Ethernet Threshold Variables

The following Ethernet Threshold variables can now be provisioned in CTC.

ReceivePauseFrames—Number of received 802.x pause frames

TransmitPauseFrames—Number of transmitted 802.x pause frames

ReceivePktsDroppedInternalCongestion—Number of received frames dropped due to frame buffer overflow (or other reasons)

TransmitPktsDroppedInternalCongestion—Number of frames dropped in the transmit direction due to frame buffer overflow (or other reasons)

TL1

Enhancements

For detailed information on TL1 support of new features in Release 3.2, refer to *Cisco ONS 15454 TL1 Command Guide*, Release 3.2.

TL1 General Support for the G1000 Card

Card provisioning, facility provisioning, alarm/event reporting and retrieval, cross-connect provisioning, and loopback have been added to the TL1 interface to support the G1000-4 card.

Commands and Autonomous Messages Enhanced to Support the G1000-4 Card

The following commands/autonomous messages have been enhanced to support the G1000-4 card.

All existing <MOD2_IO> commands:

OPR-LPBK-<MOD2_IO>

RLS-LPBK-<MOD2_IO>

All existing <MOD_PORT> commands:

RMV-<MOD_PORT>

RST-<MOD_PORT>

All existing <MOD2ALM> commands/messages:

RTRV-ALM-<MOD2ALM>

RTRV-COND-<MOD2ALM>

REPT ALM <MOD2ALM>

REPT EVT <MOD2ALM>

Enhanced Cross-Connect Commands to Support the FAC AID for the G1000-4

The following cross-connect commands have been added to support the new facility AID for the G1000-4.

ENT-CRS-<STS_PATH>

DLT-CRS-<STS_PATH>

RTRV-CRS-<STS_PATH>

ED-<STS_PATH>

RTRV-PTHTRC-<STS_PATH>

RTRV-<STS_PATH>

OPR-PROTNSW-<STS_PATH>

RLS-PROTNSW-<STS_PATH>

Password Enforcement

In accordance with Telcordia GR-815, TL1 functionality for Release 3.2 enforces password complexity as follows.

ONS 15454 TL1 enforces password complexity for TL1 and users. This rule only applies for new or changed passwords after Release 3.2 is installed; existing passwords do not need to be changed. A new password must have at least 1 numeric character (0 to 9) and at least one special character from the character set {plus-sign (+), pound-sign (#), percent-sign (%)}.

Note See the "DDTS # CSCdv62990" section on page 11 for a CTC caveat to these rules.

New Commands

The following TL1 commands are new in Release 3.2.

- ED-G1000
- RTRV-G1000

New Parameters

The following TL1 parameters are new in the Condition table (new conditions) for Release 3.2:

- MFS_TYPE — indicates the maximum frame size used by a G1000-4 card
- FLOW — indicates the type of flow control that has been negotiated for an Ethernet port
- OPTICS — the type of gigabyte Ethernet optics in place
- MUX_TYPE — BLSR Extension byte

New Conditions

RFLOWCTL — Ether (G1000) Rx excess flow control

ROVERSUB — Ether (G1000) Rx oversubscribed

TFLOWCTL — Ether (G1000) Tx excess flow control

TOVERSUB — Ether (G1000) Tx oversubscribed

TPTFAIL — Ether (G1000) transport failure

TUNDERRUN — Ether (G1000) Tx under run

Changed Conditions

The following condition has changed in Release 3.2.

The FAIL_DS3_NE_FRM_MISMATCH condition is renamed to DS3-MISM.

New Alarm

The following TL1 alarm object is new in Release 3.2:

- G1000

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15454, Release 3.2*
- *Upgrading Cisco ONS 15454 Release 2.2.x to 3.2.1*
- *Upgrading Cisco ONS 15454 Release 3.0.x to 3.2.1*

Platform-Specific Documents

- *Cisco ONS 15454 Installation and Operations Guide, Release 3.2*
- *Cisco ONS 15454 Troubleshooting and Maintenance Guide, Release 3.2*
- *Cisco ONS 15454 TL1 Command Guide, Release 3.2*
- *Cisco ONS 15454 Product Overview, Release 3.2*

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.