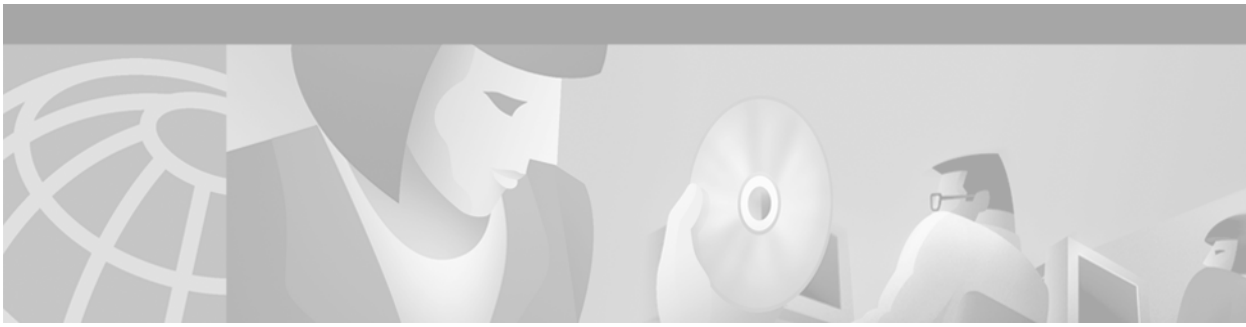

Release Notes for Cisco ONS 15454 SDH Release 3.3

May, 2002

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 Release 3.3 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 3.3, 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 SDH Release 3.3* since the production of the Cisco ONS 15454 SDH System Software CD for Release 3.3.

The following changes have been added to the release notes for Release 3.3.

Changes to Caveats

The following caveats have been added to the release notes.

SONET and SDH Card Compatibility, page 3

DDTS # CSCdx68385, page 4

Transmission Control Protocol Specification, page 9

DDTS # CSCdx78825, page 9

Ethernet Card Names, page 17

SNCP Traffic Patterns, page 17

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.

Note The following caveats refer to bugs that were originally release-noted using SONET Terminology:

DDTS # CSCdw57215, page 5
DDTS # CSCdx05444, page 7
Single-card EtherSwitch, page 8
Multicard EtherSwitch, page 8
DDTS # CSCdw64191, page 12
DDTS # CSCct03396 Ring Map Change Dialog Box, page 12
DDTS # CSCdx19598, page 15
DDTS # CSCdw57215, page 16

These have been reworded to reflect their application to the SDH platform.

Hardware

DDTS # CSCdw74751

An STM16 line card might exhibit signal fail after the unit is power-cycled twice or more. This issue can arise when multiple power cycles have occurred. The STM16 card displays a signal fail LED after these power cycles. CTC reports LOS on the affected card. When you replace that card with another STM16,

traffic returns to normal. When you insert the affected STM16 card in another node within the circuit, it now also reports signal fail (and CTC reports LOS). This issue has only been seen once, and may be specific to the card it was seen on. This issue will be resolved in Release 3.4.

DDTS # CSCdw92634

SDH electrical cards only support a VC4 J1 trace string setting for all VC4s. You cannot set the J1 byte for individual VC4s. When the J1 byte is set for a single VC4, all other VC4s in the same line card will be set to the same value. This issue will be resolved in Release 4.0.

DDTS # CSCdw14501

CTC might generate an interconnection equipment failure alarm at 55 degrees C, and 72 volts. When the operating environment is at 55 degrees C and 72 volts, CTC will generate interconnection equipment failure alarms for the following cards:

- STM16SH
- STM64LH
- STM16LH
- XC10G

The alarms could potentially occur on any BTC192 board: OC48AS, GigE, OC192 or OC192LR. This issue will be resolved in Release 3.4.

DDTS # CSCdw65251

Long recovery times are possible for an E3 or DS3 circuit when there is a disruption on the fiber span. This occurs when you either remove or soft-reset active span cards. This issue will be resolved in Release 3.4.

DDTS # CSCdw50903

E1 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 Release 3.4.

Line Cards

SONET and SDH Card Compatibility

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

Table 1 SDH Data Cards that are SONET Compatible

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

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 XC-10G
15454-E1000-2-G	Gigabit Ethernet, 2 circuit., GBIC - G

Table 3 Miscellaneous Compatible Cards

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

DDTS # CSCdx68385

Ethernet traffic on E series cards is subject to possible loss while performing a span upgrade from STM-16 (not including STM-16AS) to STM-64. To recover from such a loss, perform an XC10G switch. This issue is under investigation for possible resolution in a future release.

DDTS # CSCdw44431

Because CTC does not provide a way to set the expected payload label, the optical card cannot anticipate a particular label. The card accepts all payload labels except for unequipped without raising an HP-PLM alarm. To avoid confusion, note that if a signal is terminated on an electrical card, the card raises a PLM if the label is not correct for the terminated traffic. It is not known at this time when or if this issue will be resolved.

DDTS # CSCdw60129

When a terminal loopback is placed on an E1 port, but the port is not in service, the circuit will not reliably carry traffic. This only occurs when a port is put into terminal loopback but the port is not put into service. Placing the port in service either before or after creating the terminal loopback will cause the circuit to pass traffic correctly. This issue is under consideration for resolution in a future release.

DDTS # CSCdw80537

When the active TCCI and XC10G are removed simultaneously, the DS3I card might drop traffic. The issue does not arise if the second card is removed after the first card has completed switching. Also, this issue has only been reported when DS3I traffic entered the node through an SNCP optical ring. To recover traffic, reset or reseat the DS3I card. This issue will be resolved in a future release.

DDTS # CSCdx26746

When you insert an electrical card into an unprovisioned slot of a node with XC10G cross connect cards, in some cases, the card will fail to boot up and auto-provision itself. To recover in this situation, provision the card through the user interface. This issue will be resolved in Release 3.4.

DDTS # CSCdw80652

When one traffic card in a 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 # CSCdx00506

After monitoring traffic for several days, B3 errors may be seen on E3, STM-1, STM-4 and Ethernet traffic with the XC10G cross-connect card. This issue will be resolved in a subsequent build of the Release 3.3 software.

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 will result in a traffic hit on all existing SDH 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.

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 # CSCdw45637

Rarely, if an E1 card has been running for at least 12 hours and is in a 1:N protection group, the switch time to protection can take approximately 500 ms. This issue will be resolved in a subsequent load of the Release 3.3 software.

E Series and G Series Cards

DDTS # CSCdx53004

An STM-1 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 STM-8C, STM-4C or STM-3C) then, if new STM-1 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 STM-1 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 STM-12C or greater. If the total is less than STM-12C 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 STM-8C or less and then start re-provisioning circuits in order of smallest through largest. This issue will be resolved in Release 3.4.

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.

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.

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 # 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 VC4-8c. This issue will be resolved in a future release.

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.

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.

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.

Transmission Control Protocol Specification

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

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

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

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

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

DDTS # CSCdx78825

The ONS 15454 SDH TCCi reboots after the TCCi has received 64 or more ARP requests on a subnet different from that of the TCCi. This situation can occur when the network settings (IP address and netmask) are incorrect for the craft Ethernet environment. The node may respond to Ethernet ARP requests via its automatic host detection feature. If this feature is triggered more than 64 times, the node's TCCi will reboot. Removing the craft Ethernet connection resets the count, so this situation is unlikely to occur with an End Network Element (ENE). To avoid this issue, ensure that the node is properly provisioned for its craft Ethernet environment. In particular, ensure that the netmask is correct. For ENEs that depend on automatic host detection, avoid leaving the craft Ethernet connected for more than one day at a time. This issue is resolved in Release 3.4.

DDTS # CSCdx53993

A less than 1 ms traffic disruption can occur when deleting a DS3I 1:1 or 1:N protection group. 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 in Release 3.3. 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 0-4 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

DDTS # CSCdw82921

The ITU specification requires that if working and protect optical cards both have an SD or SF, the traffic should pass on the working card. The SONET specification does not require this. The ONS 15454 SDH platform conforms to the SONET specification, but not the ITU specification. Specifically, when an SD or SF condition occurs on a working optical card, the ONS 15454 SDH switches traffic to the protect card. When an SD or SF condition then occurs on the protect card, traffic will stay on the protect card. The ITU specification requires that traffic should revert to the working card, even though that card has an SD or SF as well. There is no degradation of service, so no workaround is really needed; however, a force command can be issued to force the traffic onto the working card if desired. This issue will be resolved in a future release.

DDTS # CSCdw78048

The boot menu's host IP address is added to the node's routing table. The host IP is used when a node downloads a software image from a network in a development environment. This occurs whenever the manufacturer's default host IP is not null in the bootline (boot menu). In general, this is not a problem since the default host IP is a reserved IP address. However, an installation engineer may want to change the default host and gateway IP to a customer's host and gateway IP, or to null, by changing the bootline through the console. In Release 3.4, the host IP will not be added to the routing table if a node is not booting from a network.

DDTS # CSCdw95301

When there are large numbers of VC4 circuits (greater than 100) and when there is a lot of circuit activity (for example, when there are a lot of updates), display of the Circuits pane can be slow and the user interface may be unresponsive for several minutes. This issue will be resolved in a future release.

DDTS # CSCdw52185

Symptom: User initiated switches (Manual or Force) are not cleared if overridden by higher priority switch requests. If a request is overridden by a higher priority request, it must be cleared manually in order to prevent possible switch oscillation. This issue will be resolved in Release 3.4.

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 # CSCdw58748

In the “Audit Trail” under the Maintenance tab, there is a status field. Sometimes this field contains an “X” character; however, the X character is not documented in the user documentation. To understand the meanings for each result in the Pass/Fail column, please consult the following:

P = function completed successfully

F = function completed with failure

X = function did not complete

This issue will be resolved in the Release 3.3 documentation.

DDTS # CSCdw45674

When there is a facility loopback in place, the E3 L3M chip will pass line traffic towards the backplane, and the facility loopback will then result in a terminal loopback. You cannot generate AIS towards the backplane in this scenario. The L3M chip does not support facility and terminal loopback at the same time. The workaround is to set loopback type equal to “none” before changing the loopback from facility to terminal and vice versa.

DDTS # CSCdx03404

If you perform a manual switch from the working to the protect card, upon removing the protect card, traffic will switch back to working within 50 ms. When the protect card is replaced and the card has rebooted, the manual switch will trigger a traffic switch back to the protect card which can cause a service disruption on the order of several hundred ms. To avoid this service disruption, remove the manual switch command before replacing the protect card. The manual switch command will be cleared upon detection of a higher priority failure (as per Telcordia GR-253) in a future release.

DDTS # CSCdw71844

When a Force or Manual switch request is made while a higher priority request is present (in other words, SD/SF or Lockout), the user-initiated switch request will not be denied. This issue is resolved in Release 3.4.

DDTS # CSCdw64191

When testing throughput and latency of VC4-8c 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 # 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:

- Two 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

This issue will be resolved in a future release.

DDTS # CSCct03396 Ring Map Change Dialog Box

When you add a node to an MS-SPRing, 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 Release 3.4.

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 Release 3.4.

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 # 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 # CSCdx29951

Normally, a node is isolated by unidirectional failures on each of its working and protect spans; however, if this isolation fails to complete for some reason, passthrough traffic can be lost. To preserve traffic, issue a force ring from the two adjacent nodes, towards the problem node. Clear the force ring on each adjacent node once the isolated node recovers from failures. This issue will be resolved in Release 3.4.

DDTS # CSCdx39743

High switch times can occur on STM1 traffic passing through MS-SPRings when the active cross connect card is pulled. Issue a manual switch of the cross connect cards, or reset the active cross connect card before removing it. Locking the spans prior to pulling the cross connect card also reduces switch time in this scenario. This issue will be resolved in a future release.

DDTS # CSCdx42388

Splitting an MS-SPRing by creating a signal failure ring (SF-R) on both the east and west spans causes the cross connect card and the TCC to reboot simultaneously. To avoid this, issue a force ring (FS-R) on the side that detects signal failure for each node affected. This issue will be resolved in a future release.

DDTS # CSCdx42436

Permanent failure of protect STM64 after both XCs self-boot can occur on a four fiber MS-SPRing with four nodes. If you introduce SF on both the working and protect spans on opposite links (to segment the ring into two smaller rings), the XCs and the TCC in Slot 7 reboot. This issue will be resolved in Release 3.4.

DDTS # CSCdx42694

Promoting signal degrade span (SD-S) to signal degrade ring (SD-R) on the same node while a higher priority span request exists in the ring can cause traffic loss. For example, if you:

1. Introduce signal degrade span (SD-S) on the west working span.
2. Introduce signal degrade span (SD-S) on the east working span.
3. Introduce signal degrade protection (SD-P) on the east working span.

Then, to recover traffic to the working span on the east, you must issue a lockout protection span on the east; or, to recover traffic to the protect span on the east, you must issue a force span on the east. This issue will be resolved in a future release.

DDTS # CSCdx42710

A cross connect card reboot and traffic loss can occur on a four fiber MS-SPRing when signal degrade span (SD-S) is promoted to signal failure span (SF-S) while signal degrade ring (SD-R) exists in the other span. The following example illustrates the conditions that can cause this issue to occur:

1. Using variable attenuators, introduce SD-R on the east span (working & protect); by attenuating the working span first and the protect span later.
2. Introduce SD-S on the west working span using a variable attenuator.
3. Escalate SD-S to SF-S by increasing the attenuation; increase a bit further and you get LOF on the west working span.
4. In this situation, WTR is raised and cleared continuously on the west working span.
5. After a few minutes, the active XC in one node attempts to reboot and all traffic is lost and then regained, but the WTR problem persists.

To prevent signal oscillation on the west working span, issue a force span command on that span. Release the force when the fiber is replaced. This issue will be resolved in a future release.

DDTS # CSCdx42820

Following issuing a force ring on a four fiber MS-SPRing on one side and creating a signal failure ring by pulling both the working and protect receive fibers on the other side, restoral of the working fiber causes the cross connect card to reboot. The same symptom can occur if you issue two force ring commands on the east and west of a node and then fail the protect fiber on either side of that node. To avoid this situation, in the first case, release the force ring command before restoring the working fiber on the other side. In the second case, issuing two force ring commands on the side node to enable isolation of a node is not recommended. Rather, issue the force ring command from the nodes adjacent to the node to be isolated. This issue will be resolved in a future release.

DDTS # CSCdx45851

On a four fiber MS-SPRing, VC4-16C traffic fails switch after restoring the database to all nodes. This only happens when you are restoring the database for all nodes at the same time. 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 # CSCdv26389

Symptom: The CLEAR command does not clear a WTR (Wait To Restore) condition on MS-SPRing (or BLSR). If the MS-SPRing (or BLSR) gets into a WTR state, there is no preemptive message that can be sent to the system to remove the WTR. This issue will be resolved in a future release.

DDTS # CSCdx20789

Clearing a force switch span (FS-S) on a four fiber MS-SPRing during a signal failure span (SF-S) can result in a condition where the FS-S still exists on the same span, and a traffic hit is incurred. To avoid this issue, do not clear a force switch span while a signal failure working is detected. This issue will be resolved in Release 3.4.

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 be resolved in a future release.

DDTS # CSCdx02278

A four fiber node with signal failure or signal degrade on the local protect might raise a K-byte PT event when a PT span K-byte is received. This issue will be resolved in a future release.

DDTS # CSCdw81494, CSCdw81592, CSCdw82811, CSCdv09279, CSCdv83805

A Manual or Force switch is not released when SD or SF occurs. This occurs under the following conditions:

In a non-revertive linear 1+1 bidirectional link between two nodes, A and B,

Step 1 Issue a manual or force switch to protect span on Node A.

Step 2 Generate a SD or SF on the protection receiver side of Node A by pulling the receive fiber.

Step 3 The line does switch from the protection to the working while the SD or SF lasts.

Step 4 The manual or force switch is never released. The requested switch to protect hangs in the CTC GUI.

Step 5 After the SD or SF is released, the line switches back to protection.

This issue will be resolved in Release 3.4.

DDTS # CSCdw62602

Node isolation caused by four unidirectional failures on the four spans of a node can result in traffic loss. To regain traffic, issue a “Force ring” on both sides of the isolated node and proceed with repairing the failures. This issue will be resolved in Release 3.4.

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 will result in a traffic hit on all existing SDH circuits defined over that same span.

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. 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 # CSCdw75434

If you perform a Force switch after performing a Manual switch on an SNCP link, you may receive an error message that “all circuits are failed to switch.” To correct this situation, clear the Manual switch on the protected link and then perform the Force switch on other link. This issue will be resolved in a future release.

Active Cross Connect or TCCi Card Removal

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

Active cross connect cards should not generally be removed. If the active cross connect or TCCi card must be removed, you can first perform an XC10G 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 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.

SNMP

DDTS # CSCdx27495

When 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 will be resolved in Release 3.4.

Documentation

SNCP Traffic Patterns

The *Cisco ONS 15454 SDH Installation and Operations Guide*, Release 3.3, Chapter 5, Section 5.2, "Creating SNCP Circuits" incorrectly states that:

> Working traffic flows in one direction and protection traffic flows in the opposite direction. If a problem occurs in the working traffic path, the receiving node switches to the path coming from the opposite direction.

With Release 3.3, all primary (working) SNCP circuits traverse the ring in the same direction on the fiber. This means that both circuits do not traverse the same fiber immediately after provisioning. One significant benefit of this feature is that a single fiber cut does not cause both directions of a two-way UPSR circuit to switch. Another benefit is that the ONS 15454 SDH SNCP circuit behaves more in line with current industry expectations.

Ethernet Card Names

In the user documentation, E1000-2 (product name 15454E-E1000-2) is called E1000-2-G; and E100T-12 (product name 15454E-E100T-12 is called E100-12-G. This issue will be resolved in Release 3.4.

Resolved Software Caveats for Release *3.3*

The following items are resolved in Release 3.3.

There are no resolved items in this release, as this is a new product.

New Features and Functionality

There are no new features and functionality to highlight, as this is a new product. Please refer to the *Cisco ONS 15454 SDH Product Overview*, Release 3.3.

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15454, and 15327 Release 3.3*

Platform-Specific Documents

- *Cisco ONS 15454 SDH Installation and Operations Guide, Release 3.3*
- *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide, Release 3.3*
- *Cisco ONS 15454 SDH Product Overview, Release 3.3*

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.