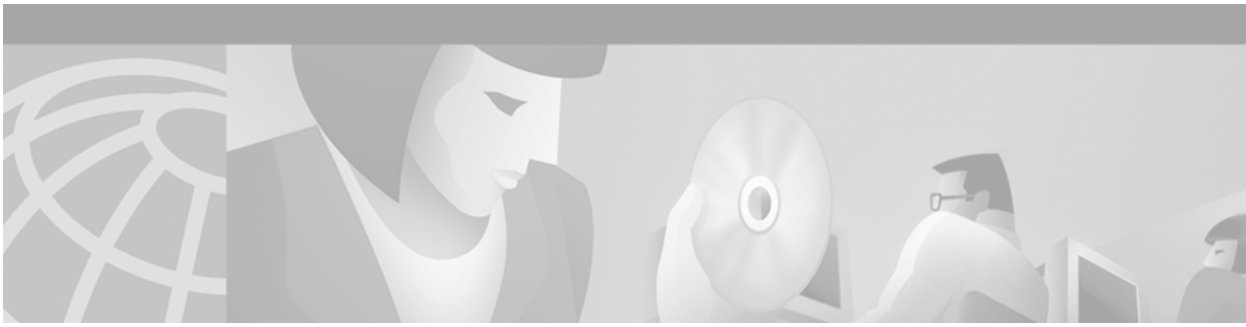

Release Notes for Cisco ONS 15454 Release 3.3

May, 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 *Cisco ONS 15454 Procedure Guide, Release 3.3*; *Cisco ONS 15454 Reference Guide, Release 3.3*; *Cisco ONS 15454 Troubleshooting Guide, Release 3.3*; *and Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide, Release 3.3*. For the most current version of the *Release Notes for Cisco ONS 15454 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 Release 3.3* since the production of the Cisco ONS 15454 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

JRE Updates, page 10

Transmission Control Protocol Specification, page 10

DDTS # CSCdz05847, page 10

DDTS # CSCdw45877, page 11

DDTS # CSCdx78825, page 11

DDTS # CSCdx71359, page 11

Inactive Login Message, page 20

The following caveat has been modified to supply further information.

DDTS # CSCdw57215, page 6

Changes to Closed Items

The following caveat has been addded to the list of maintenance issues closed in Release 3.3.

DDTS # CSCdx23202, page 21

Exercise Ring, page 23

Changes to New Features and Functionality

The following new functionailty has been documented.

UPSR Traffic Patterns, page 25

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

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 XC10G
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 # CSCdx35189

If, when OC12-4 is used for a BLSR span and the span is in the state of working-active and protection-standby, you inject (or otherwise incur) B2 errors into the span, the OC12-4 will only detect 75% of B2 counts injected. To work around this issue, compute 33% more B2 counts than you actually are seeing for this card type. This issue will be resolved in the next hardware release of the OC12-4.

DDTS # CSCdv05723

An abrupt change in reference frequency between two nodes can cause DS3 phase transient to result in test set errors. There is no resolution for this issue at this time.

DDTS # CSCdv40700

In either a DS1 or DS3 1:N protection group, removing a standby working card from the protection group can cause a traffic hit from 200 to 2000 ms. Do not remove any working cards from the protection group when the protect card is active. Instead, switch traffic away from the protect card, then remove the working card from the protection group. This issue will be resolved in a future release.

DDTS # CSCdw27380

Performing cross connect card switches repeatedly might cause a signal degrade condition on the lines or paths that can trigger switching on these lines or paths. If you must perform repeated cross connect card switches, lock out UPSR spans first.

LOS Behavior

When an OC-N card is seeing LOS and the problem is resolved (for example, the pulled fiber is reinserted) the LOS will normally clear quickly, and any other errors seen on the signal will be raised. However, in the special case where the restored signal is unframed, the LOS will remain raised (that is, the LOS will not be replaced by an LOF). This is standard SONET behavior per Telcordia GR-253 R6-54.

DDTS # CSCdv24887

An EC1 card may appear blue and not present (NP) in CTC. When you insert an EC1 card in the node, after the card has completed the bootup cycle, the Active LED on the EC1 card will be lit, while CTC still shows the card as NP. To avoid this problem, before inserting the EC1 card, pre-provision the slot for an EC1 card. Alternatively, after the card has booted up, you can use CTC to delete the card. The card will reset itself and should reboot and appear on CTC correctly. This issue will be resolved in a future release.

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 will be resolved in a future release.

DDTS # CSCdw28210

Approximately 60 ms service disruption times can occur for OC-12 1+1 protection groups when the error rate is 1E-3 or 1E-4. In an OC-12 1+1 protection group with the SF-L threshold set to 1E-3 or 1E-4, when the working card sees an error level at the 1E-3 or 1E-4 threshold, service disruption time may be greater than 50 ms. Note that SF-L thresholds of 1E-5 or lower do not have this problem. This issue will be resolved in a future release.

DDTS # CSCdw37046

DS-3 traffic hits can occur during synchronization changes (frequency offsets applied) on the node's timing. The specific scenario under which this has been seen involves configurations with multiple nodes line-timed off each other in series. If a network configuration has a DS-3 circuit routed over a

chain of nodes that are line-timed off each other in sequence (more than 1 line-timed “hop”), the DS-3 traffic might exhibit errors on timing disturbances applied on the source node. There is no resolution for this issue at this time.

DDTS # CSCdw23162

Using OC12-4 in a 1+1 protection group, and placing a port out of service and then back in service, the OC12-4 PSC counts more than one. Placing a port out of service will trigger a protection switch. The PSC count will increment by 1 as expected. Placing the port back in service then increments the PSC count by two even though no protection switch has occurred. This issue will be resolved in Release 3.4.

DDTS # CSCdw75823

OCn cards do not raise PLM-P alarms. To see this, on a 2-node setup, create a VT circuit starting at a DS-1 card on Node 1 and an STS circuit terminated at a DS-3 card on Node 2. Route these circuits to the same STS as the span cards. Feed DS-1 and DS-3 traffic to the respective cards using test sets. While the DS-3 card raises the PLM-P alarm, the DS-1 card does not. This issue will be resolved in Release 3.4.

DDTS # CSCdx03404

During a manual switch from a working to protect OC-192 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, remove the manual switch command before replacing the protect card. This issue will be resolved in a future release, wherein the manual switch command will be cleared upon detection of a higher priority failure, as per Telcordia GR253.

DDTS # CSCdx25206

If you create an STS1 circuit between a DS3XM and an OC-12 card on a node using XCs or XCVTs as the cross-connect cards, then perform several XC side switches (either manual or card pulls), you may rarely start to see switch times in excess of 60 ms. To avoid this issue, use XC10Gs. This issue will be resolved in Release 3.4

DDTS # CSCdx26701

Older versions of the DS-3 card (which are no longer manufactured) may see protection switch times on the order of 100 ms. The older DS-3 cards can be identified by the single color Active LED on the front panel. Newer DS-3 cards and the DS3E card have a bicolored Active/Standby LED. The newer DS-3 cards do not have this issue with switch times. This issue will not be resolved.

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.

In the *Cisco ONS 15454 Procedure Guide*, Release 3.3, refer to the "NTP-77 Delete Circuits" procedure to delete the 24c circuit before removing the card. Once you have deleted the circuit, refer to the "DLP-191 Delete a Card from CTC" task (also in the procedure guide) to delete the G1000-4 card. This issue will be resolved in a future release.

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. To avoid this issue, replace older OC-48 cards with OC-48AS.

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 # 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 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

You must perform a lockout in BLSR, UPSR, and 1+1 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, you cannot create 9c or 24c gigabit Ethernet circuits through any 15327.

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 in maintenance Release 3.2.1.

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.

A future hardware revision of the G1000-4 will have an improved blocking scheme to address this issue.

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 9 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

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.

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

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 # CSCdz05847

After launching CTC from an ONS 15xxx running Release 3.3 or 3.4, you cannot launch CTC (on that computer) from an ONS 15454 running Release 3.1-3.2.x. Further, no error message is displayed indicating the issue. To recover from this situation, one of the following recovery procedures may be necessary.

- Delete the CTC cache (using the button in the browser applet window) before launching from the Release 3.1 or 3.2.x node.
- Continue to launch from the Release 3.3 or 3.4 node but access the Release 3.1 or 3.2.x node (if necessary) using a login group (defined in the Edit:Preferences dialog).

This issue will be resolved in a future release.

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 # CSCdx78825

The ONS 15454 TCC+ reboots after the TCC+ has received 64 or more ARP requests on a subnet different from that of the TCC+. 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 TCC+ 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 # CSCdx71359

After the IIOP port of a node has been fixed at a user-specified constant, any attempt to change other parameters in the node view, Provisioning > Network > General tabs results in an error message indicating that the IIOP port is already in use. If you can modify the IIOP port setting and still reach the node, you can avoid this issue by changing the IIOP port back to the default, making your parameter changes, and then restoring the old IIOP port setting. This issue will be resolved in Release 3.4.

DDTS # CSCdx24738, CSCdx38749

Some nodes may appear as grayed out after an upgrade from Release 3.0.3 to 3.3. This occurs after activation of the first node is complete and subsequent nodes are activated. The grayed-out nodes are still possible to ping. If this occurs, launch a new CTC session on one of the affected nodes. All nodes should communicate with the new session. This issue will be resolved in Release 3.4.

DDTS # CSCdx40462, CSCdx47176, CSCdw22170

While upgrading nodes from releases prior to 3.2, CTC might lose connection to the far end nodes. When this occurs, you will not be able to ping the grayed-out nodes; however, if you continue the upgrade, this problem resolves itself. This issue is resolved in Release 3.2, but can still occur when upgrading from nodes with earlier software releases.

DDTS # CSCds88976

When a new circuit is created around a ring (UPSR or BLSR), the SD BER or SF BER alarm can be raised depending on the order in which the spans are provisioned. The alarms will eventually clear by themselves. Traffic is not affected. This issue will be resolved in a future release.

DDTS # CSCdw72546

In a 1:1 protection group, traffic may be lost when a protect card is removed and reinserted, while a lock on is in place. The following conditions are required to see this issue:

1. Remove the working card; traffic is now carried by the protect card.
2. Apply a Lock On to the protect card. Reinsert the working card.
3. After the working card comes up, remove & reinsert the protect card. Traffic is now carried by the working card.
4. When the protect card comes up after rebooting, traffic is lost.

To recover from this issue, remove the Lock On from the protect card; traffic is then restored to the working card. This issue is resolved in Release 3.4.

DDTS # CSCdx10929

Very rarely, after power failure of a node that drops VT traffic, the traffic is not carried on VT circuits after restoring power. This can occur when you are using the NEBS shelf assembly, with XCVT cross-connect cards, VT traffic dropped through an optical card (OC-n), and power has failed and then been restored to a drop node. To correct this issue, reset both XCVTs in the node. This issue is under investigation.

Note To determine whether you are using the NEBS shelf assembly, at the CTC node view, click the Inventory tab. Under the Hardware Part # column, if the number is not 800-19856-01, then you are using an earlier (NEBS) shelf assembly.

DDTS # CSCdv36453

Manual or Force switches are not denied or cleared when a higher priority switch is present. If an SD/SF condition exists, a Manual switch should be denied. If the failure exists on a protect line, a Force switch should also be denied (1+1 only). Likewise, if a Manual switch is present and an SD/SF condition is raised, the Manual switch should be cleared. This issue will be resolved in Release 3.4. As of Release 3.4, if a user-initiated switch will not cause a switch (because of a higher priority request), the switch will be denied. If a switch is accepted, but overridden at a later time because a higher priority request is initiated, the current switch will be cleared. This applies to 1+1, UPSR and BLSR.

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:

- You are running your CTC session from Microsoft Windows NT
- 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.

To avoid this problem, upgrade to JRE 1.3.1. This issue will be resolved in a future release.

DDTS # CSCdw66895

XCVTs (both active and standby) reboot continuously when the K3 byte is mapped to the E2 byte on one side of a WTR span. The rebooting occurs after the WTR timer expires. This has been seen on a two fiber BLSR with OC-48AS. To avoid this issue, if possible, change the K3 mapping on both ends of the span before creating the ring; or, alternatively, you can prevent the ring from reverting during the K3 mapping by setting the Ring Reversion time to "never." Once you have completed the mapping of the K3 byte to the E2 byte on both sides, return the Ring Reversion to its normal value. This issue will be resolved in Release 3.4.

DDTS # CSCdx06165

During an XC to XC10G upgrade, some traffic can be lost after switching to the new XC10G. To avoid this possible traffic loss, after the XC10G has fully booted and becomes standby, wait 30 seconds, create a simple STS test circuit on that node, and then delete the circuit. The XC10G should be ready to carry traffic. This issue will be resolved in a future release.

DDTS # CSCdw71844

If a Force or Manual switch request is made when a higher priority request is present (in other words, SD/SF or Lockout), the user request (Force or Switch) will not be denied. This issue will be resolved in Release 3.4. As of Release 3.4, if a user initiated switch should not cause an actual switch (because of a higher priority request), the switch will be denied.

If a switch is accepted but overridden at a later time because a higher priority request is initiated, the current switch will be cleared. This applies to 1+1, UPSR/SNCP and BLSR/MS-SPRing.

DDTS # CSCdw95301

When there are large numbers of VT circuits (greater than 100) and when there is a lot of circuit activity (for example, when there are a lot of updates), the circuits pane can be extremely slow to repaint, and the user interface can fail to respond for several minutes. This issue will be resolved in a future release.

DDTS # CSCdx28587

In an optical 1+1 protection group, if you issue a manual switch to protect, then remove the protect card, this will trigger a traffic switch back to the working card. The manual switch will remain in place so that upon insertion of the protect card, there will be a long switch time when traffic switches back to the protect card. To avoid this long switch time, clear the manual switch command before reinserting the protect card. This issue will be resolved in Release 3.4.

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 or later. 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 # 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 # 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 # 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 # 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.

"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 # CSCdw85065

An Exercise Span operation can be performed even when a signal fail exists on the span. Since a signal fail has higher priority than Exercise Span (per Telcordia GR-1230), the Exercise Span should be disallowed. This issue will be resolved in Release 3.4.

DDTS # CSCdx40948

In a four fiber BLSR, an Exercise Span command might remain until the WTR timer expires. The required behavior is that an exercise request should terminate after either the expected behavior is performed or a higher priority request is detected. This issue will be resolved in Release 3.4.

DDTS # CSCdx38467

A force switch ring issued on one side of a node after an manual switch span is issued on the other side might fail to take place. This issue is very rare, and has only occurred after an upgrade from Release 3.1 to Release 3.3 on a four node OC-192 BLSR, when a manual switch span was issued on the west side of a node and force switch ring was subsequently issued on the east side. If this problem occurs, clear the force switch and re-issue it. This issue will be resolved in Release 3.4.

DDTS # CSCdw32540

The two protect OC48AS cards at the ends of a four fiber BLSR span must both be configured as either K3 or Z2 (not a mixture). If both ends are not the same, the BLSR may fail to switch correctly. In Release 3.4 the BLSR wizard will ensure that both ends are configured correctly; however, you must still avoid manually changing the value on one side only (and hence, causing a mismatch) at the card level.

DDTS # CSCdv80612

In two fiber BLSR only, a Line Status mismatch can occur in the node if the active TCC is rebooted while the ring is in switched mode. Four fiber BLSR will work correctly. To correct the situation if this occurs, remove and replace the FS-R or MS-R. This issue will be resolved in Release 3.4.

DDTS # CSCdw62602, CSCdw62594, CSCdw62625

Traffic loss can occur after a node isolation caused by four unidirectional failures on the four spans of a node. To recover from this situation, issue a Force Ring on both sides of the isolated node and proceed with fixing the failures. This issue will be resolved in Release 3.4.

DDTS # CSCdw53738

During a span upgrade of a 2 fiber BLSR with OC-12 to OC-192 cards, after you insert the OC-192 card, it may take a few minutes longer to boot up than usual. This issue will be resolved in a future release.

DDTS # CSCdw58950

You must lock out protection BLSR, 1+1, and UPSR traffic to avoid long, or double traffic hits before removing an active XC, XCVT, or XC10G card. You should also make the active cross connect card standby before removing it.

DDTS # CSCdw83805

SF-S can fail to preempt a manual ring switch. This can occur under the following conditions:

Step 1 Set up 4 node, 4 fiber, OC-48 BLSR.

Step 2 Provision an STS circuit between two diagonal nodes.

Step 3 Ensure STS traffic is running normally.

Step 4 Issue a manual ring switch on the east side of the span on the first node (of the two diagonals in Step 2 and observe that switch time should be less than 60 ms.

Step 5 Remove a fiber from the east span of the same node.

Step 6 Observe that the manual ring switch should be dropped.

Step 7 Observe the SF-S should up.

When this issue is present, the ring switch is not dropped. This issue will be resolved in Release 3.4.

DDTS # CSCdx15981

Placing the near end 4-fiber protect port in service while the far end working is detecting signal degrade can cause a traffic hit. For example, if, in a four node configuration, you introduce SD on the west working of the first node, then place the east protect of the fourth node out of service (this will cause a ring switch), and then place the same east protect card back in service, there will be a traffic hit, but the ring switch will remain in effect. To avoid this, issue a Force Ring command on the last node before you put its port back in service, then place the port in service, then remove the Force Ring command. This issue will be resolved in a future release.

DDTS # CSCdx18790

On a BLSR setup, when you vary SD-L on the East side and SF-L on the West side, at the same time, the XC could reboot. This condition is very rare and has only been seen when working and protect spans were varied simultaneously, causing an oscillating switching condition in the ring. This issue will be resolved in Release 3.4.

DDTS # CSCdx20789

If you clear a force switch span (FS-S) while a signal failure span (SF-S) is detected on the same span, the force switch span still exists, and a traffic hit results. 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 # CSCdx25134

Changing ring revertive behavior from non-revertive to revertive mode while all the spans' WTRs are active will cause a signal failure ring, but the ring switch fails to take place. To correct this situation, issue a Force Switch command at both ends on the span that detects signal failure ring (LOS or LOF). This issue will be resolved in a future release.

DDTS # CSCdx28899

Under circumstances where there are signal fails on both working and protect spans on one side, and a Lockout Span on the other side of a four fiber BLSR, the fail to switch alarm will be raised repeatedly, every few seconds. To clear the alarm, restore the working or protect as soon as possible. (This will clear the SF-R.) This issue will be resolved in Release 3.4.

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 # CSCdv70175

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

DDTS # 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 # 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

DDTS # CSCdv42151

When a UPSR circuit is created end-to-end, CTC might not create the cross-connection on all the nodes along the path at the same time. This might cause an SD-P condition along the path. When the circuit is fully provisioned on all nodes, the SD-P will clear automatically. Other conditions that can be expected while the circuit is being created are LOP-P and UNEQ-P. This issue will be resolved in a future release.

DDTS # CSCdv65732

Selecting UPSR attributes does not guarantee that automatic routing will choose or even prefer a route that uses path protection (as opposed to line protection). UPSR attributes are used only if the result of the routing (automatic or manual) happens to be a route that uses Path Protection. This issue is under investigation.

DDTS # CSCdw70796

Under certain high CPU load conditions, such as several (greater than 100) UPSR circuits each consecutively switching multiple times, a TCC reset can occur. To avoid this problem, after switching large numbers of UPSR circuits, allow a 30 second delay before further switching is incurred. Some software enhancements have been made in ONS 15454 Release 3.3 that lessen the likelihood of this condition. A further software enhancement is planned for a future release.

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.

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.

Inactive Login Message

In releases prior to Release 3.3 the message "Login Not Active" was displayed whenever you entered a command without first setting up a session (act-user) with the network element. To improve security, in Release 3.3 this message is no longer displayed.

DDTS # CSCdu53509

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

Resolved Software Caveats for Release *3.3*

The following items are resolved in Release 3.3.

Line Cards

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 is resolved in Release 3.3.

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 is resolved in Release 3.3.

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 is resolved in Release 3.3.

E Series and G Series Cards

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 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 3.3.

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 in Release 3.3.

Maintenance and Administration

DDTS # CSCdx23202

Certain combinations of concatenations, when provisioned in a certain sequence, can cause a large number of spurious B3 errors to be inserted into circuits carrying G1000-4 traffic.

These false B3 errors are detectable as signal fail or signal degrade alarm conditions, which could result in a UPSR switch. The combination and sequence of concatenations that cause this problem must include STS-1s and an STS-6 or greater circuit.

In general, when unexplained signal fail and signal degrade conditions are seen on a STS-1 G1000-4 circuit, this issue could be the problem. You can safely ignore the B3 errors and Signal Fail/Signal Degrade alarms on G1000 circuits if these circuits terminate on G1000 cards upon which an STS-1 also terminates.

As a workaround the circuit may be re-provisioned (re-sized), as an STS-3c, for example. This issue is resolved in Release 3.3.

DDTS # CSCdw59020

Cisco has no plans to support downgrades from XC10G to XC or XCVT cards. However, with Release 3.3, Cisco does support cross connect card downgrades that occur during the upgrade process (backing out of an XC or XCVT to XC10G card upgrade during the upgrade), in the event that circumstances make this necessary.

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 is resolved in Release 3.3.

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 is resolved in Release 3.3.

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. This issue is resolved in Release 3.3.

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. This issue is resolved in Release 3.3.

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 is resolved in Release 3.3.

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 provides payload visibility into SNMP traps for path/payload level alarm traps).

SNMP

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 3.3.

BLSR Functionality

Exercise Ring

In a four fiber BLSR, an Exercise Ring command might remain after the operation is completed. The required behavior is that an exercise request should terminate after either the expected behavior is performed, or the required switch completion time expires. This issue is resolved in Release 3.3.

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 is resolved in Release 3.3.

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 is resolved in Release 3.3.

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 is resolved in Release 3.3.

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 is resolved in Release 3.3.

TL1

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, 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 is resolved in Release 3.3.

New Features and Functionality

This section highlights new features and functionality for Release 3.3. For detailed documentation of each of these features, consult the user documentation.

Hardware

OC12/STM4-4 Card

The provisionable, four port OC12 IR 1310 nm (STM4 SH 1310nm) card, hitherto referred to as simply the OC12-4 card, provides the same functionality as the preexisting OC12 IR 1310, but with four times the port density. The card has greater optical sensitivity than the legacy OC12, and exceeds Telcordia optical specifications. Notably, From the legacy OC12 to the OC12-4, minimum receive power has gone from -28 dBm to -30 dBm, and minimum transmit power has gone from -15 dBm to -13 dBm.

To upgrade from the preexisting OC12 card to an OC12-4 without first removing the DCC, timing, ring, protection, or circuit provisioning, you can simply right-click on the card in the CTC node view, select the Change Card option from the popup menu and select OC12_4 from the Change To pull-down menu. An OC12 to OC12-4 span upgrade can be performed without disrupting traffic by right-clicking on the OC12 span in the CTC network view and selecting OC12-4 from the Upgrade To pull down menu. Note that the OC12-4 will not appear as an option in either the Card Change or Span Upgrade menus if the OC12 card to be upgraded is in a high speed slot or if XC10Gs are not installed.

The following rules and guidelines apply when using an OC12-4 card:

- SDCC connections can be provisioned on all four ports of the OC12-4.
- The OC12-4 card requires XC10G cross connect cards to operate.
- OC12-4 cards are supported for any multispeed slot (Slots 1-4 or 14-17) of the ANSI shelf.
- CTC does not support provisioning a working and protect path on the same OC12-4 card.
- While two fiber BLSR is supported on the OC12-4, the east and west spans cannot be provisioned on the same OC12-4 card.
- Working and protect UPSR paths cannot use the same OC12-4 card.
- Four fiber BLSR is not supported for this card.
- A 1+1 protection group must use the same port number for both the working and protect cards.

Software

UPSR Traffic Patterns

With Release 3.3, all primary (working) UPSR 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 UPSR circuit behaves more in line with current industry expectations, as defined in Telcordia GR-1400.

Automatic Host Detection

Automatic host detection, commonly referred to as “ARP sniffing,” has been added for the ONS 15454 TCC+ Ethernet port for Release 3.3. Automatic host detection allows a CTC workstation on a different subnet from the ONS 15454 node to directly connect to the node and launch CTC. Once automatic host detection is enabled it remains active at all times.

To enable automatic host detection, enter the IP address of the workstation as a default gateway for LAN connection. (In Microsoft Windows NT or 2000, choose Start > Settings > Control Panel > Network and Dial-up Connections > Local Area Connection > Properties. Select Internet Protocol, click the Properties button, click Advanced, click Add, and enter the IP address.) Once you have set up your workstation you must launch CTC before automatic host detection begins.

Note If you ping a node on a different subnet from the workstation before automatic host detection has started for that workstation, the ping will fail to reach the node.

Proxy Server Feature Set

The Proxy Server feature set allows a CTC session to access ONS 15454s while at the same time restricting unauthorized IP connectivity. Proxy server features can also reduce the amount of network setup required for external routers and CTC workstations. For a complete description of Proxy Server feature combinations and their use, and for important SNTP and DHCP configuration notes, consult the *Cisco ONS 15454 Reference Manual, Release 3.3*, section 10.2, ONS 15454 IP Addressing Scenarios.

Proxy Server is a set of three options (checkboxes) in the Provisioning > Network tabs listed under Gateway Settings: Craft Access Only, Enable Proxy and Enable Firewall. These new features can be used individually or in combination. Each is described briefly in the following sections.

Enable Proxy Server

When you select Enable Proxy, a proxy server task is activated on the ONS 15454 causing the ONS 15454 to behave in a similar manner to a SOCKS proxy for any other ONS 15454s that it has a DCC connection to. A CTC workstation connected to an ONS 15454 proxy server has CTC visibility to DCC-connected ONS 15454s even if there is no direct IP connectivity. All that is required is that the CTC workstation has connectivity to the ONS 15454 that has proxy server enabled.

Firewall

The Firewall feature can prevent CTC workstations from using an ONS 15454's DCC communications path to access other workstations on the DCN. When Firewall is enabled, unnecessary IP communications are restricted between the ONS 15454's DCC channels and the TCC+ Ethernet port. The node accomplishes this by discarding craft Ethernet packets not addressed to itself and DCC packets not addressed to itself or to a DCC peer.

Craft Access Only

In previous releases, when an ONS 15454 TCC+ detected an active link on its LAN port it would advertise a route to other DCC connected ONS 15454s indicating that all packets with a destination matching its own subnet should be routed to its LAN port. If two or more ONS 15454s were on the same subnet and had active links, multiple routes would result for packets on this subnet. This would cause some packets to be sent to one of the ONS 15454s and others to be sent to another resulting in loss of connectivity to some of the nodes in CTC. In previous releases, this behavior could be prevented by entering a static host route in the ONS 15454 with the connected CTC workstation as its destination.

The Craft Access Only feature allows multiple CTC sessions to ONS 15454 which are all on the same subnet, without the need to enter static host routes. When the feature is enabled, the ONS 15454 will not advertise routes to other 15454s it has DCC connectivity to. The ONS 15454 will only send packets for the connected CTC workstation through its LAN port. Other packets arriving from or being sent to other DCC connected nodes will be routed as though the CTC workstation is not connected.

Hitless Software Upgrades

Software upgrades from a previous release to Release 3.3 can be accomplished with no bit errors on traffic traversing or terminating in the ONS 15454 outside of the standard thresholds for hitless provisioning (60ms). The exception to this capability is the E-series Ethernet cards. Due to the necessary topology change observed by the software during a TCC+ reset, and subsequent spanning tree re-convergence, E-series cards do not pass traffic from the time of the active TCC+ reset (during activation) until the E-series cards reboot, plus approximately 30 to 45 seconds for spanning tree re-convergence. The total down time for E-series Ethernet traffic is approximately five minutes.

Note G-series Ethernet cards operate at layer one and do not lose traffic during an upgrade.

Network Time Protocol

The Network Time Protocol (NTP) feature enhances the SNTP (Simple Network Time Protocol) functionality of the ONS 15454 for Release 3.3. Now NTP servers are supported. Previously, the ONS 15454 supported only an SNTP server.

Note The ONS 15454 does not act as a time server. Rather, it acts as a client, obtaining time from the provisioned server.

Routing Improvements

Release 3.3 supports the ability to add a default route for connection to external systems. When the default route is added to one node, it is then advertised to all other DCC connected ONS 15454s and ONS 15327s.

Spanning Tree Control

Release 3.3 adds the ability to Turn Spanning Tree off for Ethernet circuits. You can disable or enable spanning tree on a circuit-by-circuit basis on unstitched Ethernet cards in a point-to-point configuration. This feature allows you to mix spanning tree protected circuits with unprotected circuits on the same card, to reuse VLANS, and to set up two single-card E-series Ethernet cards on the same node to form an intranode circuit.

AIS Off Mode for J1 Path Trace

In previous releases, when a J1 trace mismatch is detected the ONS 15454 inserts AIS path in the timeslot. The AIS off mode feature will allow customers to choose between sending or not sending AIS-P downstream from the TIM-P defect. When AIS-P is inserted downstream the likelihood of a traffic outage increases. The AIS off mode feature does not require any special configurations other than J1 compatible modules. See the *Cisco ONS 15454 Reference Guide* for details on J1 compatibility.

Orderwire Passthrough

In previous releases, the ONS 15454 only allows use of the Local/Express Orderwire function if each ONS 15454 in the ring or linear network has an AIC card installed in the node. Orderwire passthrough allows you to use the Local/Express Orderwire between two nodes that each have the AIC card, but have intermediate nodes between them that have no AIC card installed.

Line Buildout

Release 3.3 allows setting the Line Buildout (LBO) distance for the ONS 15454 BITS out signal. This setting is located in the Provisioning > Timing tabs. The setting is only applicable to the BITS Out signal and has no effect on the BITS in signal.

CTC Enhancements

The following settings are new for CTC in Release 3.3.

Worldwide Time Zone Support

CTC now supports the following US and worldwide standard time zones. All time zones are listed relative to GMT.

- (GMT-11:00) Midway Islands, Samoa
- (GMT-10:00) Honolulu
- (GMT-09:00) Anchorage
- (GMT-08:00) Los Angeles, Tijuana, Vancouver
- (GMT-07:00) Aklavik, Denver, Edmonton
- (GMT-07:00) Phoenix
- (GMT-06:00) Chicago, Mexico City
- (GMT-06:00) Costa Rica, Managua, San Salvador
- (GMT-06:00) Winnipeg
- (GMT-05:00) Bogota, Lima, Quito
- (GMT-05:00) Montreal, New York
- (GMT-05:00) Havana
- (GMT-05:00) Indianapolis, Nunavut
- (GMT-04:00) Asuncion
- (GMT-04:00) Caracas, La Paz, San Juan
- (GMT-04:00) Charlottetown, Halifax, Saint John
- (GMT-04:00) Santiago
- (GMT-04:00) Thule (Qaanaaq)
- (GMT-03:30) St. John's - Newfoundland
- (GMT-03:00) Brasilia, Rio de Janeiro, Sao Paulo
- (GMT-03:00) Buenos Aires, Georgetown
- (GMT-03:00) Godthab (Nuuk)
- (GMT-02:00) Mid-Atlantic
- (GMT-01:00) Azores, Scoresbysund (Ittoqqortoormiit)
- (GMT-01:00) Praia - Cape Verde
- (GMT-00:00) Casablanca, Reykjavik
- (GMT) Greenwich Mean Time
- (GMT+00:00) Dublin, London, Lisbon
- (GMT+01:00) Amsterdam, Berlin, Rome, Paris
- (GMT+01:00) Algiers, Lagos, Luanda
- (GMT+01:00) Windhoek (Namibia)
- (GMT+02:00) Al Jizah, Alexandria, Cairo
- (GMT+02:00) Amman
- (GMT+02:00) Athens, Bucharest, Helsinki, Istanbul

- (GMT+02:00) Beirut
- (GMT+02:00) Cape Town, Harare, Johannesburg, Tallinn
- (GMT+02:00) Jerusalem
- (GMT+02:00) Kaliningrad, Minsk
- (GMT+03:00) Aden, Antananarivo, Khartoum, Nairobi
- (GMT+03:00) Baghdad
- (GMT+03:00) Moscow, St. Petersburg, Novgogrod
- (GMT+03:30) Tehran
- (GMT+04:00) Abu Dhabi, Mauritius, Muscat
- (GMT+04:00) Aqtau, T'bilisi
- (GMT+04:00) Baku
- (GMT+04:00) Yerevan, Samara
- (GMT+04:30) Kabul
- (GMT+05:00) Chelyabinsk, Prem, Sverdlovsk, Ufa
- (GMT+05:00) Islamabad, Karachi, Tashknet
- (GMT+05:30) Calcutta, Madras, Mumbai (Bombay), New Delhi
- (GMT+05:45) Kathmandu
- (GMT+06:00) Almaty
- (GMT+06:00) Colombo, Dhaka
- (GMT+06:00) Novsibrisk
- (GMT+06:30) Cocos, Rangoon
- (GMT+07:00) Bangkok, Hanoi, Jakarta
- (GMT+07:00) Krasnoyarsk, Norilsk, Novokuznetsk
- (GMT+08:00) Beijing, Shanghi, Hong Kong, Urumqi,
- (GMT+08:00) Perth
- (GMT+08:00) Singapore, Manila, Taipei, Kuala Lumpur
- (GMT+09:00) Chita, Yakutsk
- (GMT+09:00) Osaka, Sapporo, Tokyo
- (GMT+09:00) Palau, Pyongyang, Seoul
- (GMT+09:30) Adelaide, Broken Hill
- (GMT+09:30) Darwin
- (GMT+10:00) Brisbane, Port Moresby
- (GMT+10:00) Canberra, Melbourne, Sydney
- (GMT+10:00) Hobart
- (GMT+10:00) Khabarovsk, Vladivostok
- (GMT+10:30) Lord Howe Island
- (GMT+11:00) Honiara, Magadan, Noumea
- (GMT+11:30) Kingston - Norfolk Island

- (GMT+08:00) Perth
- (GMT+08:00) Singapore, Manila, Taipei, Kuala Lumpur
- (GMT+09:00) Chita, Yakutsk
- (GMT+09:00) Osaka, Sapporo, Tokyo
- (GMT+09:00) Palau, Pyongyang, Seoul
- (GMT+09:30) Adelaide, Broken Hill
- (GMT+09:30) Darwin
- (GMT+10:00) Brisbane, Port Moresby
- (GMT+10:00) Canberra, Melbourne, Sydney
- (GMT+10:00) Hobart
- (GMT+10:00) Khabarovsk, Vladivostok
- (GMT+10:30) Lord Howe Island
- (GMT+11:00) Honiara, Magadan, Noumea
- (GMT+11:30) Kingston - Norfolk Island
- (GMT+12:00) Anadyr, Kamchatka
- (GMT+12:00) Auckland, Wellington
- (GMT+12:00) Marshall Islands
- (GMT+12:00) Suva - Fiji
- (GMT+12:45) Chatham Island
- (GMT+13:00) Nuku'alofa
- (GMT+13:00) Rawaki, Phoenix Islands
- (GMT+14:00) Kiritimati, Christmas Islands

Software Download Collision Avoidance

Release 3.3 allows multiple users connected to an ONS 15454 ring to download software simultaneously. This functionality avoids collisions by prohibiting multiple software downloads from occurring on any single node. No special configurations are needed to use this feature.

Prevention of Identical User ID and Password

As of Release 3.3, CTC and TL1 prevent the creation of a userid and password that are identical. The userid and password are identical if they contain the same characters in the same numbers and sequence, irrespective of case. For example, “betsy” and “BeTSy” are considered to be the same, while “betsy”, “ysteb” and “betssy” are all different.

As of Release 3.3, CTC and TL1 prevent the creation of a password containing as a subset of characters the associated userid. The password contains the associated userid if it contains anywhere within it the same characters in the same numbers and sequence that make up the entire userid, irrespective of case. For example, password “SBeTSyXC” and userid “betsy” are disallowed, while password “betsy” and userid “SBeTSyXC”, or password “bet3sy” and userid “BeTSy” are allowed.

Enforce Password Complexity

Both TL1 and CTC will not allow creation of new passwords that do not comply with Telcordia GR-815, which states that passwords must be at least six characters long, contain at least one alphabetic, one numeric and one special character (+, # or %).

Note TL1 and CTC warn on entry only when a pre-existing non-GR815 compliant password is used, permitting the user to continue with the older password.

Password Toggling Prevention

As of Release 3.3 TL1 and CTC prevent users from changing a password to the current password value. For example, if the existing password is "*@nite", the new password cannot also be "*@nite".

TL1 Enhancements

TL1 Over VT100

As of Release 3.3, the ONS 15454 supports TL1 over VT100 through the RS-232 port.

Additional Feature Support

The following feature enhancements have been added to TL1 for Release 3.3.

- Support for 4-port G1000
- Support for 4-port OC12
- Support for STS9c and 24c
- Enhanced Setting of Timing Source (RTRV-NE-GEN, ED-NE-GEN)
- Support for reporting database changes

Commands Changed

The parameter <qres> has been changed to <qref> for the RTRV-SYNCN command.

New Commands

The following TL1 commands are new with Release 3.3.

- RTRV-ALM-RING
- RTRV-COND-RING
- REPT EVT COM
- ALW-MSG-DBCHG
- INH-MSG-DBCHG
- REPT DBCHG
- REPT EVT ENV

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15454, Release 3.2*
- *Release Notes for the Cisco ONS 15454 SDH, Release 3.3*
- *Release Notes for the Cisco ONS 15327, Release 3.3*
- *Cisco ONS 15454 Software Upgrade Guide, Release 3.3*

Platform-Specific Documents

- *Cisco ONS 15454 Procedure Guide, Release 3.3*
- *Cisco ONS 15454 Reference Guide, Release 3.3*
- *Cisco ONS 15454 Troubleshooting Guide, Release 3.3*
- *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide, Release 3.3*
- *Cisco ONS 15454 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.