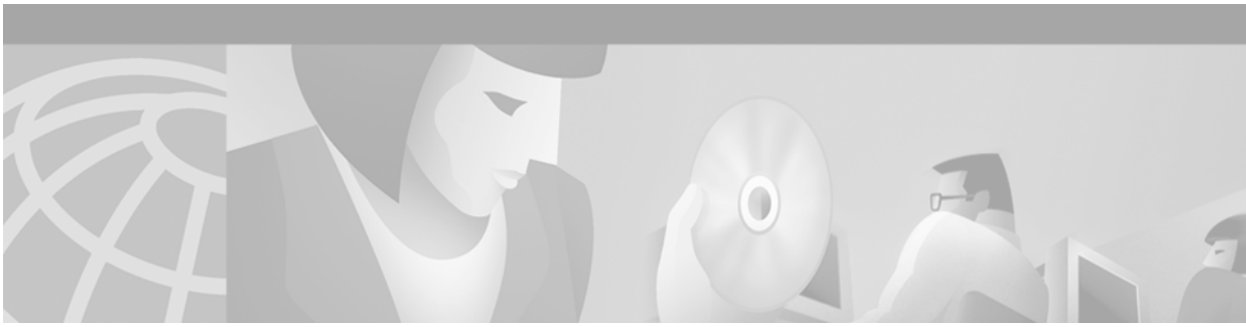

Release Notes for Cisco ONS 15327 Release 3.4.2

December, 2003

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15327 SONET multiplexer. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to Release 3.4 of the *Cisco ONS 15327 Installation and Operations Guide*, *Cisco ONS 15327 Troubleshooting and Reference Guide*, and *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide*, *Release 3.4*. For the most current version of the *Release Notes for Cisco ONS 15327 Release 3.4.2*, visit the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/ong/15327/rnotes/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

Changes to the Release Notes, page 2

Caveats, page 2

Resolved Software Caveats for Release 3.4.2, page 9

New Features and Functionality, page 12

Related Documentation, page 19

Obtaining Documentation, page 19

Obtaining Technical Assistance, page 20

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 15327 Release 3.4.2* since the production of the Cisco ONS 15327 System Software CD for Release 3.4.2.

The following changeshave been added to the release notes for Release 3.4.2.

Changes to Caveats

The following new caveat has been added to the release notes.

JRE Updates, page 2

DDTS # CSCeb05404, page 2

Caveats

Review the notes listed below before deploying the ONS 15327. 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.

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

DDTS # CSCeb05404

PWR-A/B alarms can become stuck for an ONS 15327 node in the event of a transient power failure. The alarms will clear after resetting both XTCs. This issue is resolved in Release 4.6.

DDTS # CSCea92645

Under certain conditions, CTC displays "Fail" on the XTC during software download from the active XTC card. This can occur when, on an ONS 15327 node with a single XTC, you insert a protect XTC with a different software release from that of the active XTC. The standby XTC boots up (this takes approximately 1 minute), and then begins copying software from the active XTC. In node view, CTC shows the status of the standby XTC as "Ldg" (Loading). The Maintenance > Protection > XTC Protection Group tab also shows the card as loading. CTC's node view displays the loading state for approximately two minutes, after which the state transitions to "Fail," and the LED status color shown for the card in CTC becomes red. In the Maintenance > Protection > XTC Protection Group tabs, the card is displayed as "Failed." The "Fail" state displays until the standby XTC copies all software from the active XTC (approximately 20 minutes). After this, the standby XTC reboots and comes up on its own.

Note This issue only occurs if a new XTC with a different software version is introduced in an ONS 15327 node with an existing active XTC. This issue will not occur if the software download is initiated through CTC.

To distinguish if the standby XTC has really failed or is merely copying software from the Active XTC, physically view the standby XTC card. In the case of a software download, the Act/Sby LED illuminates and the Fail LED on the standby XTC blinks for the duration of the download. In the case of a genuine failure, only the Fail LED illuminates. The XTC reboots on its own after approximately 20 minutes. If the Fail status in CTC persists beyond 20 minutes, then the standby XTC card may have undergone a genuine failure, in which case it should be replaced. This issue will be resolved in Release 4.6.

DDTS # CSCdz00573

The OC3 and EC1 are the only cards for which near end STS path PM is available to CTM . To retrieve near end path PM for other cards, use TL1, SNMP, or CTC. Note that far end STS path PM is available for all electrical cards and the OC3. This issue will be resolved in a future release.

DDTS # CSCdy10030

CVs are not positively adjusted after exiting a UAS state. When a transition has been made from counting UAS, at least 10 seconds of non-SES must be counted to exit UAS. When this event occurs, Telcordia GR-253 specifies that CVs that occurred during this time be counted, but they are not. There are no plans to resolve this issue at this time.

DDTS # CSCdy56366 and CSCdy12392

With a 1+1 protection group and OC-3 or OC-12 cards, when a protection switch occurs, the PSC and PSD fields on the performance pane do not increment. This issue will be resolved in a future release.

DDTS # CSCdy71653

A change of the alarm profile while alarms are present on a DS3 card is not correctly applied. The behavior is specific to DS3 ports on an ONS 15327 node. This issue will be resolved in a future release.

DDTS # CSCdy49608

A node connection might fail during bulk circuit creation, causing the circuit creation to also fail. For example, this has been seen while creating 224 VT 1.5 protected circuits, on a UPSR consisting of eight ONS 15327 nodes. If you experience a bulk circuit creation failure of this type, cancel the circuit creation batch, then delete any incomplete circuits. Restart the batch from the last successful circuit. This issue will be resolved in a future release.

DDTS # CSCdx35561

CTC is unable to communicate with an ONS 15327 that is connected via an Ethernet craft port. CTC does, however, communicate over an SDCC link with an ONS 15327 that is Ethernet connected, yielding a slow connection. This situation occurs when multiple ONS 15327s are on a single Ethernet segment and the nodes have different values for any of the following features:

- Enable OSPF on the LAN
- Enable Firewall
- Craft Access Only

When any of these features are enabled, the proxy ARP service on the node is also disabled. The ONS 15327 proxy ARP service assumes that all nodes are participating in the service.

This situation can also occur immediately after the aforementioned features are enabled. Other hosts on the Ethernet segment (for example, the subnet router) may retain incorrect ARP settings for the ONS 15327s.

To avoid this issue, all nodes on the same Ethernet segment must have the same values for Enable OSPF on the LAN, Enable Firewall, and Craft Access Only. If any of these values have changed recently, it may be necessary to allow connected hosts (such as the subnet router) to expire their ARP entries.

You can avoid waiting for the ARP entries to expire on their own by removing the SDCC links from the affected ONS 15327 nodes. This will disconnect them for the purposes of the proxy ARP service and the nodes should become directly accessible over the Ethernet. Network settings on the nodes can then be provisioned as desired, after which the SDCC can be restored.

This issue is under investigation.

DDTS # CSCdy11012

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

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

To work around this issue, if no firewall enabled, then the network configuration of the CTC host can be changed to allow CTC to see all nodes in the network. The launch node must be on its own subnet to prevent network partitioning, and craft access must not be enabled. The CTC host must be provisioned with an address on the same subnet as the initial node (but this address must not conflict with any other node in the network), and with the default gateway of the initial node. CTC will now be able to contact all nodes in the network.

If a firewall is enabled on any node in the network, then CTC will be unable to contact nodes outside of the initial OSPF areas. This issue is under investigation.

DDTS # CSCdy37198

On Cisco ONS 15454 and ONS 15327 platforms equipped with XC or XCVT cross-connect cards, Ethernet traffic may be lost during a BLSR protection switch, with no accompanying alarm or condition raised. Possible affected circuits will be between Ethernet cards (E100T-12 and/or E1000F-2) built over Protection Channel Access (PCA) bandwidth on BLSR spans. When BLSR issues the switch, the PCA bandwidth is preempted. Since there is no longer a connection between the ends of the Ethernet circuit, traffic is lost. Further, in nodes equipped with XC or XCVT cards, neither the E100T-12 nor the E1000F-2 cards raise an alarm or condition in CTC. In nodes equipped with XC10G, these Ethernet cards will raise an AIS-P condition. This issue will be resolved in a future release.

DDTS # CSCdy38603

VT Cross-connects downstream from a DS1 can automatically transition from the OOS-AINS state to the IS state even though the DS1 signal is not clean (for example, when there is an LOS present). This can occur when you have created a VT circuit across multiple nodes with DS1s at each end, and you have not yet applied a signal to the DS1 ports, and then you place the DS1 ports in OOS-AINS, OOS-MT, or IS. When you then place the circuit in OOS-AINS, the circuit state changes to IS (within one minute). This issue will be resolved in a future release.

DDTS # CSCdw43896

A software revert from Release 3.3 or 3.4 to 1.0.1 or 1.0.2 can cause a PDI-P alarm on intermediate nodes of a DS3 circuit after an XTC switch on the node terminating this circuit. This can occur when, after you revert all the nodes of a UPSR from Release 3.3-4 to Release 1.0.1-2, then perform an XTC side switch on the node terminating the DS3 circuit. If this occurs, remove the active XTC (software reset will not work) on the node terminating the DS3 circuit. This issue is resolved for Releases 3.3 and later, but will still occur when you revert from one of these releases to Release 1.0.1-2. The issue cannot be resolved for these earlier releases.

Upgrades from Release 1.0

If you wish to upgrade from Release 1.0 to Release 3.4, you must first upgrade to maintenance Release 1.0.2. If you are already running maintenance Release 1.0.1, you do not have to perform the intermediate upgrade.

DDTS # CSCds23552

You cannot delete the standby XTC once it is removed. If you have two XTC cards and then decide to operate with only one, you will get a standing minor alarm. The alarm cannot be removed by CTC. The XTC is a combo card, combining the functionality of the ONS 15454 TCC+, cross connect, DS1 and DS3 cards, with a protection group automatically provisioned. On the ONS 15454, similar behavior occurs for the TCC+ card. The cross connect card for the ONS 15454 can only be deleted if there are no circuits provisioned. DS1 and DS3 cards can only be deleted if they are not in a protection group. It is not known at this time when or if this issue will be resolved.

E Series and G Series Cards

DDTS # CSCdy41135

When using a G1000-2 card, TIM-P can be mistakenly raised on a PCA circuit after a protection switch. This occurs when path trace is enabled on a PCA circuit that is no longer in use after a protection switch. To work around this issue, either disable path trace or use alarm profiling to filter out the unwanted alarm. This issue is under investigation.

DDTS # CSCdy63172

With E100/E1000 cards, a CARLOSS alarm present, and port alarms suppressed from CTC, Manual Alarm Suppression does not correctly suppress CARLOSS alarms. This issue is under investigation.

DDTS # CSCdy47038

G1000-2 path alarm profiles applied on port 2 are not updated to reflect the correct alarm severities. This issue is under investigation.

DDTS # CSCdy13035

Excessive Ethernet traffic loss (greater than 60 ms) may occur when the active XTC is removed from the chassis while using the G1000-2. On rare occasions, permanent loss of traffic may occur. Do not remove the active XTC from the chassis to force a protection switch. Instead, perform a soft reset of the active XTC through the network management interface. Once the XTC is in standby mode, it can be removed from the chassis without inducing excessive traffic loss. A future hardware release will incorporate improved hardware PLL circuitry on the G1000-2 line card to allow an active XTC removal without causing excessive traffic loss.

BLSR Functionality

DDTS # CSCdy65890

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

DDTS # CSCdy48872

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

To see this issue, on a node participating in a two fiber BLSR with PCA circuits terminating at the node over the two fiber BLSR, cause an SF-R by failing the receive fiber in one direction (say, west). Then, issue a lockout span in the other direction (in our example, east). Since the lockout span has higher

priority than the SF-R, the ring switch should clear and PCA traffic should be restored on spans without a fiber fault. The ring switch does clear, but PCA traffic does not restore. To correct this issue, clear the fiber fault. All traffic restores properly. This issue will be resolved in Release 4.0.

DDTS # CSCdy30125

In a two by two BLSR configuration, with PCA circuits passing through the common node, if one of the rings is a two fiber BLSR and you upgrade it, a PCA connection will be promoted to become protected on the upgraded ring side. In this scenario, you can end up with a circuit that is PCA on one ring and protected on the other ring.

This can occur with any colliding STSs; in other words, any situation where the STS from the working side is going to overlay the STS from the protection side when a ring or span switch occurs. On a span switch in a four fiber BLSR this would be STS #1 on the working and STS #1 on the protect on the same side (i.e. east or west). For a ring switch on a four fiber BLSR it would be STS #1 on the working and STS #1 on the protect on the opposite side of the ring. In a two fiber BSLR there is only a ring switch, so the colliding STSs would be STS #1 on one side of the ring and STS #7 on the opposite side (for an OC-12 ring, for example). Symptoms of a failure will be protected traffic that is dropped or that has a stuck AIS-P.

When you perform a two fiber BLSR upgrade in a two by two configuration, ensure that no PCA circuits cross through the common node before you start the upgrade. Note that the PCA circuits that are added and dropped on the same ring are safe, as they will be promoted to become fully protected. All PCA circuits that cross the common node to go to another ring must be deleted before the upgrade, then recreated once the upgrade is successfully finished. This issue will be resolved in Release 4.0.

DDTS # CSCdy10805

If you upgrade one of the rings in a two by two BLSR configuration, an EXTRA-TRAF-PREEMPT alarm may be raised and subsequently fail to clear on one of the rings. If the ring that has the stuck alarm already has some PCA circuits on it, you can issue and then clear a Force Ring. This should clear the stuck alarm. If no PCA circuits exist on the ring, then create one temporarily, and follow the above procedure to clear the alarm. After the alarm clears, you can remove the Force Ring, then delete the PCA circuit. This issue will be resolved in Release 4.0.

DDTS # CSCdv89939

After a BLSR span or ring switch, traffic is switched to a different set of nodes and a protection STS is used. At this point, any ongoing J1 monitoring does not follow the switch. As a result, there is no J1 monitoring on the protection path. If there is a mismatch of the J1 string on the protection path, the TIM_P alarm will not be raised. Also, you can retrieve the actual captured J1 string on the working path, but if BLSR switched from working to protect, you cannot retrieve the J1 string on the protect path. BLSR support for J1 trace is a feature request that will be addressed in a future release.

DDTS # CSCdy59242

Under some circumstances, if a fail-to-switch alarm is raised upon introducing SF-R with the existing Lockout Span command, the alarm becomes stuck after the SF-R and Lockout Span are cleared.

The following example illustrates how this can occur.

In a two fiber BLSR, say the east side of Node 1 is connected to the west side of Node 2.

Step 1 Perform a Lockout Span on the east side on Node 1.

Step 2 Remove the transmit fiber on the east span of Node 1. (Node 2 detects signal failure on its west side.) Traffic is lost, as expected, due to the Lockout Span on the ring. A Fail-to-Switch alarm is raised.

Step 3 Re-insert the transmit fiber. Traffic comes back, but the fail-to-switch alarm is still reported.

Step 4 Clear the Lockout Span. The Fail-to-Switch alarm becomes stuck.

The issue is that Node 2 ignores a long-path Lockout Span on its east side and initiates a ring switch with a local SF-R request, then fails.

To avoid this issue, make sure the ring is in the idle state and issue an Exercise Ring command on the span that reports Fail-to-Switch alarm to clear that alarm. This issue will be resolved in Release 4.0.

DDTS # CSCdy59877

Rarely, an optical card participating in a BLSR may lose communication with the XC card in the same node, resulting in a traffic switch away from that optical card and a COMIOXC alarm raised on the XC. To recover from this situation, issue a soft reset on the optical card from CTC. This issue will be resolved in Release 4.0.

DDTS # CSCdw66416

Traffic along a running ring segment cannot be restored while a participating node is rebooting. To see this problem, in a two fiber BLSR with circuits created along a given ring segment, you must isolate that ring segment by powering down two or more nodes where one of the nodes powered down is at the edge of the segment and the others are outside of the segment. Then power up and reboot the node at the edge of the segment. The circuits along this segment will not be restored even though the nodes on the segment are both up and running. You must restore power to all nodes before the traffic is restored. This issue will be resolved in a future release.

BLSR Support for Mixed Node Networks

The ONS 15327 is supported for BLSR in combination with ONS 15454 nodes only if Release 3.3 or greater is installed and running on all BLSR nodes. If you wish to provision a BLSR on a combination of ONS 15327 and ONS 15454 nodes, you should upgrade to Release 3.3 or greater on all ONS 15454 and ONS 15327 nodes first.

UPSR Functionality

DDTS # CSCdy62713

If you change the state of a UPSR VT non-revertive circuit from IS to OOS and back to IS, then fail an active fiber span carrying the circuit, the circuit will not switch, and this can result in traffic outage. To avoid this, make sure the circuit is revertive before placing it in the OOS (out of service) state. Wait at least 30 seconds before changing a VT UPSR selector from one state to another. This issue will be resolved in a future release.

DDTS # CSCdw66071

After a switch to protect is cleared for a revertive UPSR circuit, the WTR alarm is not raised, although the wait period is observed and the circuit reverts back to working. This issue will be resolved in Release 4.0.

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.

Commands not Supported in Release 3.4.1 or 3.4.2

The following commands are not supported:

- OPR-UPGRADE
- DLT-<MOD2>, ENT-<MOD2>, RMV-<MOD2>, and RST-<MOD2> do not apply to DS1, STS1, STS3C, STS12C, STS48C, VT1
- ED-EQPT
- ED-VT1
- RTRV-VT1

These commands will be supported in a future release.

Performance Monitoring

DDTS # CSCdt10886

The far-end STS PM counts do not accumulate on an OC-48 linear 1+1 circuit even though the near-end STS PM counts on the other end are increasing. To see this issue, connect two nodes with an OC-12 or OC-48 linear 1+1 protected span. Place a piece of test equipment in the middle of the span and inject B3 errors. The near-end STS PM counts accumulate, but the far-end STS PM counts do not accumulate. To work around this issue, Use the near-end STS PM count from the adjacent node to see the far-end STS PM count for the current node. This issue will be resolved in a future release.

Resolved Software Caveats for Release 3.4.2

The following items are resolved in Release 3.4.2.

Maintenance and Administration

DDTS # CSCeb82474

Rarely, a routing loop may be inadvertently created on the nodes in a network using OSPF. This can occur after a topology change (DCC link down, or LAN interface down). If this occurs, wait for 20 minutes for OSPF to refresh. This issue is resolved in Releases 3.4.2 and 4.x.

Performance Monitoring Using Cisco Transport Manager

In Release 3.4, Cisco Transport Manager users that performed PM retrievals might have encountered any or all of the following issues:

- G1000 statistics appearing unpredictably in the wrong fields
- Missing PM data
- Correct PMs falsely marked as invalid
- Incorrect PMs not marked as invalid

These issues were most likely to occur with SONET path data. SDH path data was unaffected. All of these issues have been resolved in Release 3.4.1.

DDTS # CSCdx02680

If you create a VT circuit, set the DS1 port in service, generate any alarm, then set the port out of service, you may see VT alarms that will not clear. To clear the alarms, delete the VT circuit. This issue is resolved in Release 3.4.

DDTS # CSCdw71844

If a manual switch request is made when a higher priority request is present (in other words, SD/SF or lockout), the user request 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. This issue is resolved in Release 3.4.

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 is resolved in Release 3.4.

DDTS # CSCdt30119

VT1.5 circuits might require new VT tunnels despite sufficient bandwidth on existing VT tunnels. In complex configurations of the Cisco ONS 15327 that use both 1+1 and UPSR protection, automatic circuit routing may fail to use existing VT tunnels. When you create new VT1.5 circuits with automatic

circuit routing, the ONS 15327 might prompt you to create new VT tunnels even though sufficient bandwidth is available in existing VT tunnels. Use manual routing to specify a path for the VT1.5 circuit through the existing VT tunnels. This issue is resolved in Release 3.4.

Line Cards

DDTS # CSCdt50628

B3 errors might appear on an OC-12 span after an XTC side switch. A one-time burst of B3 errors might occur after an XTC side switch when the ONS 15327 is configured with an OC-12 line card. This is a rare condition which has been seen in approximately 1% of such XTC side switches. The result is less than 1 errored second. No traffic outage is associated with this burst of B3 errors. The issue only arises with OC-12 configurations. OC-48 configurations are not affected. This issue is resolved in Release 3.4.

BLSR Functionality

DDTS # CSCdw64086

For a given BLSR node equipped with two XTCs or two TCCs, say Node 1, if you back up the database, change the node ID of any of the other nodes in the ring, and then restore the database for Node 1, following completion of the database restoral, a node ID mismatch condition will exist. However, the node ID mismatch alarm may not be raised to warn you that BLSR will not function properly. If this occurs, after the database restoral has completed, you can change the local node's Node ID (you can then change it back to the previous ID if you prefer) to restore functionality of the BLSR (and clear the alarm, if it is raised). If you perform a database restoral on a BLSR node, always verify afterwards that all nodes in the ring have the correct ring map. This will ensure that any such issue for which an alarm is not raised can be found and corrected. This issue is resolved in Release 3.4.

UPSR Functionality

DDTS # CSCdx40081

If, in an OC-48 UPSR network, there is an STS-3C circuit, using STS 4-6, that terminates on OC-12 IR cards, and 28 VT circuits are bulk provisioned between two nodes on the ring, the STS-3C circuit can take at least one traffic hit during the VT circuit provisioning process. This only occurs if an OC-12 IR card has been reset after the STS-3C circuit was created.

Deleting one or more VT circuits in the same situation may also cause an STS3C traffic hit. This issue is resolved in Release 3.4.

TL1

DDTS # CSCdz08632

If you do not explicitly specify the SdBer attribute when using TL1 to create UPSR circuits, the default path SdBer value is incorrectly set to E-7. The correct default value is E-6. This issue is resolved in Release 3.4.1.

DDTS # CSCdy85319

TL1 sessions launched using the CTC TL1 client appear to be slow and eventually fail if CTC cannot make a direct connection to the node. This can happen if CTC is separated from the node by a firewall and is using the proxy server on a gateway node to manage an exterior node. To avoid this issue, when choosing a node in the Select Node dialog, choose the gateway node rather than the exterior node. When entering

TL1 commands, specify the exterior node in the TID field (between the first and second colons) of each command. For instance, if the exterior node is named ENE, you would log in using the command:

```
ACT-USER:ENE:johndoe:$::********;
```

This issue is resolved in Release 3.4.1.

New Features and Functionality

This section highlights new features and functionality for Release 3.4.x. For detailed documentation of each of these features, consult the user documentation.

New Hardware

G1000-2

Release 3.4 introduces the G1000-2 card for the ONS 15327. This card enables the creation of a carrier-class Ethernet private line service over a SONET/SDH network. The G1000-2 card maps up to two Gigabit Ethernet interfaces onto a SONET transport network. The G1000-2 card provides line rate forwarding for all Ethernet frames (unicast, multicast and broadcast) and can be configured to support Jumbo frames (defined as a maximum of 10,000 bytes). The two ports on the G1000-2 can be mapped independently to any combination of STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-24c and STS-48c circuit sizes, as long as the sum of the sizes of circuits terminating on a card does not exceed STS-48c.

Note Read the Release Notes "Caveats" section on page 2 before creating circuits on the G1000-2 card.

G1000-2 cards are equipped with two SFP-LC (Small Form-factor Pluggable) connectors used for optical cable termination. The SFPs must be ordered separately. G1000-2 cards are rated at about 30 watts per card.

The G1000-2 supports Asymmetric 802.3x flow control and frame buffering to reduce data traffic congestion. The G1000-2 supports end-to-end Ethernet link integrity.

Before installing the G1000-2 card, the ONS 15327 node must be running Release 3.4 or greater. The G1000-2 card can be installed into any general-purpose line card slot.

New Software Features and Functionality

Microsoft Windows XP

Release 3.4.x supports the Microsoft Windows XP operating system.

Queued & Preemptive Switching

In releases prior to 3.4, the node accepted and stored switch commands regardless of higher priority requests. Once the higher priority request was cleared, the lower priority command was applied. Also, although the software preempted lower priority user commands for higher priority requests, it reapplied the lower priority command once the higher priority request had been cleared or completed.

Release 3.4 complies with Telcordia GR-253 Issue 2, allowing a higher priority, local or remote request to preempt (override) an external, lower priority request. The preempted request is not retained in memory or in a queue for completion (in other words, when the higher priority request is cleared, the preempted switch request will not be reinitiated). Thus, when you attempt to apply a switch command under these circumstances, the request will be denied.

In Release 3.4, you will be notified immediately if a condition occurs in which a command is overridden. The software will deny a switch request immediately if a higher priority request already exists.

This behavior applies to all protection types: 1:1, 1:N, 1+1, BLSR and UPSR. (Note that in Release 3.3, 1:1 and 1:N are fully compliant).

For details on possible switch commands and their associated priority levels, as well as other actions can affect the Automatic Selector Criteria switch state, consult the user documentation for Release 3.4.

Multiple OSPF Areas

In releases prior to 3.4, only one OSPF area was supported within a data communication channel (DCC) network. With Release 3.4, you can configure multiple areas on different DCC links for the same node. This type of configuration limits the amount and size of flooded Link State Advertisement (LSA) updates to individual areas that occur each time there is a topology change or scheduled update. This gives you the ability to better control the amount of traffic over each DCC link.

RIP Support

In releases prior to 3.4, only static routes and OSPF routing protocols were supported for a TCC LAN. Many deployed networks today use RIP to exchange IP routing information. Release 3.4 provides RIP as a routing protocol option, giving the network designer increased flexibility and more choices for network design. In a small network, RIP has the advantage of very little overhead in terms of bandwidth used and configuration and management time. RIP is also easy to configure and implement.

RIP is a distance vector routing protocol, in which the router only exchanges routing information between connected neighbors. RIP Version 1 advertises routes by sending updates to the broadcast address 255.255.255.255. All devices on the LAN receive and process broadcasts. RIP Version 1 is a

classful routing protocol. Classful routing always summarizes routes by the major network numbers and always considers the network class. This is always done at network boundaries. Subnets are not advertised to other major networks. Non-contiguous subnets are not visible to each other.

RIP Version 2 advertises routes by sending updates to IP multicast address 224.0.0.9. To reduce unnecessary load on those hosts that are not listening to RIP-2 messages, the IP multicast address is used for periodic broadcasts. RIP Version 2 is a classless routing protocol. Classless routing differs from classful routing in that the prefix length is transmitted. The prefix length is evaluated at each point it is encountered throughout the network. Thus, the prefix length can be changed to advertise routes differently at different locations within a network. Classless routing enables more efficient use of IP address space and reduces routing traffic.

The RIP-2 feature can be enabled on a LAN management interface through CTC to advertise to a router on the network. You can choose between OSPF and RIP, with “None” as the default.

Up to 25 occurrences each of the address-family identifier (AFI), address, and metric fields are permitted in a single IP RIP packet. That is, up to 25 routing table entries can be listed in a single RIP packet. If the AFI specifies an authenticated message, only 24 routing table entries can be specified.

RIP uses hop count to rate the value of each different route. The hop count is the number of routers that can be traversed in a route. A directly connected network has a metric of zero; an unreachable network has a metric of 16.

To avoid a potential routing loop when distributing routes between RIP and OSPF, a node only advertises routes it knows through RIP. Any RIP updates the node receives from the routers on the LAN are discarded. For any network behind the directly connected router, static routes must be provisioned on the node.

Static Route Enhancement

In releases prior to 3.4, ONS 15454s discovered each other on the network using OSPF through IP, over PPP, over SDCC. In Release 3.4, static route enhancement allows ONS 15454s and ONS 15327s to communicate with 3rd party equipment using IP over PPP over SDCC. You can disable OSPF on the CTC SDCC Termination screen. You can then create route entries in the Static Route tab to access IP-enabled 3rd party equipment.

Note Static Route Enhancement will not allow visibility to 3rd party equipment using IP over PPP over SDCC when the proxy/firewall feature is enabled.

Enhanced State Model

The Release 3.4 enhanced state model adds increased control of the service state for ports and circuits. This state model provides increased options for entities (ports, equipment, or circuits) out of service, awaiting automatic activation, or out of service and under maintenance. The new state model provides the ability to provision an entity as service-ready while awaiting the arrival of an additional required item (traffic or physical card) before going into service.

In addition to the established states, IS (In Service) and OOS (Out of Service), the enhanced state model adds the Out of Service-Auto In Service (OOS-AINS) and Out of Service-Maintenance (OOS-MT) states.

Note Loopbacks are only allowed when the entity is in the OOS_MT, or OOS_AINS state.

Maintenance Mode

The OOS-MT mode is the same as the IS mode except that alarms are not reported autonomously, yet they can still be retrieved. Maintenance is allowed while an entity is in this state. This OOS-MT state applies to the port level and the circuit level.

Auto In-Service Provisioning

The enhanced state allows any entity to be in an Auto In-Service (OOS-AINS) state. This state allows you the ability to provision an entity (port, equipment, or circuit) to be ready to be placed in service, but to await the arrival of the required item (traffic or physical card) before actually going into service. This allows pre-provisioning of circuits and cards, which then automatically activate upon the detection of the appropriate signal or hardware (for example, when a card is inserted). The OOS-AINS state saves carriers from the need to filter alarms due to the pre-provisioning of circuits before the signal is received from their customers. In the case of cards, the feature permits accurate reflection of the expected status of the card while the card itself has yet to be inserted. When an entity is in the OOS_AINS state, alarms associated with the entity are reported in the conditions pane, rather than the alarms pane.

For details on the uses and behaviors of this state, consult the user documentation for Release 3.4.

Node Defaults

In Release 3.4, you can override the system default values for the node and card level that exist on the ONS 15454, ONS 15454 SDH, or ONS 15327. This function is provided at the node provisioning pane level and will change the value which the node will use for the parameter setting. Many default provisioning values are now configurable. For example, you can decide whether ports on a certain type of card should default to OOS, OOS-AINS, OOS-MT, or IS when the card is pre-provisioned or inserted.

In Release 3.4 CTC there is a Defaults Editor tab accessible from the Node View > Provisioning tabs. Default values can be changed, exported, imported, and applied. Default values can also be reset to revert the defaults from the most previous “Apply” to the node. The export file is an ASCII text file, similar to the “.ctcrc” file. CTC can save and load the default overrides to or from a file.

Application of new, card level and lower defaults does not affect items already provisioned or pre-provisioned. These defaults only apply to entities created after them. Also, ONS 15327 electrical port/line-level defaults are not affected, since the ports and lines always exist (they are on the XTC).

Application of new node level defaults is an alternate way of provisioning those values. This method is made available because there is no way to apply the new values when the node is created later, since applying the values to the node requires that the node already exist. The exceptions to the node level defaults are the node.protection and node.circuits defaults, which are used only when 1+1 or BLSR protection is provisioned, or when a UPSR circuit is provisioned. Previously provisioned 1+1 or BLSR will not be affect by these changes to defaults, nor will any previously provisioned UPSR circuits.

BLSR Wizard

Release 3.4 introduces the BLSR wizard, which allows you to create, edit, and delete a BLSR from the network view of CTC. The BLSR wizard reduces common errors in creating rings from distant nodes. The wizard also facilitates creating and deleting rings over a much shorter period than it took in previous releases to individually turn up BLSR attributes on a node-by-node basis. For specific functions and limitations of the BLSR wizard, consult the user documentation for Release 3.4.

Filtering of Circuit Table

Release 3.4 adds options in the Circuit window to filter to a specific port on a card. These are in addition to the options to filter by network, node, or card level. These options will restrict the circuits listed to only those items allowed by the filter and associated with the current view.

Overhead Circuits Provisioning

Release 3.4 introduces A-Z provisioning of overhead circuits. Consult the user documentation for further details on this enhancement.

Convert Circuits to TL1 Cross Connects

Reference bug numbers: DDTS # CSCdz12915 and CSCdz15802

If you create TL1 a circuit using CTC you must select the option (in CTC) to create the circuit using TL1 commands. If you do not select this option, and the resulting circuit is later modified with TL1, then CTC will not be able to splice the circuit together and the circuit will show up as two “incomplete” circuits.

To address this issue, Release 3.4.1 (and forward) provides a new function, “Convert Circuits to TL1 Cross Connects” (accessible from the Circuits > Tools tabs in CTC). This function downgrades a selected circuit to a TL1-type circuit by changing the circuit information in the database, and can thus be used to repair TL1-modified circuits.

The function does not apply for VT Tunnels or Ethernet circuits.

TL1 Circuit Provisioning from CTC

With Release 3.4 CTC provides the ability to provision TL1 circuits. Consult the user documentation for further details on this enhancement.

SNMP Enhancements

The SNMP Agent has been modified in Release 3.4 to accommodate the new enhanced state model changes for the ONS 15454 and ONS 15327. The SNMP MIBS have been modified to accommodate the various state changes.

SNMP Agent modifications for the enhanced state model only affect one MIB variable, ifAdminStatus, which is part of the ifEntry table.

The new enhanced states and the corresponding return values for the ifAdminStatus states are outlined in Table 1.

Table 1 IfAdminStatus

Enhanced State Model	IfAdminStatus return value
IS	up(1)
OOS	down(2)
OOS_MT	testing(3)
OOS_AINS	down(2)

Note These states are also displayed in CTC when provisioning a port in or out of service.

TL1

The following TL1 features are new for release 3.4. For detailed instructions on using TL1 commands, consult the TL1 Command Guide for Release 3.4.

FTP TL1 Download Support

The new FTP TL1 download support feature allows you to download and activate system software via FTP using the TL1 interface. The following new commands support the FTP download functionality.

- APPLY
- COPY-RFILE
- REPT^EVT^FXFR

New Schedule PM Related Commands

- ALW-PMREPT-ALL
- INH-PMREPT-ALL
- RTRV-PMSCHED-ALL
- RTRV-PMSCHED-<MOD2>
- SCHED-PMREPT
- REPT^PM^<MOD2>

BLSR Enhancements (Ring Map Support)

- ENT-BLSR
- DLT-BLSR
- RTRV-<OCN_TYPE>, added support for displaying ringid and blsrtype
- ED-BLSR, allowed editing of ringid and nodeid
- EX-SW-<OCN_BLSR>

State Model Enhancement

The following features were added to TL1 to support the new state model enhancements in Release 3.4.

- ED-CRS-<STS_PATH> and ED-CRS-VT1
- Support has been added for the Secondary State (SST -> AINS,MT), in addition to the Primary State (IS,OOS). All commands related to EQPT, Facility (rr), STS, and VT now have provisioning to retrieve the SST; and commands related to Facility (rr), STS, and VT also have provisioning to set the SST.

- SOAK time is provisionable for all ports that support AINS (all but Ethernet ports). Note that TL1 soak time units are expressed in 15 minute increments.
- Facility Loopbacks are now ONLY allowed while in OOS-AINS or OOS-MT state (before facilities can be put in loopback independent of state).
- All port and circuit level maintenance activities (and their corresponding TL1-commands) are now only allowed either in OOS-AINS or OOS-MT

G1000 Support

The following commands are now supported for G1000.

- ED-G1000
- RTRV-G1000

Environmental Control and Alarms

The following features have been added to TL1 for Release 3.4 to support environmental control and alarms.

- OPR-ACO-ALL

Added support for Momentary Duration in OPR-EXT-CONT.

Autonomous Alarms

Support for autonomous alarms has been added as follows.

- All Autonomous Alarms (REPT^ALM^*), Events (REPT^EVT^*), and Autonomous CANC messages now report the fractional ATAG component.

Added Command Buffer Feature

- Maximum 20 commands can be stored in TL1 Command History
- Buffer Recall keys: ^ - to move forward, $to move backwards
- Telnet TL1 sessions are now in character mode instead of line mode. As a result TL1 users do not need to press the Enter Key to submit a TL1 command to a node. The TL1 command is processed as soon as the semicolon (;) is entered.
- TL1 Telnet Port 3082 no longer echoes

Additional TL1 Support

The following additional support has been added to TL1 for Release 3.4.

Support PDI-P Switching

Release 3.4 adds the SWPDIP parameter in ED-<STS_PATH> and RTRV-<STS_PATH>.

Additional New Commands

- RTRV-CRS (to retrieve all cross-connects on the NE)

- RTRV-MAP-NETWORK (to retrieve all DCC-Connected NEs on the Network)
- RTRV-TACC (to retrieve all Test Access Points, TAPs, on the NE)
- RTRV-USER-SECU (to retrieve all userids with their corresponding privilege levels on the NE)
- RTRV-NE-GEN, ED-NE-GEN (added get/set of IIOP port, PROTLOAD field will display "DownloadInProgress" during Software Downloads)
- REPT^EVT^COM
- REPT^EVT^ENV
- REPT^EVT^BITS
- RTRV-COND-ENV
- RTRV-PROTNSW-OCn/STSn [to determine active path determination in a 1+1 (facility)/UPSR (path) respectively]

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15327, Release 3.4.1*
- *Release Notes for the Cisco ONS 15454 SDH, Release 3.4.2*
- *Release Notes for the Cisco ONS 15454, Release 3.4.2*
- *Cisco ONS 15327 Software Upgrade Guide, Release 3.4*

Platform-Specific Documents

- *Cisco ONS 15327 User Documentation, Release 3.4*
- *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide, Release 3.4*
- *Cisco ONS 15327 Product Overview, Release 3.4*

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.