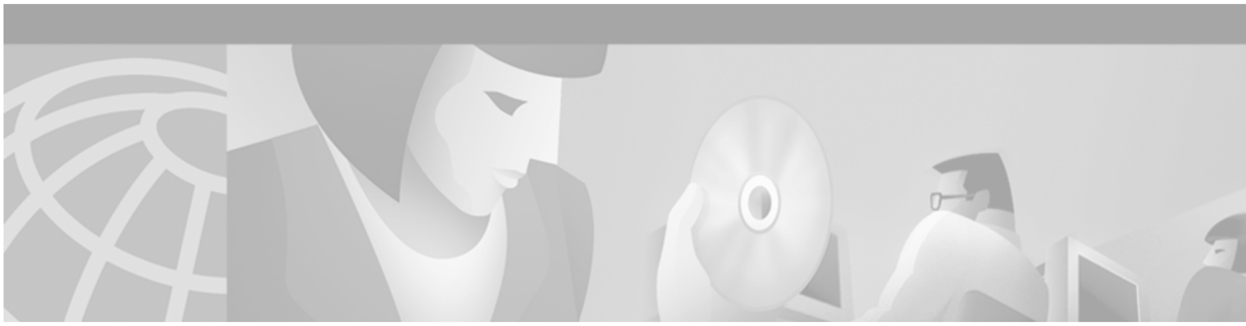

Release Notes for Cisco ONS 15454 Release 3.4.1

November, 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 3.4.1*; *Cisco ONS 15454 Reference Guide, Release 3.4*; *Cisco ONS 15454 Troubleshooting Guide, Release 3.4*; *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 15454 Release 3.4.1*, visit the following URL:

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

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

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

Contents

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15454 Release 3.4.1* since the production of the Cisco ONS 15454 System Software CD for Release 3.4.1.

The following changes have been made to the release notes for Release 3.4.1.

Changes to Caveats

The following caveats have been added to the release notes.

DDTS # CSCdz43813, page 10

Transmission Control Protocol Specification, page 10

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.

Hardware

DDTS # CSCdy15615

In some instances, the AIC-i card could reboot as a result of a 500 V DC line power surge, as defined by CISPR24/EN55024 and EN61000-6-1. This issue will be resolved in a future release.

DDTS # CSCdy00622

Very rarely, an Equipment Failure Alarm can occur on an externally timed TCC+ or TCC-I card after a reset. If this occurs, BITS will be displayed as good for one TCC, but bad for the other. If the issue occurs on the standby TCC, a second reset could clear the problem. If the issue occurs on the active TCC, the card must be replaced. This issue is under investigation.

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 # 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 3.4.1, 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.

Line Cards

DDTS # CSCdy48966

Rarely, a user requested switch on a DS3 1:1 protection group with an STS circuit going through OC-48 may undergo unexpected traffic hits. This issue will be resolved in a future release.

DDTS # CSCdy59228

OC-3 1+1 protection switch time may exceed 60 ms following a fiber pull. This issue is under investigation.

DDTS # CSCdy60775

For DS1, DS3, or DS3XM cards, when the working card is removed, traffic switches to the protect card. However, upon inserting a working card, the power on diagnostics test will be run on the card, and, if the card fails, the red FAIL LED on the front panel will remain lit, but, the protect card will start the restore timer and will switch traffic back to the working card after the timer has expired. To avoid losing traffic, remove the working card that failed the diagnostics before the protect card's restore time has expired. This issue will be resolved in a future release.

DDTS # CSCdy63760

If you place a DS3E, OC-12, STS-1 circuit in the OOS state, while the port is still IS, traffic remains. To stop the traffic, delete the circuit. This issue will be resolved in a future release.

DDTS # CSCdy47148

Traffic loss can occur when a working DS1 card is reset while the protect card is in a wait to restore state. This occurs with DS1 cards in a 1:N protection group, where traffic is running on the protect card and the protect card is in the wait to restore state. Under these conditions, resetting another active working card will result in a traffic loss while the working card is resetting. To avoid this issue, switch the traffic from the protect card to the standby working card before resetting the other working card. This issue will be resolved in a future release.

SONET and SDH Card Compatibility

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

Table 1 SDH Data Cards that are SONET Compatible

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

Table 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 # CSCdv40700

In either a DS1 or DS3 1:N protection group, deleting a standby working card from the provisioned protection group can cause a traffic hit of greater than 60 ms. Do not delete any working cards from the protection group when the protect card is active. Instead, switch traffic away from the protect card, then delete 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 the corresponding span (UPSR, BLSR, or 1+1) first, or, wait 60 seconds between cross connect switches to avoid causing signal degrade crossings for bit error rate thresholds up to 10E-9.

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 R6-57, Method 1, where to clear LOS the signal must also contain valid framing alignment patterns.

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 # CSCdx26701

Older revisions of the DS-3 card (which are no longer manufactured) may be subject to 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. This issue will not be resolved on these older cards. 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.

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.

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 (or with OC-48 cards with a revision number higher than 005D).

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, E-series traffic disruptions can exceed seven minutes. 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, traffic loss could occur if a DS-N card is preprovisioned and then added to the group while another working card in the group is removed from its slot. To avoid this, before adding slots to a protection group ensure that:

- The protect card is not actively carrying traffic (that is, the card is in standby)
- Any working slot you add to the group actually contains a working card at the time you add it

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-N12 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 # CSCdy69624

If alarms are suppressed at the port level from CTC, an incorrect CARLOSS may be reported on a E100 or E1000 card. The Incorrect CARLOSS alarm can be ignored. This issue will be resolved in a future release.

DDTS # CSCdx35561

CTC is unable to communicate with an ONS 15454 that is connected via an Ethernet craft port. CTC does, however, communicate over an SDCC link with an ONS 15454 that is Ethernet connected, yielding a slow connection. This situation occurs when multiple ONS 15454s are on a single Ethernet segment and the nodes have different values for any of the following features:

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

When any of these features are enabled, the proxy ARP service on the node is also disabled. The ONS 15454 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 15454s.

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

You can avoid waiting for the ARP entries to expire on their own by removing the SDCC links from the affected ONS 15454 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 # CSCdy37198

On Cisco ONS 15454, ONS 15454 SDH, 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 # CSCdy24967 and CSCdy21173

A G1000-4 card cannot auto-negotiate with a Catalyst 6500, CatOS Version 7.1.2, using the supervisor-1A module (8-port gig-e module). To avoid this issue, use previous version of CatOS, or use an IOS native image, or do not use flow control. This issue will be resolved in a future release of the Catalyst card and/or the G1000 card software.

DDTS # CSCdr94172

Multicast traffic can cause minimal packet loss on the E1000-2, E100-12, and E100-4 cards. Packet loss due to normal multicast control traffic should be less than 1%. This issue was resolved in Release 2.2.1 for broadcast, and in Release 2.2.2 for OSPF, and some multicast frames. As of Release 3.0.3, the ONS 15454 supports HSRP, CDP, IGMP, PVST, and EIGRP, along with the previously supported broadcast and OSPF.

Note If multicast is used for such applications as video distribution, significant loss of unicast and multicast traffic will result. These cards were not designed for, and therefore should not be used for, such applications.

Note If the multicast and flood traffic is very rare and low-rate, as occurs in most networks due to certain control protocols and occasional learning of new MAC addresses, the loss of unicast frames will be rare and likely unnoticeable.

Multicast MAC addresses used by the following control protocols have been added to the static MAC address table to guarantee no loss of unicast traffic during normal usage of these MAC addresses:

Table 0-1 Protocols Added to the MAC Address Table

Protocol	Release Protocol Introduced In
Broadcast MAC (used by many protocols)	2.2.1
Open Shortest Path First (OSPF)	2.2.2
Cisco Discovery Protocol (CDP)	2.2.2
Per-VLAN Spanning Tree (PVST)	2.2.2
Enhanced Interior Gateway Routing Protocol (EIGRP)	2.2.2
Internet Group Management Protocol (IGMP)	2.2.2
Hot Standby Routing Protocol (HSRP)	3.0.3

E1000-2/E100T

Do not use the repair circuit option with provisioned stitched Ethernet circuits.This issue is under investigation.

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.

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 # CSCdz43813

Occasionally duplicate or non-existent circuits may appear in the CTC circuits table after using the "Convert CTC Circuits to TL1 Cross Connects" tool on a set of selected circuits. To recover from this situation, restart CTC. This issue is resolved in Release 4.0.

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 # 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 # 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 # CSCdy27484

The UCP ND-FAIL alarm is not functional. This issue will be resolved in a future release.

DDTS # CSCdy55161

A hard reset of the TCC card can cause a 1+1 circuit not carrying traffic to prematurely transition from the OOS-AINS state to the IS state. To recover from this situation, place the circuit back in the OOS-AINS state. This issue will be resolved in a future release.

DDTS # CSCdy57891

An LOP-P alarm can be inadvertently cleared by an LOS that is raised and cleared. On OC48AS, OC192, and OC12-4 cards, when an LOP condition and an LOS condition are both present on the input, an LOS will be raised as per Telcordia GR 253 alarm hierarchy. However, upon clearing the LOS with the LOP still present, the LOP alarm, which should then be raised, is not. An AIS-P condition will be visible. This issue will be resolved in a future release.

DDTS # CSCdy56693

Microsoft Windows XP uses more memory than previous Microsoft operating systems, and this may result in reduced CTC performance. To avoid reduced performance, you can:

- Limit the number of nodes you log into
- Avoid or limit bulk operations
- Avoid bulk circuit deletion
- Prevent CTC’s discovery of DCC connected nodes by using the login “Disable Network Discovery” feature
- Prevent CTC’s discovery of circuits unless needed by using the login “Disable Circuit Management”

DDTS # CSCdy62092

When a node connected via SDCC has no Ethernet LAN connectivity, display of SDCC termination alarms is delayed if the fiber connecting a DCC connected node is removed. This issue cannot be resolved.

DDTS # CSCdy64663

If there is PCA traffic on a protection span and an orderwire connection passes through the working span, the orderwire connection may be lost after a protection switch. If this occurs, delete the affected orderwire circuit and recreate it after the protection switch. This issue will be resolved in Release 4.0.

DDTS # CSCdy63102

ONS 15454s reject send code requests on DS3XM ports (DS3 level). If you attempt a send code maintenance operation, CTC passes the send code operation to the NE but the NE improperly rejects it. Further, the message returned improperly indicates that the port is in an invalid state, even though it is in OOS-MT state. To work around this issue, establish the loopback directly on the remote equipment. It is not known if or when this issue will be resolved.

DDTS # CSCdy65599

DS1 VT alarms report as occurring only on port 1 regardless of which port they actually occurred on. This issue will be resolved in a future release.

DDTS # CSCdy73904

Because test access systems do not have the ability to automatically change the state of a connection, testing using intrusive modes of test access (SPLT) will fail if the circuit or connection is not already in the OOS-MT state. To avoid this issue, prior to testing the circuit or connection, ensure that its state is set to OOS-MT by changing the state using CTC or TL1. This issue will be resolved in a future release.

After testing, use CTC or TL1 to change the state from OOS-MT.

DDTS # CSCdy61275

Far end path FC-P is not counted on EC1 or OC3 cards. When a path defect is transmitted to the far end, it reports RDI-P. However, the condition is not examined and reported as a PM count. 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 # CSCdy52361

While provisioning an STS-x UCP circuit, the STS pulldown menu allows more STSs than are defined in CTC's circuit provisioning specification, or in Telcordia GR253. Do not use these extra STSs. If you do try to use one of these extra, invalid STSs, the node will reject it with an appropriate exception. This issue will be resolved in Release 4.0.

DDTS # CSCdy55556

In a 1:N protection group, where a protect card is protecting a failed card and another working card, which is missing, has a lockon condition, upon removing the lockon condition from the missing working card, the protect card may switch from the card it had been protecting to carry the traffic of the missing working card that just had the lockon removed. To avoid this issue, replace the failed working card before removing the lockon. 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 # 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 # CSCdu62591

After deleting a node from a ring, any circuits that had passed through that node show INCOMPLETE status in CTC. The deleted node is still visible to CTC, along with the reduced ring. CTC sees the cross-connects on the deleted node as being part of the pass-through circuits, but cannot connect the now-disjoint pieces of the circuit.

To correct this issue if it occurs, restart CTC so that it sees only the reduced ring nodes. Make sure the deleted node is not still visible due to other DCC links. The pass-through circuits will now have ACTIVE status.

If you need to remove the pass-through cross-connects from the deleted node, start CTC from that node with network discovery disabled. From the Circuits tab of either former trunk card, delete all INCOMPLETE circuits.

Note It is imperative that you do this from a CTC session managing only the deleted node, otherwise the circuits on the reduced ring might be deleted.

This issue will be resolved in a future release.

NE Defaults

The following caveats apply for NE defaults.

- OC12-4 allows provisioning of PJStsMon from 0 to 48. The workaround is to limit provisioning to between Off and 1 to 12 only.
- CTC displays “PJStsMon=off” in the standard provisioning pane when provisioning PJStsMon off; however, TL1 and the NE Defaults editor both display 0 for this same condition.
- If you only make changes to a single default in the NE defaults editor, you must click on another default or column before the Apply button becomes functional.

DDTS # CSCdx89312 and CSCdy52392

A sub-millisecond traffic hit can occur on DS3, DS1, E1 and E3 cards upon activation to the Release 3.4 software during an upgrade. This issue will be resolved in release 4.0.

DDTS # CSCdy36936

An existing database file could be deleted if a database backup fails. This only occurs when you choose to name the database file the same name as the existing file. In this case, CTC warns you in advance that the existing file will be overwritten. If the database backup then fails, the existing file is deleted. To prevent this issue from occurring, use a new file name for each consecutive database backup. This issue will be resolved in a future release.

DDTS # CSCdy35514

The terminology used for provisioning overhead circuits has changed in Release 3.4 as follows.

Overhead Circuit Types

- LDCC_TUNNEL has changed to DCC Tunnel D4-D12
- SDCC_TUNNEL has changed to DCC Tunnel D1-D3

Overhead Channel Types

- SDCC has changed to DCC1(D1-D3)
- LDCC_TUNNEL1 has changed to DCC2(D4-D6)
- LDCC_TUNNEL2 has changed to DCC3(D7-D9)
- LDCC_TUNNEL3 has changed to DCC4(D10-D12)
- LDCC has changed to DCC(D4-D12)

Note These circuits are now provisioned at the network level, rather than on a node-by-node basis.

DDTS # CSCdy47562

Orderwire may fail after a direct OC-12 to OC-192 upgrade. To correct this, delete the Orderwire and then add it again. This issue will be resolved in a future release.

DDTS # CSCdy48478

When you generate a lamp test, the lamps on the fan tray may fail to cycle. This issue will be resolved in a future release.

DDTS # CSCdy48494

A Maintenance Security user can provision an EXT AEP on an AIC-I card, although this user level is not expected to have this capability. This issue will be resolved in a future release.

DDTS # CSCdy01598

Rarely, there is a delay in CTC before the correct card status is displayed after a protection switch. When a manual or forced switch is made to a protection type, the protection switch occurs immediately, but the card status might take a while approximately 2 minutes to show up under rare circumstances. If a switch is not reflected right away, wait for the status change to occur. This issue is under investigation.

DDTS # CSCdy47232

F1 UDC circuits can not be terminated from an optical card in a 1+1 protection group. The circuit will be created, but it will not function. This is true regardless of whether the circuit is created first or the protection group is created first. There is no workaround; however, D4-D12 UDC circuits (over LDCC) will work correctly with 1+1 protection groups and can be used in place of F1 UDC circuits. This issue will be resolved in a future release.

DDTS # CSCdy43742

When a UDC circuit is created with no UDC traffic running yet, there is normally an LOS alarm raised to indicate the lack of UDC traffic. However, when such a circuit with no traffic running on it is present and the AIC-I card is removed and reinserted, no UDC LOS alarm is reported once the card is reinserted. To work around this issue, after reinserting the AIC-I card, delete and then recreate any UDC circuits. This issue will be resolved in Release 4.0.

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 # 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 # 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 a future release.

ONS 15454 Conducted Emissions Kit

If you are deploying the Cisco ONS 15454 within a European Union country that requires compliance with the EN300-386-TC requirements for Conducted Emissions, you must obtain and install the Cisco ONS 15454 Conducted Emissions kit (15454-EMEA-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 # 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 extremely large networks. To correct the problem, abandon the attempted circuit creation and start over. 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.

“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 # CSCdz31562

Rarely, after all spans are upgraded for a BLSR, you cannot create circuits on higher STSs. To recover from this situation, delete the ring and then recreate it. This issue is resolved in Release 4.0.

DDTS # CSCdy58058

Clearing a signal degrade on the working span with an existing signal degrade on the protect span in both directions may fail to cause a ring switch to drop.

For example, in a four-fiber BLSR, say the east side of Node 1 is connected to the west side of Node 2.

Step 1 Inject SD into the east protect span of Node 1.

Step 2 Inject SD into the west protect span of Node 2.

Step 3 Inject SD into the east working span of Node 1. A Ring switch occurs.

Step 4 Clear the SD on the east working span of Node 1. The ring switch does not drop, even after the WTR timer expires.

To recover from this situation, issue a lockout span to return traffic to the working span. This issue will be resolved in a future release.

DDTS # CSCdy59242

A fail-to-switch alarm is raised when introducing SF-R with an existing lockout span command. The alarm can become stuck after the SF-R and lockout span are cleared.

For example, 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 existing on the ring. A fail-to-Switch alarm is raised.

Step 3 Reinsert the transmit fiber. Traffic returns, but the fail-to-switch alarm is still reported.

Step 4 Clear the lockout span. The fail-to-Switch alarm becomes stuck.

To clear the alarm, ensure that the ring is in the idle state, then issue an exercise ring command on the span that reports the fail-to-Switch. This issue will be resolved in Release 4.0.

DDTS # CSCdy64543

After you issue a BLSR protection switch command with a switch type other than ring or span, TL1 cannot query any BLSR ring info.

For example, say the entered switch type is “frcdwkswbk,” so you entered:

```
opr-protnsw-oc192::fac-6-1:ff::frcd,frcdwkswbk;
```

This results in subsequent failures to query BLRS information in TL1 or CTC. CTC is unable to retrieve any BLSR information from the node, and other possible issues may arise. If at this point you close CTC, it may not launch again.

To recover from this issue, call the TAC and tell them which side you entered the incorrect command for.

DDTS # CSCdy68207

Failing the working and protect spans on a four-fiber BLSR while an extra traffic (PCA) circuit runs over the span and a lockout is on the span can cause the ET to permanently fail, with no AIS.

The failure scenario is only reproducible by failing and restoring fibers in the following sequence.

Step 1 Create a four-fiber BLSR.

Step 2 Create extra traffic circuits (one or more) over one of the spans, say, from Node A east to Node B west. At Node A, issue a lockout span east. This causes the BLSR to not switch in the event of a span failure.

Step 3 At node A, remove the working transmit fiber east, then remove the protect transmit fiber east. Both protected traffic and extra traffic are down, as expected.

Step 4 Reinsert the protect transmit fiber east, then reinsert the working transmit fiber east. Protected traffic is restored, but extra traffic is not restored.

If this issue occurs, clear the lockout span. All extra traffic is immediately restored. You may then reissue the lockout span. This issue will be resolved in Release 4.0.

DDTS # CSCdy68414

If you issue a lockout on the protection span of a BLSR where an SD preexists, traffic may remain on the SD span, even though it should switch. To recover from this situation, issue a force span on the SD-affected span, then clear the command once the switch occurs. This issue will be resolved in Release 4.0.

DDTS # CSCdy56668

Ethernet circuits may appear in the CTC circuit table with an INCOMPLETE status after a BLSR/MSSP span is upgraded. The circuits, when this occurs, are not truly incomplete. They are unaffected and continue to carry traffic. To see the circuit status correctly, restart CTC. This issue is under investigation.

DDTS # CSCdy69580

An oscillating SF-P can prevent the WTR-R timer from expiring indefinitely. If this occurs, issue a lockout span to normalize the ring. This issue will be resolved in Release 4.0.

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 # CSCdy54882

After a software upgrade from Release 3.3 to 3.4, where a Lockout Protect Span is issued on all nodes before activation (as it should be), the lockout conditions may persist even after clearing them in CTC. To correct this situation, reissue each lockout and then clear it again. This issue will be resolved in Release 4.0.

DDTS # CSCdy48872

Issuing an LK-S 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 an LK-S in the other direction (in our example, east). Since the LK-S 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 # CSCdy37654

Nodes may appear in CTC as gray and auto-ranged circuit creation may fail when CTC is connected to a large BLSR. This usually only occurs when most of the nodes in the ring are not connected to the LAN, and so, management traffic is flowing through the DCC channels.

Avoid creation of a large number of auto-ranged circuits for large BLSRs. Also try to connect more nodes to the LAN and try running OSPF on the LAN to avoid this issue. This issue will be resolved in a future release.

DDTS # CSCdy37939

In OC-12 BLSR configurations, a WKSWPR alarm that occurs can take several seconds before it appears. The workaround is to simply wait for the alarm, which should appear after a brief delay. This issue will be resolved in a future release.

DDTS # CSCdv89939 and CSCdy46597

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 # CSCdy22745

In a 2 fiber BLSR, if there is a ring or span Wait to Restore (WTR), the Clear button in CTC will clear the WTR state and revert traffic to Working right away, while the TL1 RLS-PROTNSW command does not behave in this same manner. To get the WTR to clear immediately, you must use the CTC Clear button. This issue will be resolved in Release 4.0.

DDTS # CSCdy35901

In a four-node, OC-192, four fiber BLSR, traffic remains lost after a lockout is cleared on an adjacent node when the local node has an SF-R raised. To correct this problem if it occurs, issue a force ring on the side of the SF-R affected node that the SF-R is raised on. This issue will be resolved in Release 4.0.

DDTS # CSCdy19310

Rarely, in a four-node, OC-192, four fiber BLSR, traffic can remain lost after an LOS recovery on an adjacent node when the local node has an SF-R raised. To correct this problem if it occurs, issue a force ring on the side of the SF-R affected node that the SF-R is raised on. This issue will be resolved in Release 4.0.

DDTS # CSCdy48209

Under some conditions, a lockout-of-protect span condition might be raised (or fail to clear) upon creating a BLSR. If this occurs, issue a manual switch ring command, then check to see that the ring switched properly. Afterwards, clear the command. This issue will be resolved in Release 4.0.

DDTS # CSCdy45902

Traffic that should be dropped remains unaffected when a BLSR Protection Channel Access (PCA) VT tunnel is placed OOS. You must place all circuits in the tunnel OOS before the traffic will be dropped. This issue will be resolved in a future release.

DDTS # CSCdy48538

After a 2 fiber BLSR is deleted, in some cases the PCA links remain in the Manual Routing and Circuit Edit pane. This usually occurs when there is a loss of connection between CTC and one of the BLSR nodes during deletion of the BLSR. To clear the pane, restart CTC. This issue will be resolved in Release 4.0.

DDTS # CSCdy48690

On a four-node, OC-192, four fiber BLSR, switching will not occur when an SD-R is present after clearing an SD-P. After clearing the SD-P, issue a force ring on the side of the SD-R affected node that the SD-R is reported against. This issue will be resolved in a future release.

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 ensures 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. If you do mismatch bytes at the card level, you can discover this by going to the BLSR edit map tied in with the BLSR wizard. The mismatched span will be red, and right-clicking on the span will allow you to correct the problem.

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 # 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 # 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 # CSCdy62713

If you change non-revertive UPSR VT circuits for IS to OOS and then back to IS, then fail an active fiber span carrying the circuit, the circuit will fail to switch, resulting in traffic outage. To avoid this issue, make sure the circuit is revertive before placing it in the OOS (out of service) state, and wait at least 30 seconds before changing the VT UPSR selector from one state to another. This issue will be resolved in a future release.

DDTS # CSCdx58989

Occasionally, the UPSR span upgrade wizard may fail to release a force switch on a UPSR span. It is not clear what prompts this response. If this occurs, from the Network Map, right-click on the span and invoke the “Circuits on Span” dialog box. Select Clear from “Perform UPSR span switching” combo box, then click the Apply button. This will switch all circuits back onto this span. 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.

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.

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.

DDTS # CSCdy68877

If you create STS1 and STS3C circuits through TL1 and then put the pass through cross connect in the OOS state, traffic remains, when it should stop. To work around this issue, either use CTC to place the circuit in the OOS state, or place the end cross connects in the OOS state in TL1, instead of pass through cross connect. This issue will be resolved in a future release.

DDTS # CSCdy71894

The TL1 ED-BLSR command changes the ring-id even though the command is denied because of a duplicate node-id. The following example illustrates.

Set up a BLSR (with a Ring ID of 1) with node IDs 1 and 2 (for a 2 node BLSR). On Node 1, use the ED-BLSR command to try to change the Ring ID to 2 and the Node ID to 2. Since, the Node ID is a duplicate, the command is denied. However, the Ring ID is still changed to 2. To avoid this issue, use 2 separate ED-BLSR commands to change the Node ID and Ring ID. This issue will be resolved in Release 4.0.

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 3.4.1

The following items are resolved in Release 3.4.1.

Line Cards

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 is resolved in Release 3.4.

DDTS # CSCdx03404

Following 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 preexisting 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 is resolved in Release 3.4, wherein the manual switch command is cleared upon detection of a higher priority failure, as per Telcordia GR253.

DDTS # CSCdw75823

PLM-P alarms are not raised for VT circuits terminated on DS1 or DS3XM cards. To see this, on a two-node setup, create a VT circuit inside Node 1 between a DS1 (or DS3XM) card and the optical span card to Node 2. Then in Node 2, create an STS circuit between the optical span card to Node 1 and a

DS-3 card in Node 2. Route the two circuits to the same STS on their 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 (or DS3XM) card does not. This issue is resolved in Release 3.4.

DDTS # CSCdv83422

Removing or resetting the active cross connect on a node can cause a traffic disruption on an OC-12 or DS-3E card in that node. To avoid this issue, perform a side switch on the cross connect before resetting. This issue is resolved in Release 3.4.

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 is resolved in Release 3.4.

DDTS # CSCdv49271

In a 1:1 protection group, it is possible to create a situation wherein both cards are temporarily in the active state, causing traffic loss. This can occur if you switch traffic to the protect card, lock on the protect card, reseat the working card, and then soft reset the protect card before the working slot has finished booting. Both cards will reboot simultaneously and both with come up active, and traffic will be temporarily 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 is resolved in Release 3.4.

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 is resolved in Release 3.4.

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 a second time even though no protection switch has occurred. This issue is resolved in Release 3.4.

E Series and G Series Cards

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.

This issue is resolved with a new oscillator, which is now a part of the G1000-4 hardware assembly (reference PCN # E069039). Cards with the new oscillator have an assembly (revision) number of 800-08578-02 Rev A0 or newer.

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 is resolved in Release 3.4, and in maintenance Release 3.2.1.

Maintenance and Administration

DDTS # CSCdy82224

Ports in the OOS-AINS state may transition to IS with no signal applied. This can occur when E100 or E1000 cards are present in the ONS 15454 node. This issue is resolved in Release 3.4.1.

DDTS # CSCdy79481

In DS3XM cards, ports may transition from OOS-AINS to IS with no signal applied. The transition may occur with no user interaction, but chances of occurrence are increased by resets of the DS3XM, TCC+ or cross connect cards. This issue is resolved in Release 3.4.1.

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 is resolved in Release 3.4.

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 is 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 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 not reproducible.

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 is resolved in Release 3.4.

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 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 # 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 # 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 is 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 # 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 is resolved with a new oscillator, which is now a part of the G1000-4 hardware assembly (reference PCN # E069039). Cards with the new oscillator have an assembly (revision) number of 800-08578-02 Rev A0 or newer.

DDTS # CSCct03396 Ring Map Change Dialog Box

In Releases 2.0-2.2.2 and 3.0-3.3, 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 is resolved in Release 3.4.

DDTS # CSCdt94185

CTC can fail to drop user initiated switch requests (Manual or Force) when a higher priority request is initiated. This issue can arise when a switch request is made by the user and then another, higher priority request is made. CTC should preempt the user request with the higher priority request. If CTC fails to clear the request, manually clear the request. This issue is resolved in Release 3.4.

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 is 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 is 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 is resolved in Release 3.4.

BLSR Functionality

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 is 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 is resolved in Release 3.4.

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 is resolved in Release 3.4.

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 is 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 is 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 is resolved in Release 3.4.

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 is 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 is resolved in Release 3.4.

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 is resolved in Release 3.4.

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 is resolved in Release 3.4.

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 is resolved in Release 3.4.

DDTS # CSCdw81494, CSCdw81592, CSCdw82811, CSCdv09279

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 is resolved in Release 3.4.

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 is 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 is 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 is resolved in Release 3.4.

UPSR Functionality

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 resolved in Release 3.4.

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 were made in ONS 15454 Release 3.3 that lessened the likelihood of this condition. 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 3.3. For detailed documentation of each of these features, consult the user documentation.

New Hardware

AIC-I

The Alarm Interface Controller – International (AIC-I) card expands the system management capabilities of the AIC card for the ONS 15454 SONET platform.

The AIC-I (Alarm Interface Controller – International) module is an optional card that expands systems management capabilities for customer-defined alarm I/O, user data, and orderwire functionality. This card resides in one of the common slots (Slot 9), but is not required for node operation unless the expanded AIC-I features are desired.

The AIC-I supports 8 light indicators as follows.

Table 4 AIC-I Light indicators

Light Indicator	States
FAIL light indicator	OFF when module is operating properly, RED when the module is sensed as failed, or when the card is coming up.
ACT light indicator	OFF when the module is not operational, GREEN when the module is active.
PWR light indicator (A or B feed)	GREEN when the power is within the normal range, AMBER when the power is below normal but still functional, RED when the power feed is out of range (either too low or too high).
INPUT/OUTPUT light indicators	INPUT light is OFF when there is no input alarm raised, YELLOW when an alarm exists. OUTPUT light is OFF when no external controls have been triggered, YELLOW when one has.
RING light indicators (one for LOW and one for EOW)	OFF when no call is present on the orderwire, GREEN Flashing when a call is received.

AIC-I Features

Table 5 lists the available ANSI support for AIC-I card features.

Table 5 AIC-I Feature Support

AIC-I Feature	Support in ANSI
Input/Output alarm contact support	4 I/O
Input only contact support	12-Input
F1 64K User Data Channel	Yes
D4-D12 576K Data Communication Channel	Yes
A-Law support	Yes
Mu-Law support	Yes

Table 5 AIC-I Feature Support

AIC-I Feature	Support in ANSI
Selective station calling	Yes
Interoperability with existing AIC	Yes

Input and Input/Output Alarm Contacts Support

The AIC-I card provides additional input/output alarm contact closures for customer use: up to 12 user-defined input, and 4 user-defined input/output contacts. The 4 input/output contacts are provisionable either as all inputs or all outputs. They default to input contacts.The alarms are user-definable via CTC. An LED for inputs and another for outputs are included on the front panel to indicate the overall status of the alarm contacts.. Input alarms are typically used for external sensors like open doors, temperature sensors, flood sensors and other environmental conditions. Output contacts are typically used to drive visual or audible devices like bells, lights, pagers, or even to control generators, heaters, fans, etc.

All of the contacts (input and input/output) can be programmed separately via the AIC-I card view Provisioning tab.

F1 User Data Channel (F-UDC)

The user data channel allows the local user to physically connect a dedicated data channel of 64 Kbps (F1 byte in SOH) between two nodes in a 15454 network. Each AIC-I supports two F-UDCs, and each UDC can be routed to a unique and separate optical interface on the ONS 15454 system. The F1 UDC is a 64 Kbps point-to-point channel and is routed between optical interfaces via the TCC/TCC+ module in intermediate locations. Provisioning of a UDC function is accomplished via the Overhead Circuits tab within the Provisioning tab in the Network view.

D4-D12 Data Communication Channel (DCC)

The DCC utilizes the line data communication channel and allows you to physically connect a dedicated data channel of 576 Kbps (D4-D12 bytes in Section/Line Overhead) between two nodes in an ONS 15454 network. Each AIC-I supports two DCCs, and each DCC can be routed to an individual and separate optical interface on the ONS 15454. The DCC is a 576 Kbps channel and is routed between optical interfaces via the TCC/TCC+ modules in intermediate locations. Provisioning of a DCC function is accomplished via the Overhead Circuits tab within the Provisioning tab in the Network view.

Orderwire Functionality

Orderwire provides a craftsperson the ability to plug a standard phone set into an ONS 15454 and communicate with one or more other craftspeople working at other ONS 15454s. The orderwire is a PCM-encoded voice channel that rides on bytes E1 or E2 in the section and line overhead. The orderwire interface on the AIC-I supports both 4-wire and 2-wire connection via an RJ-11 jack.

The AIC-I allows simultaneous use of both local (SONET Section overhead) and express (SONET Line overhead) orderwire channels on a SONET ring or a particular optics facility.

Provisioning of an orderwire function is accomplished via the Overhead Circuits tab within the Provisioning tab in the Network view. Both of the EOW and LOW channels can also be adjusted via the AIC-I card view.

Note The OC3/STM-1 card does not support the express orderwire channel.

AEP Support

The Alarm Expansion Panel (AEP) provides the ability to expand the number of alarms supported by the AIC-I to 32 input contacts and 16 output contacts. The AEP is only provided for the ANSI chassis. The AEP daughter card mounts to the lower rear of the chassis and connects to the wire wrap pins on the shelf backplane. It must be enabled via the Provisioning tab in the AIC-I card view. The AEP is provided as an expansion unit and is non-mandatory for system operation.

The AEP connects with the ANSI shelf using the wire wrap pins on the shelf backplane and communicates with the AIC-I via the P1 connector on the AEP board. AEP support is enabled via the Card tab in the AIC-I card view.

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.x 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.x, 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.x, 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.x 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.x, 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.

UCP

Unified Control Plane (UCP) is a modular software feature set that provides functions that increase networking control capabilities in the areas of routing, signaling, and provisioning. UCP also provides resource and service discovery. In past releases, provisioning was a manual process requiring users of management systems to set up multiple segments in an end-to-end circuit configuration. UCP was developed to automate end-to-end optical network provisioning, with the addition of mesh restoration capability and drive intelligence within nodes.

UCP O-UNI (Optical User Network Interface) is a well-defined set of protocols used for signaling and routing between a service provider network and equipment in a client network based on an emerging standard. The UNI 1.0 specification describes the set of services, interfaces, and signaling capabilities.

In the ONS 15454 O-UNI 1.0 implementation, services are used to invoke:

- Connection creation
- Connection deletion
- Connection status inquiry
- Autonomous connection status change notification update

Note Connection modification is not supported in this release.

Clients request services of the optical network using O-UNI signaling. UNI signaling agents (that is, client side agents), referred to as O-UNI-C, make requests of network side agents (O-UNI-N) using O-UNI signaling messages. These messages are transported over an IP control channel “in band” (IB) or “out of band” (OB) using RSVP-TE.

O-UNI-C provides signaling termination functionality. O-UNI-N provides signaling pass-through and inter-working functionality, circuit routing, and reachability information to O-UNI-C. O-UNI-C is implemented in Release 3.4.x. O-UNI-N will be implemented in a future release.

Protection Channel Access

In compliance with Telcordia GR-1230-CORE, section 3.4, protection channel access (PCA) is supported with the ONS 15454 Release 3.4.x. Normal BLSR utilizes only 50% of ring bandwidth, while the other 50% remains idle until a ring or span switch occurs. PCA circuits can run through the idle bandwidth. These circuits will be preempted when a switch occurs, making room for protected circuits. PCA circuits are provisionable on the protection channels of 2, or 4 fiber BLSR configurations. PCA circuits are restored after the wait-to-restore timer times out following a switch. This feature allows service providers to utilize their networks more efficiently.

Circuit routing preferences for Release 3.4.x are enhanced to support PCA circuit creation. Circuit routing preferences can be viewed as being divided into primary and secondary preferences. The primary routing preference (PRP) determines if the entire path is protected (fully protected path) or unprotected. The PRP is set when the circuit is created via CTC and cannot be changed. The Secondary Routing Preference (SRP) depends on the PRP and is also set when the circuit is created via CTC.

Table 6 Routing Preferences

Primary Routing Preference (PRP)	Secondary Routing Preference (SRP)
Protected (fully protected path)	Node Diverse Required, Node Diverse Desired, Link Diverse
Unprotected	PCA enabled/disabled

For details on provisioning PCA, consult the user documentation for Release 3.4.

Enhanced State Model

The Release 3.4.x 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.x, 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.x 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.

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.x 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.x 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.x 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 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.x 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.x 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 7.

Table 7 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.x. 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-<MOD2>
- 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>

New UCP Related Commands

The following commands were added to support UCP in Release 3.4.x.

- DLT-UCP-CC
- DLT-UCP-IF
- DLT-UCP-NBR
- ED-UCP-CC
- ED-UCP-IF
- ED-UCP-NBR
- ED-UCP-NODE
- ENT-UCP-CC
- ENT-UCP-IF
- ENT-UCP-NBR
- RTRV-ALM-UCP
- RTRV-COND-UCP
- RTRV-UCP-CC

- RTRV-UCP-IF
- RTRV-UCP-NBR
- RTRV-UCP-NODE
- REPT^ALM^UCP
- REPT^EVT^UCP

State Model Enhancement

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

- 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

Environmental Control and Alarms

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

- OPR-ACO-ALL

Added support for AICI Card and its 16 Provisionable Contacts. Supported commands include:

- OPR-EXT-CONT, RLS-EXT-CONT, RTRV-ATTR-CONT,RTRV-EXT-CONT, SET-ATTR-CONT
- REPT^ALM^ENV, REPT^EVT^ENV, RTRV-ALM-ENV, RTRV-ATTR-ENV, RTRV-COND-ENV, SET-ATTR-ENV

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.x.

Support PDI-P Switching

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

Support for Protection Channel Access

Release 3.4.x adds the following protection channel access (PCA) support.

- New Cross-Connect Types: 1WAYPCA and 2WAYPCA
- Creation (ENT-CRS-<STS_PATH> and ENT-CRS-VT1), Deletion (DLT-CRS-<STS_PATH> and DLT-CRS-VT1), and Retrieval of PCA Cross-connects
- Test Access support on PCA

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]

TL1 Syntax Changes

Command Changes

In the following sections, each Release 3.3 command is listed first, with the corresponding Release 3.4.x command listed second.

ED-G1000 changed:

```
ED-G1000[:<TID>]:<aid>:<CTAG>[:::MFS=<mfs>,][FLOW=<flow>][:<pst>];
```

```
ED-G1000[:<TID>]:<aid>:<CTAG>[:::MFS=<mfs>,][FLOW=<flow>,][SOAK=<soak>][:<pst>,][<sst>];
```

ED-<OCN_TYPE> changed:

```
ED-<OCN_TYPE>:[<TID>]:<aid>:<CTAG>:::[DCC=<dcc>,][SYNCMSG=<syncmsg>,][SENDDUS=<senddus>,][PJMON=<pjmon>,][SFBER=<sfber>,][SDBER=<sdber>,][MODE=<mode>,][MUX=<mux>][:<pst>];
```

```
ED-<OCN_TYPE>:[TID]:<aid>:<CTAG>:::[DCC=<dcc>],[SYNCMSG=<syncmsg>],[SENDDUS=<senddus>],[PJMON=<pjmon>],[SFBER=<sfber>],[SDBER=<sdber>],[MODE=<mode>],[MUX=<mux>],[SOAK=<soak>]:[<pst>],[<sst>];
```

ED-<STS_TYPE> changed:

```
ED-<STS_TYPE>[:<TID>]:<aid>:<CTAG>[:::SFBER=<sfber>,][SDBER=<sdber>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][EXPTRC=<exptrc>,][TRC=<trc>,][TRCMODE=<trcmode>,][TACC=<tacc>][:];
```

```
ED-<STS_TYPE>[:<TID>]:<aid>:<CTAG>[:::SFBER=<sfber>,][SDBER=<sdber>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][SWPDIP=<swpdip>,][EXPTRC=<exptrc>,][TRC=<trc>,][TRCMODE=<trcmode>,][TACC=<tacc>]:[<pst>],[<sst>];
```

ED-T1 changed:

```
ED-T1[:<TID>]:<aid>:<CTAG>[:::LINECDE=<linecde>,][FMT=<fmt>,][LBO=<lbo>,][TACC=<tacc>][:<pst>];
```

```
ED-T1[:<TID>]:<aid>:<CTAG>[:::LINECDE=<linecde>,][FMT=<fmt>,][LBO=<lbo>,][TACC=<tacc>,][SOAK=<soak>][:<pst>,][<sst>];
```

ED-T3 changed:

```
ED-T3[:<TID>]:<aid>:<CTAG>[:::FMT=<fmt>,][LINECDE=<linecde>,][LBO=<lbo>,][TACC=<tacc>][:<pst>];
```

```
ED-T3[:<TID>]:<aid>:<CTAG>[:::FMT=<fmt>,][LINECDE=<linecde>,][LBO=<lbo>,][TACC=<tacc>,][SOAK=<soak>][:<pst>,][<sst>];
```

ED-VT1 changed:

```
ED-VT1[:<TID>]:<aid>:<CTAG>[:::RVRTV=<rvrtv>,][RVTM=<rvtm>,][TACC=<tacc>];
```

```
ED-VT1[:<TID>]:<aid>:<CTAG>[:::RVRTV=<rvrtv>,][RVTM=<rvtm>,][TACC=<tacc>]:[<pst>],[<sst>];
```

ENT-CRS-<STS_TYPE> changed:

```
ENT-CRS-<STS_TYPE>[:<TID>]:<from>,<to>:<CTAG>[::<cct>][::];
```

```
ENT-CRS-<STS_TYPE>[:<TID>]:<from>,<to>:<CTAG>[::<cct>]::[<pst>],[<sst>];
```

ENT-CRS-VT1 changed:

```
ENT-CRS-VT1[:<TID>]:<from>,<to>:<CTAG>[::<cct>][::];
```

```
ENT-CRS-VT1[:<TID>]:<from>,<to>:<CTAG>[::<cct>]::[<pst>],[<sst>];
```

RMV-EC1 changed:

```
RMV-EC1[:<TID>]:<aid>:<CTAG>[::,];
```

```
RMV-EC1[:<TID>]:<aid>:<CTAG>[::<cmdMode>,][<pst>,][<sst>];
```

RMV-<MOD_PORT> changed:

```
RMV-<MOD_PORT>[:<TID>]:<aid>:<CTAG>[::,];
```

```
RMV-<MOD2_IO>[:<TID>]:<aid>:<CTAG>::[<cmdMode>],[<pst>],[<sst>];
```

Note The MOD_PORT command in Release 3.3 includes EC1, G1000, OC12, OC192, OC3, OC48, T1, and T3. The new MOD2_IO command in Release 3.4.x includes DS1, EC1, G1000, OC12, OC192, OC3, OC48, T1, and T3.

ED-NE-GEN changed:

ED-NE-GEN[:<TID>]::<CTAG>[:::NAME=<name>,][IPADDR=<ipaddr>,][IPMASK=<ipmask>,][DEFRTR=<defrtr>,][NTP=<ntp>];

ED-NE-GEN[:<TID>]::<CTAG>[:::NAME=<name>,][IPADDR=<ipaddr>,][IPMASK=<ipmask>,][DEFRTR=<defrtr>,][IIOPPORT=<iiopport>,][NTP=<ntp>];

OPR-SYNCNSW changed:

OPR-SYNCNSW[:<TID>][:<aid>]:<CTAG>::<switchto>;

OPR-SYNCNSW[:<TID>][:<aid>]:<CTAG>::<syncsw>,[<sc>];

Response Changes of TL1 Commands

In following section, each Release 3.3 response is listed first, with the Release 3.4.x response listed second:

Response to RTRV-CRS-STSn changed:

“<from>,<to>:<cct>,<level>”

“<from>,<to>:<cct>,<mod>::<pst>,[<sst>]”

Response to RTRV-CRS-VT1 changed:

“<from>,<to>:<cct>”

“<from>,<to>:<cct>::<pst>,[<sst>]”

Response to RTRV-EC1 changed:

“<aid>::[PJMON=<pjmon>,][LBO=<lbo>,][RXEQUAL=<rxequal>]:[<pst>]”

“<aid>::[PJMON=<pjmon>,][LBO=<lbo>,][RXEQUAL=<rxequal>,][SOAK=<soak>]:<pst>,[<sst>]”

Response to RTRV-EQPT changed:

“<aid>:<aidtype>,<equip>,[<role>],[<status>]:[PROTID=<protid>,][PRTYPE=<prtype>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][CARDNAME=<cardname>]:[<pst>]”

“<aid>:<aidtype>,<equip>,[<role>],[<status>]:[PROTID=<protid>,][PRTYPE=<prtype>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][CARDNAME=<cardname>]:[<pst>],[<sst>]”

Response to RTRV-G1000 changed:

“aid>::[MFS=<mfs>,][FLOW=<flow>,][LAN=<lan>,][OPTICS=<optics>]:[<pst>]”

“<aid>::[MFS=<mfs>,][FLOW=<flow>,][LAN=<lan>,][OPTICS=<optics>]:<pst>,[<sst>]”

Response to RTRV-T1 changed:

“<aid>::[LINECDE=<linecde>,][FMT=<fmt>,][LBO=<lbo>,][TACC=<tacc>]:[<pst>]”

“<aid>::[LINECDE=<linecde>,][FMT=<fmt>,][LBO=<lbo>,][TACC=<tap>,][SOAK=<soak>]:<pst>,[<sst>]”

Response to RTRV-T3 changed:

“<aid>::[FMT=<fmt>,][LINECDE=<linecde>,][LBO=<lbo>,][TACC=<tacc>]:[<pst>]”

"<aid>::[FMT=<fmt>,][LINECDE=<linecde>,][LBO=<lbo>,][TACC=<tap>,][SOAK=<soak>]:<pst>,[<sst>]"

Response to RTRV-VT1 changed:

"<aid>::[RVRTV=<rvrtv>,][RVTM=<rvtm>,][TACC=<tacc>]"

"<aid>::[RVRTV=<rvrtv>,][RVTM=<rvtm>,][TACC=<tacc>]:[<pst>],[<sst>]"

Response to RTRV-NE-GEN changed:

"[IPADDR=<ipaddr>,][IPMASK=<ipmask>,][DEFRTR=<defrtr>,][NTP=<ntp>,][NAME=<name>,][SWVER=<swver>,][LOAD=<load>]"

"[IPADDR=<ipaddr>,][IPMASK=<ipmask>,][DEFRTR=<defrtr>,][IIOPPORT=<iiopport>,][NTP=<ntp>,][NAME=<name>,][SWVER=<swver>,][LOAD=<load>,][PROTSWVER=<protswver>,][PROTLOAD=<protload>,][DEFDESC=<defdesc>]"

Response to RTRV-SYNCN changed:

"<aid>:<ref>,<refval>,[<qref>],[<status>]"

"<aid>:<ref>,<refval>,[<qref>],[<status>],[<protectstatus>]"

ENUM Value Changes

The following parameter values for the associated enumerated types have been added in Release 3.4.x.

Related to EX-SW-OCN-BLSR / OPT-PROTNSW-<MOD2> / OPR-SYNCNSW / RTRV-PROTNSW-<MOD2>

- Multiple SWITCH items added. Multiple SWITCH_TYPE items added
- New SWITCH types values are "APS_CLEAR," "CLEAR," and "EXERCISE"
- New SWITCH_TYPE values are "FRCDWKSWBK," "FRCDWKSWPR," "LOCKOUTOFWK," "MANWKSWBK," "MANWKSWPR," and "LOCKOUTOFPR"

Related to RTRV-EXT-CONT / OPR-EXT-CONT

- "CONTS" added a DURATION

Related to RTRV-PMSCHED-ALL / RTRV-PMSCHED-MOD2

- "ALW" added as an INH-MODE

Related to Enhanced State Model

- "AINS" and "MT" added as SST, multiple old unused values dropped.

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15454, Release 3.3*
- *Release Notes for the Cisco ONS 15454 SDH, Release 3.4*
- *Release Notes for the Cisco ONS 15327, Release 3.4*
- *Release Notes for the Cisco ONS 15454, Release 3.4*
- *Cisco ONS 15454 Software Upgrade Guide, Release 3.4*

Platform-Specific Documents

- *Cisco ONS 15454 Procedure Guide, Release 3.4.1*
- *Cisco ONS 15454 Reference Guide, Release 3.4*
- *Cisco ONS 15454 Troubleshooting Guide, Release 3.4*
- *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide, Release 3.4*
- *Cisco ONS 15454 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.