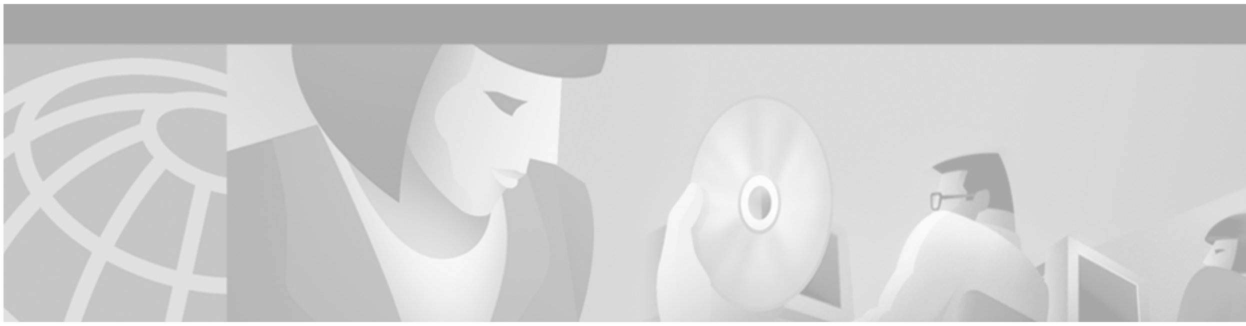


Release Notes for Cisco ONS 15454 Release 3.0.3

Release Notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15454 SONET multiplexer. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to Release 3.0. of the *Cisco ONS 15454 Installation and Operations Guide, Cisco ONS 15454 Troubleshooting and Reference Guide*, and *Cisco ONS 15454 TL1 Command Guide.* For the most current version of the Release Notes for Cisco ONS 15454 Release 3.0.3, visit the following URL:

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

Contents

This document contains the following sections:

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

November 2001

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15454 Release 3.0.3* since the production of the Cisco ONS 15454 System Software CD for Release 3.0.3.

The following supplemental changes have been added to the release notes for Release 3.0.3.

Changes to the Caveats

The following caveats have been added.

DDTS # CSCdv14523 IMPROPRMVL Alarm does not Clear, page 15

DDTS# CSCdu50983 Manual Protection Switch does not Clear After a Higher Priority Switch, page 15

DDTS # CSCdw45877, page 17

TCC Software Synchronization, page 18

DDTS # CSCdw16886, page 18

DDTS # CSCdv66003, page 20

DDTS # CSCdv72286, page 20

DDTS # CSCdv72434, page 20

DDTS # CSCdw06182, page 19

DDTS # CSCdv72264, page 19

DDTS # CSCdv72457, page 19

DDTS # CSCdv83675, page 19

DDTS # CSCdv64833, page 19

DDTS # CSCdv77176, page 19

DDTS # CSCdv72317, page 19

DDTS # CSCdv81254, page 20

Span Upgrade, page 20

DDTS# CSCdu28367, page 24

DDTS # CSCdu29530, page 26

DDTS # CSCdt79962, page 27

DDTS # CSCdv83748, page 27

DDTS # CSCdv46667, page 27

DDTS # CSCdw01019, CSCdv21120, and CSCdu89221, page 28

DDTS # CSCdw01054, page 28

DDTS # CSCdv76001, page 28

DS1 Electrical Transmit Path PMs, page 25

DDTS # CSCdv73802 and CSCdv74996 Far End PM Monitoring, page 25

DDTS # CSCct03396 Ring Map Change Dialog Box, page 27

DDTS # CSCdw02830, page 27

Release Notes Caveat Closed, page 29

DDTS # CSCdv74990, page 31

DDTS # CSCdv76146, page 31

DDTS # CSCdv86514, page 31

The following caveat has changed in the release notes; the caveat was enhanced to provide more information:

DDTS # CSCdr94172, page 16

Changes to the Maintenance Issues Closed in Release 3.0.3

The following closed items have been added.

DDTS # CSCdu06367 Traffic Disruption on BLSR Protection Switch, page 12

DDTS # CSCdv73379, page 12

The following item has been removed from this section and returned to the caveats section.

DDTS # CSCdv14523 IMPROPRMVL Alarm does not Clear, page 15

Changes to New Features and Functionality

The following has been added to the new features and functionality for TL1:

CTAGs, page 46

The following has been updated in New Features and Functionality to more accurately depict the functionality of the ONS 15454:

CTC Platforms, page 39

Maintenance Issues Closed in Release 3.0.3

Upgrades

DDTS # CSCdu38992

Cisco recommends Release 3.0.0 for new system installations (or what is commonly termed "Greenfield applications") only.

When you upgrade from ONS 15454 Release 2.2.x to 3.0.0, a condition may arise that can cause a post-upgrade reset of the node at a point after the upgrade process after you perform a provisioning change on the node. During testing, this condition was experienced in less than 2% of the systems upgraded. This condition will not be seen on new, or "Greenfield," systems initialized with Release 3.0.0.

As the node activates the new software load, each card in the node is loaded with the new software release. If any one of the cards fails to load the software successfully, you may see a communication failure (CONTBUS) condition that persists after the activation is completed indicating the node has entered this state. Once the node is in this state, any provisioning changes will cause the node to go into a system-wide reset wherein all cards perform a soft reboot and reload the new software image (except for the card that failed to reset originally; this card must be either reseated or replaced). If the node falls into this condition, traffic may be affected on provisioned circuits.

If you choose to upgrade nodes to Release 3.0.0, perform the upgrade within a maintenance window. To ensure that your upgrade activation has succeeded, Cisco recommends that you execute a provisioning change to the node by toggling the timing reference (waiting one minute between toggles), thus setting a 30-minute timer in motion and allowing the node reset to occur during the maintenance window, or while personnel are on site. If the node does not reset 30 minutes after the provisioning change and no SYSBOOT alarm is present in the CTC alarms panel for the node, the software activation was successful. For details on this procedure, see “Upgrading Cisco ONS 15454 Release 2.2.x to 3.0.0 Using the TCC+ Card.”

This issue is resolved in Release 3.0.1.

DDTS # CSCdu35824

After an upgrade from Release 2.2.x to 3.0, pointer justification thresholds are incorrect. They can be zero or a number that is too large. Incorrect pointer justification thresholds occur with OC-3, OC-12, OC-48, and EC-1 cards. This issue will not occur for new OC-N cards inserted after an upgrade.

This issue is resolved in Release 3.0.1.

DDTS # CSCdu20446

In previous releases, a CTC I/O exception could occur during an activation to a new software load.

This issue is resolved in Release 3.0.1.

Traffic Protection

False UNEQ-P Alarms

In previous releases, false unequipped path (UNEQ-P) alarms might have occurred during protection switching between cards.

This issue is resolved in Release 3.0.

Traffic Loss When Resetting an Electrical Card While in Lock on

In previous releases, if you placed a working card from an electrical protection group in the “Lock on” state and performed a soft reset of the card, you would lose traffic until the working card became active.

This issue is resolved in Release 3.0.

Line Cards

DDTS # CSCdv12685

DS-1 and OC-3 threshold crossing alarm (TCA) events do not report the correct port number in the History tab. When you put a DS-1 or OC-3 port in service, the History tab displays an LOS alarm with the correct port number. After the UASP threshold crossing (10 seconds), the TCA reports are displayed with an incorrect port number.

This issue is resolved in Release 3.0.3.

DDTS # CSCdv53765

In DS-1, DS-3, or DS-3XM 1:1 protection switching, service can fail after a force switch to protection has been performed and subsequently the protect card is soft reset. Should a loss of service occur, service will not return until the protect card finishes rebooting and becomes active.

This issue is resolved in Release 3.0.3.

DDTS # CSCdv40582

Adding or removing a DS-1 card in a DS-1 1:N protection group can cause permanent loss of existing traffic.

This issue is resolved in Release 3.0.3.

DDTS # CSCdv33569

ONS 15454 DS-3N cards might not maintain alarm reports consistently when a card has facility loopbacks provisioned to it and is used in a DS-3 1:N protection group. With DS-3 1:N protection, the Facility Loopback alarm on the protect card clears when the protect card becomes active.

This issue is resolved in Release 3.0.3.

DDTS # CSCdu30706 and CSCdu30624

Occasionally when a two fiber BLSR carrying STS-Nc traffic does a protection switch, a traffic disruption of greater than 50 ms can occur for the STS-Nc traffic.

This issue is resolved in Release 3.0.3.

DDTS # CSCdu36139

In previous releases, traffic hits or loss could occur after deleting an adjacent drop card. A payload bus alarm accompanies the service-affecting incident. This issue has occurred with the EC-1 card.

This issue is resolved in Release 3.0.1.

DDTS # CSCdu34969

Removing the active TCC+ can cause a communication bus failure (CONTBUS) alarm.

This issue is resolved in Release 3.0.1.

False Card Failure Alarms

In previous releases, false card-failure alarms could appear during hard resets (card pulls) of active XCVT cards.

This issue is resolved in Release 3.0.

DDTS # CSCct03114

In previous releases, SONET section data communication channel (SDCC) was only supported on Ports 1 and 3 of the four-port OC-3 card.

This issue is resolved in Release 3.0.

E-Series Cards

DDTS # CSCdv20345

In previous releases, under excessive multicast and unicast traffic, you might have seen an Ethernet carrier loss that could last for several seconds. This carrier loss would characteristically only decrease if multicast traffic decreased. This issue is resolved in Release 3.0.3

DDTS # CSCdv33422

When using an E1000 card, multicast HSRP packets can cause unicast frames to drop.

This issue is resolved in Release 3.0.3. With Release 3.0.3, the ONS 15454 now supports HSRP, CDP, IGMP, PVST, EIGRP, and ISIS, along with the previously supported broadcast and OSPF.

DDTS # CSCdv63885

In certain rare configurations, deleting multiple circuits at once can cause E1000 cards reboot.

This issue is resolved in Release 3.0.3.

DDTS # CSCds68558

In rare cases, an Ethernet circuit might fail to go into a forwarding state. If this occurs, the card will not carry traffic until the TCC is reset.

This issue is resolved in Release 3.0.3.

SNMP

DDTS # CSCdv36186

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

This issue is resolved in Release 3.0.3.

DDTS # CSCdv62307

In previous Releases, all the versions of the SNMP agent allow access to the IP routing table if the SNMP request is made with a general purpose word as community name. With Release 3.0.3, access to basic MIB-II objects can only occur if the community name matches completely with one of the community names in the CTC:provisioning:SNMP panel.

This issue is resolved in Release 3.0.3.

Maintenance and Administration

DDTS # CSCdu64439

If two nodes fail at acquiring a valid MAC address and both are subsequently assigned the same default MAC address, 00-10-cf-ff-ff-ff, a broadcast storm can ensue.

This issue is resolved in Release 3.0.3.

DDTS # CSCdv64824

If a 1+1 protection group is created using a line that currently has VT circuits or VT Tunnel terminations on it, attempts to create more VT circuits on same STS as pre-existing VT circuits or on pre-existing

VT Tunnel terminations will fail. Attempts to create VT circuits on STSs that were not previously VT-mapped will succeed. The workaround is to delete the VT circuits and VT Tunnels prior to creating the 1+1. Alternatively, you can wait until you need to add more VT circuits to an STS and then delete any VT circuits on the STS that you want to add new VT circuits to.

This issue is resolved in Release 3.0.3.

DDTS # CSCdv58534

Linear automatic protection switch times may exceed 50 ms.

This issue is resolved in Release 3.0.3.

DDTS # CSCdv55792

You must reset the active TCC+ on any node for which the MEM-LOW or MEM-GONE alarm is raised. This issue is resolved in Release 3.0.3.

DDTS # CSCdv53496

The performance of a TCC+ card can decrease after a large number of auto-range circuits are created. This issue is resolved in Release 3.0.3.

DDTS # CSCdv50493

You must not attempt to provision a node while the standby TCC+ is in the process of initializing its software. Any provisioning done in this time frame may be lost.

This issue is resolved in Release 3.0.3.

DDTS # CSCdv38817

When resetting the active TCC+ from CTC during a database transfer, occasionally, the standby TCC+ could fail to take over and become active. In this case, the active TCC+ reboots, and then becomes active again. During the time it takes for the TCC+ card to reboot and become active, there is no active TCC+ card for the line cards to communicate with or to derive timing from.

This issue is resolved in Release 3.0.3.

DDTS # CSCdv49672

In CTC, when standby OC-3 ports in a 1+1 protection group are switched to active, the hash marks (#) that indicate that the ports are standby remain on the graphic until the user forces a screen refresh; for example, by moving the mouse over the graphic. In general, no protection group-related changes are reflected in the port graphic until the screen refreshes.

This issue is resolved in Release 3.0.3.

DDTS # CSCdv24546

An override, revertive switch can cause a traffic loss in a 1:N DS1 protection group.

This issue is resolved in Release 3.0.3.

DDTS # CSCdu06369

CTC may display a node selection error when you attempt to create a circuit if a participating node is temporarily disconnected. This can occur when, in the circuit creation dialog box, the first node in the list is pre-selected. If the first node is disconnected, CTC will display an error message. You can recover from this condition by closing the error dialog, then selecting another node in the list.

This issue is resolved in Release 3.0.3.

DDTS # CSCdv46209

An attempted database backup can fail, generating an error message. When the backup fails, a file will be generated but will contain no data (byte size is zero). This issue has been seen when two database backups for the same node were attempted at the same time. Cisco recommends that you check the file size of database backups to ensure that they contain data, especially if any errors were encountered during the backup.

This issue is resolved in Release 3.0.3.

DDTS # CSCdu40207

A TCC+ reset can cause active alarms to clear prematurely. If your TCC+ resets, you must reset any alarmed cards afterwards if you wish to restore their current alarm conditions.

This issue is resolved in Release 3.0.3.

DDTS # CSCdu27989

When a network has too many concurrent CTC sessions open, CTC can subsequently open too many file handles, resulting in an unexpected TCC reset. To avoid this issue, restrict the number of CTC sessions to a maximum of four.

This issue is resolved in all Releases 3.0.x, which allow a user to log in with “Exclude Dynamically Discovered Nodes” enabled. This opens a node level view rather than the typical network level view, limiting the number of open file handles on the local node. Releases 3.0 and forward also optimize the number of file handles opened during initialization.

DDTS # CSCdt86355, CSCdv14052

Previous releases of CTC were capable of losing synchronized status between CTC and an ONS 15454 node. Symptoms indicating that this issue has arisen might be inaccurate card status, false alarms, or other misinformation reported by CTC. To resolve this issue, reset the TCC+ card, then immediately close the CTC session. A new CTC session should show the correct status for the node.

This issue is resolved in Release 3.0.2.

DDTS # CSCdu28401

In previous releases, false AIS-V and UNEQ-V alarms could be raised on the trunk cards for some VT circuits. Traffic remained error-free. This issue could occur in a BLSR after node isolation, or in other protection mechanisms (UPSR, 1+1) if multiple switches occurred in rapid succession. The false alarms could also be raised if a VT circuit was deleted while it was alarmed. The alarm condition will not clear on its own. To clear the alarms you must force a switch from the active TCC+ to the standby TCC+. This will force an alarm resynchronization and clear the erroneous alarms.

This issue is resolved in Release 3.0.2.

DDTS # CSCdu26570

In previous releases, if you selected multiple circuits in two concurrently running CTC sessions and then deleted the circuits simultaneously, the TCC+ might have reset. This occurred when two CTC sessions were connected to the same node and STS or VT circuits were set up on the node.

This issue is resolved in Release 3.0.2.

DDTS # CSCdv22380: CORBA Communication Exception

In previous releases, if CTM was connected to an ONS 15454 network (or node) for a prolonged period (48 hours +), the connection could fail with a “Corba:comm.” failure error. Once the connection is lost, it will not return. The workaround was to restart the client software.

This issue is resolved in Release 3.0.2.

DDTS # CSCdu53428

Normally you can connect a workstation directly to an ONS 15454 node and then provision a static route on the workstation, run CTC, and view the entire DCC network; however, in Release 3.0, if another node in the network is connected to a LAN while OSPF is turned on for that LAN, some nodes in the network might not be visible from the CTC session on the workstation.

This issue is resolved in Release 3.0.1.

DDTS # CSCdu55720

In Release 3.0 default static routes do not propagate from a single node to the entire network. To propagate to all nodes you must use a network or host route.

This issue is resolved in Release 3.0.1.

LOS on DS-1 Protect Card Reported as Minor, Non-Service Affecting After Switch

In previous releases, after a switch from the working to the protect DS-1 card, the loss of signal (LOS) alarm for the protect card (the new working card) might have been reported as having a minor, non-service affecting (MN NSA) severity instead of a major, service affecting (MJ SA) severity.

This issue is resolved in Release 3.0.

DDTS # CSCdt14510

In previous releases, DS3XM/DS-1 traffic might have been interrupted during software activations .

This issue is resolved in Release 3.0.

DDTS # CSCdt53432: IMPROPRMVL Alarm

In previous releases, CTC did not consistently report improper removal (IMPROPRMVL) of XC/XCVT cards.

This issue is resolved in Release 3.0.

DDTS # CSCds15889: Add Node Feature

In previous releases, the Add Node feature was only supported when you added a new, isolated node in either a bidirectional line switched ring (BLSR) or a unidirectional path switched ring (UPSR) configuration. If a node was already part of a network, the Add Node feature was not supported.

This issue is resolved in Release 3.0.

DDTS # CSCdt14323: Provisioning of C-Bit TCA

In previous releases, C-Bit Threshold Crossing Alerts (TCAs) in C-Bit framing mode could not be provisioned from CTC.

This issue is resolved in Release 3.0.

DDTS # CSCdt82081: TIM-P Alarm on Protection Switch

In previous releases, existing path trace string mismatch (TIM-P) alarms in DS3E protection groups might have been lost during protection switches.

This issue is resolved in Release 3.0.

Performance Monitoring

DDTS # CSCdu50988 and CSCdv38748

CTM Release 2.2 does not support SONET section and DS-3 PM parameters for the Cisco ONS 15454 Releases 3.0.x. Use CTC to retrieve SONET section and DS-3 PM data. The PM parameters not supported by CTM Release 2.2 are:

- SONET section PM: CV-S, ES-S, SES-S, STS FC-P, PSC-W, PSD-W, PSC-S, PSD-S, PSC-R, PSD-R
- DS-3 PM: LOSS-L

This issue is resolved in Release 3.0.3 and CTM Release 2.2.1.

DDTS # CSCdv10889 and # CSCdv47419

While you are retrieving bulk PM data, you will not be able to open a CTC session with the node. Cisco recommends that you open a CTC session with the node before beginning bulk PM transfer, in the event that you may need to access the node during the transfer.

This issue is resolved in Release 3.0.3.

Interoperability

DDTS # CSCdt25702

In previous releases, when you provisioned circuits between rings on a node configured with both BLSR and UPSR topologies, XC cards might have reset.

This issue is resolved in Release 3.0.

UPSR on Top of BLSR or 1+1

In previous releases, the TL1 interface erroneously allowed the user to overlay UPSR protection on BLSR or 1+1 protection.

In general, the working and protect UPSR paths should be over unprotected spans. However, it is possible to route intermediate portions of a UPSR circuit over 1+1 or BLSR if the UPSR drop points are not on the same node where the 1+1 or BLSR is defined.

The UPSR drop can, however, be on a BLSR or 1+1. In other words, you can interconnect a UPSR and a BLSR on the same node by “dropping” the UPSR circuit onto the BLSR or 1+1 spans.

This issue is resolved in Release 3.0; the TL1 interface now prevents the user from overlaying UPSR protection on BLSR or 1+1 protection.

SONET/SDH

DDTS # CSCct04091

In previous releases, you had to provision all circuits as bidirectional. Unidirectional circuits were not supported. If a unidirectional circuit was provisioned, loss of signal (LOS) alarms would be generated.

This issue is resolved in Release 3.0.

UPSR Functionality

DDTS #: CSCct03852

In previous releases, no alarm was reported when a UPSR protection switch occurred. The event was reported in the event log but not as a standing alarm.

This issue is resolved in Release 3.0.

BLSR Functionality

DDTS # CSCdu06367 Traffic Disruption on BLSR Protection Switch

Occasionally a disruption of greater than 60 ms on STS-Nc traffic can occur when a 2-fiber BLSR carrying STS-Nc traffic makes a protection switch. This issue is resolved in Release 3.0.3.

DDTS # CSCdv73379

In previous releases, following a BLSR switch due to SD-L or SF-L, switched traffic may have undergone continued, intermittent disruption. The traffic disruption is caused by K-byte update messaging from the cross connect card to the OC-48 cards in pass-through nodes. The K-byte update messaging is the root cause of the traffic problems. When these traffic problems occurred, it was after the switch had taken place and nodes had gone into pass-through mode. This issue is resolved in Release 3.0.3.

DDTS # CSCdu38133 and CSCdu37768: Precautions Needed After BLSR Deletion

In previous releases, the following precautions were needed after deleting a BLSR:

To ensure optimum provisioning performance, after deleting a BLSR, perform a software-initiated reset on the standby XC/XCVT and wait for it to reboot. When the standby XC/XCVT has finished rebooting, perform a software-initiated reset on the active XC/XCVT.

This issue is resolved in Release 3.0.1.

DDTS # CSCdt38383: Force Switch on OC-48 Spans

In previous releases when forcing a switch on OC-48 spans in BLSR configurations, traffic disruptions in excess of 50 ms could occur.

This issue is resolved in Release 3.0.

DDTS # CSCds58575: Fiber Pulls on OC-48 Spans

In previous releases, when pulling fibers on OC-48 spans in BLSR configurations, traffic disruptions in excess of 50 ms could occur.

This issue is resolved in Release 3.0.

Multiple Span Failure in a BLSR Configuration

In previous releases, Cisco did not recommend disabling multiple spans in a BLSR configuration. Multiple span failures might have caused intermittent switching between working and protect paths on the circuits in the remaining spans.

This issue is resolved in Release 3.0.

Synchronization

DDTS # CSCdr03214

In previous releases, line-timed nodes could lose connectivity to their primary reference source during software upgrades. The loss of connectivity forced the nodes into a hold-over state or to switch to the secondary source. This did not affect traffic.

This issue is resolved in Release 3.0.

TL1

DDTS # CSCdv12827

In previous releases, execution of the RTRV-BLSR command might have caused the TCC+ to reboot.

This issue is resolved in Release 3.0.2.

DDTS # CSCdv08712

In previous releases, if you entered 1024 or more characters in a TL1 (or CTM/TL1) session, TL1 agent would raise an exception and reset the TCC. To avoid this problem, you could avoid entering 1024 or more characters in a TL1 session, or you could use CTM Release 2.2. This issue is resolved in ONS 15454 Release 3.0 and CTM Release 2.2.

Documentation

Release Notes

In the release notes for Releases 2.2.1, 2.2.2, 3.0, and 3.0.1 the following caution was mistakenly associated with the DDTS number CSCds34584:

> When provisioning VLANs, you cannot provision the same VLAN to both ports at once. Each port must have a separately-provisioned VLAN. When the cards are initially provisioned, set the VLAN membership before enabling the port.

This caveat was intended to be general advice and should not have been associated with any DDTS number.

In the release notes for Releases 3.0 and 3.0.1, this caveat was moved to the closed items section and described as “resolved.” This is also inaccurate, because the conditions described are a normal function of the CTC design.

MIB Readme Information

The README.txt file in the **15454/MIBS** directory of the *Cisco ONS 15454 System Software* CD has been updated to include the following information. In previous releases, this information was available only through the release notes. This issue is resolved in Release 3.0.2. The information is now included in theREADME.txt file.

> IMPORTANT: Note that different MIB files are used for the ONS 15454 and ONS 15327, respectively. The file CERENT-454-MIB.mib contains the object and trap definitions pertaining to the ONS 15454. The file CERENT-GENERIC-MIB.mib contains the object and trap definitions pertaining to the ONS 15327.
>
> When provisioning the Network Management System for the ONS 15454, use the file CERENT-454-MIB.mib.
>
> When provisioning the Network Management System for the ONS 15327 use the file CERENT-GENERIC-MIB.mib.

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.

Traffic Protection

DDTS # CSCdu44181

In a DS-1 1:N protection group, if a working card has switched traffic to the protect card, removing the working card from the protection group when it is standby can cause a traffic outage. To avoid this issue, you must switch traffic back to the original working card before removing the card from the protection group.

DDTS# CSCdu50983 Manual Protection Switch does not Clear After a Higher Priority Switch

An automatically initiated switch request (for example, LOS, or LOF) will not clear a user-configured switch request (for example, Manual, or Force). The user-configured switches are queued when preempted by higher priority commands and will be reinstated when the higher priority command is cleared. You must manually clear user configured switches. This issue will be resolved in a future release.

Line Cards

DDTS # CSCdv14523 IMPROPRMVL Alarm does not Clear

When a line card is removed from its slot at the same time that a provisioning message is sent to the card, the node can enter a state where the IMPROPRMVL alarm associated with the card removal will not clear after the card is deleted from the node. This issue will be resolved in a future release.

DDTS # CSCdt90845 and CSCdu46771

No alarm will be generated if the line type set on a DS3E card does not match the incoming signal (for example, if the line type is set to C-bit and the incoming signal is actually M23). This issue will be resolved in a future release.

DDTS # CSCdv64474

When the active TCC+ is removed and then replaced rapidly (within 5-10 seconds), an AUTORESET alarm, which normally indicates that the TCC+ reset as a result of an internal condition, may be mistakenly raised against the card. This alarm clears when the TCC+ completes rebooting, but remains in the alarm history log. This issue will be resolved in a future release.

DDTS # CSCdv62565

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

To avoid possible problems, before adding slots to a protection group, ensure that:

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

This issue will be resolved in a future release.

DDTS # CSCdu71847: DS3 Equipment Protection

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

E-Series Cards

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. With Release 3.0.3, the ONS 15454 now 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 Ethernet circuits. This issue will be resolved in a future release.

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 provisoned 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 17 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/E100T-12

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

DDTS # CSCdw45877

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

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

This issue is resolved in Release 3.4.

TCC Software Synchronization

In every release prior to Release 3.0.3, when you place a standby TCC into the chassis it receives the software from the active TCC on its primary flash only. With Release 3.0.3 and forward, the standby TCC loads both the primary and the secondary (backup) versions of the software, if needed. This process can cause a longer wait for a card to come up under certain conditions, as explained below.

When a standby TCC (TCC+ or TCCi) is inserted in the shelf, it will synchronize its software and database with the active TCC. The standby TCC checks first for the current software version it is running. If it finds a mismatch, the standby TCC copies the software from the active TCC and resets itself to come up again on the same software as the active TCC. If both are running the same version, the standby then checks its own backup version of software, and, if its version does not match the backup version on the active TCC, the standby copies the backup software from the active TCC, then resets again. Each copy process (with a reset) takes 15-20 minutes. If both the primary and secondary software versions on the standby TCC match those on the active TCC, no copying and thus no extra resets are needed, and the time for the standby TCC to come up will be one or two minutes.

DDTS # CSCdw16886

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

ONS 15327 Release 1.0

ONS 15327 Release 1.0.1

ONS 15454 Release 3.0

ONS 15454 Release 3.0.1

ONS 15454 Release 3.0.2

ONS 15454 Release 3.0.3

ONS 15454 Release 3.1

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

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

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

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

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

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

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

DDTS # CSCdw06182

In the CTC Edit > General > Preferences menu, you can specify an alternate user preferences file for your local workstation by entering the file path in the Include File field. The purpose of this feature is to allow you to have a network-wide CTC preference file that can be referenced by each workstation.

Any changes to the user preferences are stored in the default user preferences file (for Windows, CTC.ini; for UNIX, .ctcrc) that resides on the individual workstation.

In CTC Releases 3.0.x, the include file does not override the default user preferences file, though it can still be specified and CTC will retain the file location. This issue will be resolved in a future release.

DDTS # CSCdv72264

A Java “Illegal Argument Exception” can occur when a manual switch request is applied in the CTC Maintenance > Timing tab for the EXT1 BITS Out. To clear this exception, relaunch CTC and clear the manual switch request. This issue will be resolved in a future release.

DDTS # CSCdv72457

If a two-way VT circuit is created on any port of a DS1 card, UNEQ-V is raised on all other ports on the card that are in service, or any port that is placed in service after the circuit creation. This issue will be resolved in Release 3.1

DDTS # CSCdv83675

After clearing LOS, LOF, or AIS-L on an STS path, a pre-existing LOCKOUT-REQ condition can disappear from the conditions pane of CTC or the TL1 logs. This issue will be resolved in a future release.

DDTS # CSCdv64833

In CTC Release 3.0.3, a condition can occur wherein you will no longer be able to manually switch timing references to a third reference, even though the status shows that manual switching is enabled. If you then try to clear the manual switch, or to perform another switch, the Apply button will remain grayed out (inactive) and you will be unable to apply any further reference switches. To return CTC timing reference switching to an operational state, restart your CTC session. This issue will be resolved in a future release.

DDTS # CSCdv77176

The working switched to protect (WKSWPR) condition is not reported upon a manual or force ring switch in BLSR. This issue will be resolved in a future release.

DDTS # CSCdv72317

Traffic disruption can occur upon placing the working port out of service (OOS) in a 1+1 linear protection group using optical cards. To avoid this disruption, perform a manual switch before placing the port OOS. This issue has been seen with OC-48 and OC-3. This issue will be resolved in Release 3.3.

DDTS # CSCdv81254

When an IP address is added to the list of networks managed by CTC, CTC should add management of the new network during the current session. However, in CTC Release 3.0.3, newly added nodes are not visible unless you close your current CTC session and reopen CTC with the “additional nodes” option selected. This is also the case for deletion of nodes. This issue will be resolved in Release 3.1.

Span Upgrade

You cannot perform a span upgrade in Release 3.0.x. This feature is enabled in Releases 3.1 forward.

DDTS # CSCdv66003

The working switched to protection (WKSWPR) alarm condition might not be reported by a node participating in a 1+1 revertive protection group. This issue can arise after applying a manual or force switch to a working OC-48 card in a 1+1 linear protection group. This issue is not traffic affecting. This issue will be resolved in Release 3.1.

DDTS # CSCdv72286

A facility loopback can mistakenly generate a loss of frame (LOF) alarm (along with the expected AIS-P) when applied to an OC-3 card that is physically looped back to another optical card and a test set (where traffic runs from the test set to the other optical card, and then to the OC-3 card). This has been seen in a two-node, OC-48, 1+1 protection group, and only occurs with OC-3.

DDTS # CSCdv72434

In a 1:1 or 1:N protection group, if a lockout is placed on a working card, and the protect card is removed, causing a loss of traffic, the alarm raised is IMPROPRMVL MN NSA. It should be IMPROPRMVL CR SA, since traffic will be down. This has been seen on DS-3E 1:1, EC1 1:1, DS-3 1:N, and DS-1 1:N. This issue will be resolved in a future release.

DDTS # CSCdv50711 and CSC76389

In the node view of CTC, the following screens fail to provide a horizontal scroll bar:

Provisioning tab

- Ethernet Bridge
- Ring
- SONET DCC
- Alarming

Maintenance tab

- Ring
- Software Route Table

This issue will be resolved in a future release.

DDTS # CSCdv61249

Under rare circumstances, a node may become grayed out in CTC after an activation to Release 3.0.3 and a subsequent TCC+ removal. This issue is not traffic affecting, and you can regain the connection with the node by re-launching CTC. This issue will be resolved in a future release.

DDTS # CSCdv70067

An LOS alarm may be lost upon switching traffic to a protect card. This issue will be resolved in a future release.

DDTS # CSCdv62314

Under certain unknown conditions, a node that is reachable may appear as grayed-out in CTC. To resolve this issue, open a CTC session with the node having trouble. You will be able to view all nodes from this node. This issue is not traffic affecting. This issue will be resolved in a future release.

Reserved Ports

The following ports are reserved on all ONS 15XXX platforms:

0 — ZERO

2001–2017 (inclusive) — IOCARDS_TELNET_PORTs

2018 — ACTIVEDCC_PORT

5001 — BLSR_SERVER_PORT

5002 — BLSR_CLIENT_PORT

7200 — SNMP_ALM_INPUT_PORT

9100 — EQM_TCP_PORT

9300 — TCC_UDP_PORT

9401 — TCC_BOOT_PORT

Well known ports (for example, those commonly associated with HTTP, FTP, TELNET, etc.) should be avoided as well. Well known port values are typically less than 1024.

DDTS # CSCdv60230

Some nodes in a DCC mesh might not appear in the CTC network view even though the CTC host has IP network connectivity to the nodes. That is, CTC can be started from any node in the DCC mesh but the CTC network view might not necessarily show all the nodes. Also, sometimes the nodes appear but not all DCC links appear.

This condition occurs only when a node has an IP address whose third octet is zero and whose fourth octet is less than 32 (decimal). Thus, a node with an IP address of 192.1.0.5 is vulnerable, but nodes with addresses 192.1.1.5 or 192.1.0.64 are not.

To avoid this issue causing problems in your network, provision each IP address with a non-zero third octet. All nodes in the DCC mesh must have the corrected IP addresses.

This issue will be resolved in Release 3.1 and ONS 15327 Release 3.3.0.

DDTS # CSCdv63402

In rare cases, after a CTC session has remained open for a prolonged period, or after activation to a new software release, the Maintenance > Software pane may mistakenly show “Major Alarm” or “Critical Alarm” in the Node Status column. To verify whether or not there is a real alarm, look in the Alarms pane, which will only show an alarm if one actually exists. To clear a false alarm report, close and reopen CTC. This issue will be resolved in a future release.

DDTS # CSCdv62990

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

Note For TL1 password functionality, please see the “Password Enforcement” section on page 46.

DDTS # CSCdv33367

When you place a line (traffic) card in a slot provisioned for another card type, CTC displays a mismatch equipment attributes (MEA) alarm and a communication bus failure (CONTBUS) alarm, both of which will clear once you delete the provisioned card type and reprovision the correct card type for the actual physical card in the slot. However, when you place a line card in a slot provisioned for another card type, TL1 and SNMP display an MEA alarm, but no CONTBUS alarm. For TL1 and SNMP the CONTBUS alarm appears momentarily after you delete the provisioned card type and re-provision the correct card type for the actual physical card in the slot, and then both alarms clear. This issue will be resolved in a future release.

DDTS # CSCdv40561

If you place an OC-N port out of service when it participates in a unidirectional 1+1 protection group, you must first perform a manual or force switch away from the port.

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. 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 # CSCdu81874

When you are not running DNS and there is no entry in the hosts list for a given node name/IP address pair, a situation can arise wherein CTC might fail to recognize a node by its IP address.

This behavior is most often seen when using CTM. When CTM attempts to enter node view for an unlisted node, CTC fails to recognize the node and this results in the CTC session being aborted.

It is also possible to see this behavior while running CTC alone. In this case, CTC can lose connection to the node after you create a login group in which the node participates and you subsequently close your session with the node, then attempt to open a new session using the IP address of the unlisted node.

To avoid this issue, use DNS. If you cannot use DNS, you must:

Check to ensure that all nodes are given valid names (node names should contain alphanumeric characters or hyphens, but no special characters or spaces).

Ensure that all nodes that will be monitored by CTM or will participate in a login group are listed in the hosts file as a valid node name/IP address pair.

This issue will be resolved in Release 3.1.

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. This issue will be resolved in a future release.

DDTS # CSCdu69006

The DCC OSPF area contains “0.0.0.0” by default. When you activate OSPF on the TCC+ LAN, its default area is 0.0.0.0. The TCC+ LAN area and the DCC area are configurable, but initial edits to the DCC area might not take. Normally, after changes are made and applied to the DCC area, the TCC+ reboots and the changes take effect; however, the first time you edit the DCC area, your applied changes might not take, even though the TCC+ reboots. After the TCC+ finishes rebooting, check to ensure that your provisioning was properly applied. If the default “0.0.0.0” still appears, you must enter and apply the changes a second time, then allow the TCC+ to reboot once more before your edits will take effect. This issue will be resolved in a future release.

OSPF Virtual Links

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

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

The CTC Protection pane that displays the status of protection groups might not refresh to reflect that a protect card has been removed. The Improper Removal alarm is raised, however. This issue will be resolved in a future release.

DDTS # CSCdt88289: Processing of FEAC Loopback Commands

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

"Are you sure" Prompts

Whenever a proposed change occurs, the "Are you sure" dialog box appears to warn the user that the action can change existing provisioning states or can cause traffic disruptions.

DDTS # CSCdr98061: AIP Card Change

Changing the Alarm Interface Panel (AIP) card can cause some circuits to become Incomplete. Repair each circuit, one node at a time, using the Repair button from the Circuits tab in CTC. Some circuits might still appear erroneously as Incomplete. After completing the repair operation, you must relaunch CTC. This issue will be resolved in a future release.

DDTS# CSCdu28367

After a node reverts from Release 3.0 to an earlier release, its SDCC connections become intermittent. CTC will show the SDCC connection alternating between up and down, and the node will become unreachable through its SDCC connection. This problem occurs when two nodes that are SDCC connected are both running Release 3.0, and one of the nodes reverts to an earlier release. To recover from this situation, open a CTC session for the remote node running Release 3.0, delete the SDCC link to the peer node, then recreate the link. The SDCC link will function normally. This issue will be resolved in a future release.

Protection Groups

DDTS # CSCdu34970

When you place a lock on a protection group and remove the protect card, the severity of the improper removal alarm (IMPROPRMVL) is reported as Minor, Non-Service affecting instead of the expected Critical, Service affecting. This issue will be resolved in Release 3.1.

DDTS # CSCdu34972

If you remove a protect card that is reporting an LOS alarm from a non-revertive 1:1 protection group the LOS alarm does not immediately appear for the active card. The delay time before the alarm appears is approximately 80 seconds. This problem exists for all electrical cards (DS-1, DS-3, DS3E, DS3XM, and EC-1). The problem does not occur if the protection group is revertive.

As expected, the improper removal alarm (IMPROPRMVL) immediately appears for the removed protect card. This issue will be resolved in Release 3.1.

DDTS # CSCdu34975

When you set a port to Out of Service (OOS), the reported severity of the LOS alarm changes from Critical, Service affecting to Minor, Non-service affecting before the LOS alarm clears. The severity of the alarm should not change before the alarm clears. This issue will be resolved in Release 3.1.

DDTS # CSCdu34977

When you create a circuit on a DS-1 card, the severity of any existing minor LOS alarm (such as would be left after having previously deleted circuits on the port while it was out of service and then placed the port back in service) does not escalate to Major, Service affecting. This issue will be resolved in Release 3.1.

DDTS # CSCdu34978

The reported severity of an LOS alarm on a DS3XM-6 card does not de-escalate from Critical, Service affecting after you delete all DS3XM-6 circuits. This issue will be resolved in Release 3.1.

DDTS # CSCdu34980

After deleting a protection group and circuit on an EC1-12 card, putting the EC1-12 port into service raises an LOS alarm with a reported severity of Critical, Service affecting instead of the expected Minor, Non-service affecting. This issue will be resolved in Release 3.1.

SNMP

DDTS # CSCdv69960

SNMP sonetMediumValidIntervals and sonetMediumInvalidIntervals for a node increment whether or not the associated port is in service. To see the correct valid or invalid intervals, use the CTC GUI. This issue will be resolved in a future release.

DDTS # CSCdv69964

SNMP dsx1IntervalValidData for a node returns true after card provisioning whether or not the associated port is in service. To see the correct valid status, use the CTC GUI. This issue will be resolved in a future release.

Performance Monitoring

DS1 Electrical Transmit Path PMs

No threshold crossing alarms are reported for a DS1 electrical transmit path. The CTC provisioning pane, electrical path thresholds tab, has only one set of thresholds. PMs are reported for DS1 electrical receive and transmit, but a threshold crossing alarm is generated only for the receive electrical path.

DDTS # CSCdv73802 and CSCdv74996 Far End PM Monitoring

In Releases 3.0.x, CTC allows you to set thresholds for far-end P-bit DS3XM PMs, but the DS3XM does not perform far-end P-bit monitoring at this time. You cannot monitor far-end P-bit DS3XM PMs on the Performance screen, so the Provisioning tab should display far end P-bit as grayed out. TL1 and CTC also allow setting of thresholds and apparent monitoring of STS Far End PMs, which is not supported. To monitor far end PMs, use IPPM at the far end and monitor the near end path parameters on the other node. These issues will be resolved in a future release.

DDTS # CSCdv26401

When you view the Provisioning > Elect Path Threshold tabs for a DS3-E card and select Far End and DS3Pbit, PM thresholds are displayed. These thresholds are invalid. The DS3Pbit applies to Near End thresholds only. Do not attempt to set error levels for DS3-E DS3Pbit when the far end is selected. This issue will be resolved in a future release.

DDTS # CSCdv30999

You can view IPPM data on protection circuits if you designate the protection group before you create circuits. In a future release, IPPM data for protection circuits will be available independent of provisioning sequence.

DDTS # CSCdu10769: Performance Monitoring Statistics

STS performance monitoring (PM) statistics will not be triggered by a Path Trace String Mismatch (TIM-P) or Payload Label Mismatch (PLM-P). Certain STS PM statistics should trigger in a TIM-P or PLM-P situation (see Table 6-15 of Telcordia GR-253, Footnote c). With one-bit RDI-P support, these are CV-P, ES-P, SES-P, and UAS-P. This issue will be resolved in a future release.

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 # CSCdu29530

In a 4 node, 2 Fiber BLSR configuration, applying lockout on the West side of all 4 nodes might cause traffic loss at one of the nodes. This traffic loss only occurs when you place a lockout on both east and west sides of the 4 nodes, clear the lockout from all nodes, and then apply lockouts on the west sides of each node. To avoid this problem:

For software upgrades in Release 3.0.x, apply the lockout on the east and west sides of all nodes.

For XC (cross connect) side switches, apply lockouts on the peer nodes, on the side that shares the span with the node whose XC is to be side switched. This avoids the need for applying a lockout only on the west side of each node.

This issue is resolved in Releases 3.0.4 and 3.1.

DDTS # CSCdt79962

An XC or XCVT side switch can cause a 1+1 OC-N or a BLSR protection switch. This can occur in any 1+1 OC-N configuration, although it is more likely with OC-48s. This can also occur in a BLSR configuration. This issue is independent of ONS 15454 timing (BITS, internal, line) or OC-N slots.

For Releases prior to 3.1, take the following steps to avoid this problem:

1. Ensure that the working span is active (on both the local and remote node).
2. Ensure that the working span is carrying error-free traffic.
3. Lockout the protect span prior to initiating an XC/XCVT side switch.

Note: An XC/XCVT side switch can be initiated in any of the following ways:

- Reset the active XC/XCVT
- Remove the active XC/XCVT
- Issue a switch XC/XCVT command

This issue is resolved in Releases 3.0.4 and 3.1.

DDTS # CSCct03396 Ring Map Change Dialog Box

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

DDTS # CSCdw02830

In a two ring, two fiber BLSR network, do not change the ring ID of the first ring to the same ring ID as the second ring. You can only do this from a node that participates only in the first ring (not the shared node), but to do so can cause a cross connect reset. This issue will be resolved in a future release.

DDTS # CSCdv83748

In a BLSR configuration, if a power failure occurs on a node, traffic passing through that node will switch away within 50 ms. However, when power is restored to the node and the ring returns to an idle state, traffic may be interrupted for greater than 50 ms during the restoration process. This issue will be resolved in Release 3.1.

DDTS # CSCdv46667

After a ring switch on a non-revertive BLSR, some LOP-P alarms might fail to clear. To clear these alarms you must perform an automatic ring switch. This issue will be resolved in a future release.

DDTS # CSCdw01019, CSCdv21120, and CSCdu89221

In BLSR, a force span switch (FE-FRCDWKSWPR-RING) alarm, or ring switch east (RING-SW-EAST) alarm, may be cleared from the alarm and history tabs by a second switch request; however, the original condition that caused the alarm might still be present. This issue will be resolved in Release 3.1.

DDTS # CSCdw01054

After a BLSR ring switch, the WTR alarm might fail to clear. This issue will be resolved in a future release.

DDTS # CSCdv76001

In a Release 3.0.3 BLSR, when an SDCC to a node is disconnected (as in when a fiber is removed from the node), it is possible for alarms on the ring to get out of synchronization due to communication to the node being rerouted around the ring. If this occurs, the node may become temporarily grayed out (approximately 30 seconds) in CTC and alarms either reported or cleared to the node during the grayed out period may not appear in the Alarms tab. To ensure visibility of all alarms associated with that node, click the Synchronize Alarms button in the Alarms tab. This issue will be resolved in a future release.

DDTS # CSCdu65073 and CSCdv34627

If you apply a force on a ring, you must clear it before applying a lockout to any span on the ring. This issue will be resolved in Release 3.1.

DDTS # CSCdv33547

You must choose node IDs in the range of 0-15 for the first 16 nodes deployed in a BLSR. Also, as a precaution against possible traffic interruption, before releasing any BLSR lockout, ensure that all fibers removed since the lockout are replaced. This issue will be resolved in Release 3.1.

Four-Fiber BLSR Configuration

4-fiber BLSR configurations are not currently supported. 4-Fiber BLSR configuration will be supported in Release 3.1.

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 (refer to the *Cisco ONS 15454 Installation and Operations Guide, Release 3.0* for details on these procedures):

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.

Upgrades

DDTS # CSCdv01219

Upon activation of Release 3.0.3, you might receive the Java exception error, “IOExeception: Connection reset by peer.” Please disregard this message as it is a product of changes instituted in the Java code base for Release 3.0.3 that Release 2.2.x is unable to interpret. The Java exception has no adverse effect. This issue will be resolved in a future release.

DDTS # CSCdu57328

After activation of a node during upgrade, you should receive a message indicating that the activation was successful, followed by a message that you have lost connection to the node (this is normal during the rebooting portion of activation). Rarely, you may receive the message “TCC activation has been successfully initiated. Activate status unavailable.” This message does not indicate any serious issue with your upgrade. Click OK to clear the message from your screen and resume the upgrade procedure normally. This issue will be resolved in a future release.

Documentation

Release Notes Caveat Closed

The initial version of the *Release Notes for Cisco ONS 15454 Release 3.0.3* showed the DDTS defect, CSCdv14523, as resolved in Release 3.0.3. This was incorrect. The issue is still open in Release 3.0.3, and is now documented in the *“DDTS # CSCdv14523 IMPROPRMVL Alarm does not Clear”* section on page 15 of the list of caveats.

Troubleshooting and Reference Documentation

The following 15 alarms and conditions were added to the Alarm Troubleshooting chapter of the Cisco *ONS 15454 Troubleshooting and Reference Guide* for release 3.0.3. Each alarm or condition entry contains a description, alarm severity and troubleshooting procedure. Page numbers refer to the online version of the *Cisco ONS 15454 Troubleshooting and Reference Guide,* Release 3.0.3.

APSCDFLTK, page 1-5

APSCNMIS, page 1-8

AUTOLSROFF, page 1-9

CONCAT, page 1-14

FAILTOSWR, page 1-28

FAILTOSWS, page 1-30

FEPRLF, page 1-33

LOF (BITS), page 1-40

LOS (BITS), page 1-46

MAN-REQ, page 1-51

RING-MISMATCH, page 1-60

SFTWDWN, page 1-63

SFTWDWN-FAIL, page 1-63

SSM-FAIL, page 1-65

TRMT, page 1-69

The following two procedures have been updated in the *Cisco ONS 15454 Troubleshooting and Reference Guide, Release 3.0*.

Replace an In-Service XC/XCVT Card

Caution Removing any active card from the ONS 15454 can result in traffic interruption; therefore, only replace standby cards. If the active card needs to be replaced, follow the steps below to switch the XC/XCVT card to standby prior to removing the card from the node.

An XC/XCVT reset or switch can cause a linear 1+1 OC-N protection switch or a BLSR protection switch.

Step 1 Take the following precautions before performing an XC/XCVT reset or switch to avoid causing a linear 1+1 or BLSR protection switch:

a. Ensure the working span is active on both the local and remote nodes.

b. Ensure the working span is carrying error-free traffic (no SD or SF alarms present).

c. Lockout the protection span prior to initiating an XC/XCVT reset.
In a BLSR, place a lockout on the East and West cards of the nodes adjacent to the XC/XCVT switch node; for example, to switch the XC/XCVT on Node B, place the lockout on the West card of Node A and on the East card of Node C. No lockout is necessary on Node B. Before the lockout is set, verify that the BLSR is not switched. If a lockout is set while the BLSR is switched, traffic can be lost.
<------East [Node A] West------East [Node B] West------East [Node C] West------>
In a 1+1 protection scheme, place a lockout on the protect card and verify that the traffic is traveling over the working span before setting the lockout.

Step 2 Determine the active XC/XCVT card. The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is yellow.

Note You can also place the cursor over the card graphic to display a popup identifying the card as active or standby.

Step 3 Switch the active XC/XCVT to standby:

a. In the node view, select the **Maintenance** > **XC Cards** tabs.

b. From the Cross Connect Cards menu, choose **Switch**.

c. Click **Yes** on the Confirm Switch dialog box.

Note After the active XC/XCVT goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

Step 4 Physically remove the new standby XC/XCVT card from the ONS 15454.

Step 5 Insert the replacement XC/XCVT card into the empty slot.
The replacement card boots up and becomes ready for service after approximately one minute.

Step 6 Release the protection lockout.

TL1 Documentation

The following commands were erroneously included in the *Cisco ONS 15454 TL1 Command Guide* for Release 3.0. These commands are not supported in Releases 3.0.x.

ALW-MSG-DBCHG

INH-MSG-DBCHG

REPT DBCHG

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 # CSCdv74990

A TL1 session on a serial port produces an unexpected echo. This occurs when you connect to a TCC+ front panel serial port via a TL1 session. The session echoes duplicate characters.

DDTS # CSCdv76146

TL1 commands to retrieve individual PM parameters for OC-48 (both 15 minute and one day) are denied in the TL1 session. To access these parameters in TL1, you must retrieve all. This issue will be resolved in a future release.

DDTS # CSCdv86514

In accordance with Telcordia GR-815, Cisco ONS 15454 Release 3.0.3 requires that a password must have at least 1 numeric character (0 to 9) and at least one special character from the character set {plus-sign (+), pound-sign (#), percent-sign (%)}. Before you begin your upgrade from Release 2.2.x to Release 3.0.3, ensure that all passwords are Telcordia-compliant to avoid possible problems logging in with TL1. This issue will be resolved in a future release.

DDTS # CSCdv70043

TL1 does not support autonomous RING alarms in Release 3.0.x. These alarms can be retrieved using RTRV-ALM-ALL or RTRV-COND-ALL. This issue will be resolved in Release 3.1.

DDTS # CSCdu31489: TL1 Gateway

A Gateway Network Element (GNE) receiving commands from an operations support system (OSS) and passing them to an End-Point Network Element (ENE) is case-sensitive when determining the command path. The GNE will reject commands sent to an ENE when the case of the TID used in the command differs from the case of the assigned TID for the ENE. To ensure that all commands sent through a gateway are properly received, use the exact case of the ENE name as assigned. This issue will be resolved in Release 3.1.

Commands not Supported as of Release 3.0

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

ED-CRS-<STS_PATH>

ED-CRS-VT1

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

OPR-UPGRADE

New Features and Functionality

This section describes new features and functionality for Release 3.0.x.

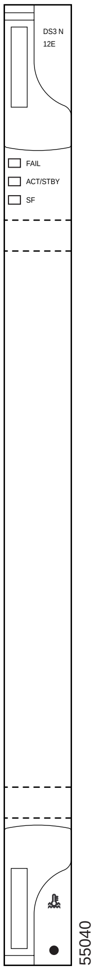
Hardware

Enhanced DS-3 PM Card

The Enhanced DS-3 PM card provides enhanced performance monitoring functions. In addition to providing B3ZS error monitoring on the facility, the DS3-12E and the DS3N-12E cards provide the following enhanced feature set:

- Auto-detection and auto-provisioning of framing format
- P-Bit monitoring
- C-Bit Parity monitoring
- X-Bit monitoring
- M-Bit monitoring
- F-Bit monitoring
- Idle Signal detection
- FEBE monitoring
- FEAC status alarm detection
- FEAC loopcode detection/activation
- PRBS generation and detection
- J1 Path Trace support

Figure 1 DS3-12E Card



The introduction of the DS3-12E and DS3N-12E provides the capability to detect several different errored logic bits within a DS-3 frame and thus gives the Cisco ONS 15454 the ability to identify a degrading DS-3 facility caused by upstream electronics (that is, DS-3 Framer). As logic error rates increase, the chance of violating the B3ZS coding scheme increases. However, by monitoring additional overhead in the DS-3 frame, even subtle degradations within the network can be detected.

Card Specifications

- Incoming Frame Format Detection: allows you to set an expected incoming framing format on a per port basis. Acceptable values are C-Bit, M23, and Unframed.
- Auto-Framing Detection: automatically reports the framing format being received. Acceptable values are C-Bit, M23, and Unframed. You select a value in the Provisioning tab.
- DS-3 Auto-Provision: allows you to auto provision the DS3N-12E on a per port basis. When selecting the Auto Provision Mode, the node automatically sets the expected incoming framing format based on the detected framing format.
- Path Trace Detection (SONET Side): detects path trace failure based on the expected incoming J1 path trace string as provisioned in CTC. A TIM-P alarm is generated if the values do not match.
- Path Trace Byte Transmission: allows you to transmit a character string within the J1 byte such that a SONET-based optical interface can transport the byte transparently.

- J1 Byte (Path Trace) Support: supports the SONET path trace function as defined by GR-253-CORE.
- Framing Bit Error Detection and Accumulation: counts framing errors based on the expected incoming framing format as provisioned in the software.
- OOF Detection: detects Out Of Frame (OOF) based on the OOF detection criteria defined in GR-499-CORE.
- Parity Calculation: calculates parity based on both DS-3 “P-bit” and DS-3 “C-bit.”
- Parity Error Detection and Accumulation: counts parity errors based on the expected incoming parity as provisioned in the software.
- Loopback Request Acknowledgment (Facility Side): responds to FEAC loopbacks codes as they apply to the payloads being processed by the node (for example, DS-3 Intact Payloads). Any valid FEAC code is recovered by the DS3N-12E. (Note that this function is only valid in C-bit framing mode.)
- Idle Signal Detection: detects an “idle” signal as defined by GR-499-CORE. The signal format is “1100” in the payload with specific C-bit values.
- Far End Block Error Event Detection: detects FEBE occurrences and increments the FEBE register upon each occurrence.
- X-Bit Mismatch: detects X-bits that are mismatched (for example, 10 and 01) and counted as X-bit mismatch errors.
- P-Bit Mismatch: detects P-Bits that are mismatched (for example, 10 and 01) and counted as P-bit mismatch errors.
- LOS Detection and OOF Reporting: If a OOF was declared previously, followed by a LOS on the same facility, the Out Of Frame alarm will be cleared.
- Parity Error Monitoring: reports received parity errors based on the expected incoming parity values and processes this performance monitoring information.
- FEAC Loopback Enabling: allows you to provision a port such that FEAC loopback is allowed or not allowed, where the default is “not allowed.”
- FEAC Loopback Activation: activates a loopback upon receipt of a DS-3 FEAC loopback request only if FEAC loopbacks have been allowed on that port; otherwise the request is denied.
- DS-3 RDI Reporting: reports a DS-3 Remote Defect Indication if the expected X-bits match those being received in a manner defined by GR-499-CORE.
- PRBS Transmit, Receive, and Error Detect Support: on-board PRBS Transmit, Receive, and Error Detection functions. Transmit functions are supported from the node toward the SONET line while Receive functions support PRBS patterns received from the DS-3 facility.
- NEBS3 Compliance: compliance with NEB3 requirements as defined by GR-1089-CORE, GR-063-CORE, and associated Regional Bell Operating Company standards.
- Temperature Operation: ambient temperatures between -40 degrees Celsius and +65 degrees Celsius.
- Temperature Storage: ambient temperatures between -40 degrees Celsius and +85 degrees Celsius.
- Humidity Operation: The DS3N-12E cards shall be capable of operating at relative humidities of 5% to 95%, non-condensing. With ambient temperatures above 29 degrees Celsius, the relative humidity may be limited to that corresponding to a specific humidity of 0.024 pounds of water per pound of dry air.

- Humidity Storage: relative humidities of 5% to 95%, non-condensing. With ambient temperatures above 29 degrees Celsius, the relative humidity may be limited to that corresponding to a specific humidity of 0.024 pounds of water per pound of dry air.
- Quality and Reliability: meets the quality and reliability specification of TR-NWT-000332.
- Lifetime: minimum predicted mean time between failure of 20 years using the calculation procedure outlined in TR-NWT-000332, Issue 4, method 1.

General Purpose Slot Support

The following equipment configurations support the DS3N-12E card when placed in Slots 1 through 6 and 12 through 17:

- Stand-alone (cross connect)
- Optical point to point (2-fiber terminals)
- Linear ADM (4 high speed slots)
- 2-Fiber unidirectional path switched rings
- 2-Fiber bidirectional line switched rings
- 2 x 2-Fiber bidirectional line switched rings (4 high speed slots)
- 4-Fiber bidirectional line switched rings
- 2 x 2-Fiber unidirectional path switched rings

Software

Alarm Suppression

At the card level, you can suppress alarms on specific ports. At the node level, you can suppress alarms on specific cards or the entire node.

If alarms are suppressed, they do not appear on the CTC Alarm screen. On the History and Conditions screens a message states that the alarm or alarms are suppressed. The node sends out autonomous messages to clear any raised alarms. When alarm suppression is turned off, the node sends out autonomous messages to raise any suppressed alarms.

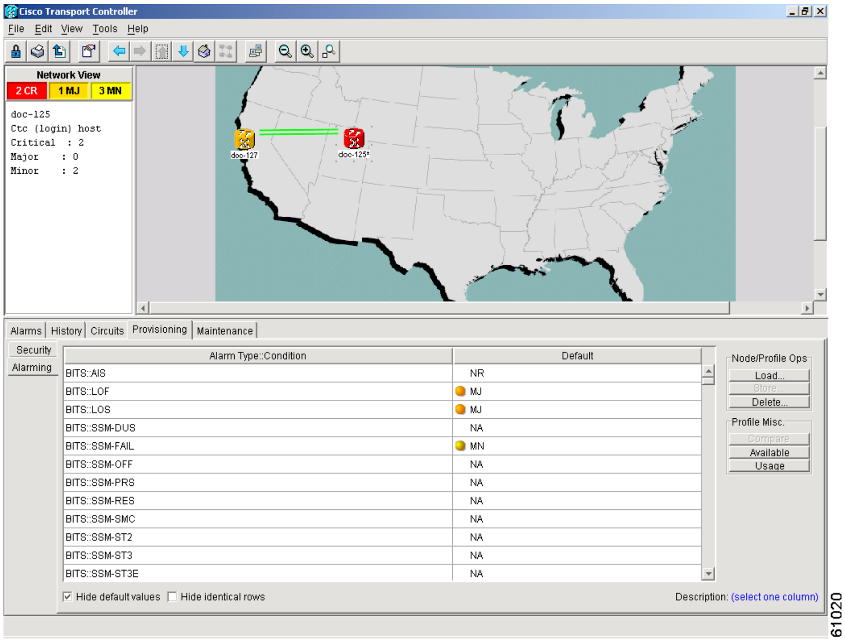
Alarm Profiles

The ONS 15454 includes an alarm profile feature. This allows you to change the default alarm severities (for example, change an alarm severity from minor to major) and apply the new severities at the card, port, node, or network level.

Default Reporting of AIS and RFI

To improve compliance with Telcordia GR-253, Release 3.0.x reports AIS and RFI failures as not alarmed (NA). These will appear on the conditions pane only. Users can change this default with the Alarm Profile feature described in the “Alarm Profiles” section on page 36.

Figure 2 Creating alarm profiles with the Alarming tab



```
doc-125
Ctc (login) host
Critical  : 2
Major     : 0
Minor     : 2
```

Alarm Type::Condition	Default
BITS::AIS	NR
BITS::LOF	● MJ
BITS::LOS	● MJ
BITS::SSM-DUS	NA
BITS::SSM-FAIL	● MN
BITS::SSM-OFF	NA
BITS::SSM-PRS	NA
BITS::SSM-RES	NA
BITS::SSM-SMC	NA
BITS::SSM-ST2	NA
BITS::SSM-ST3	NA
BITS::SSM-ST3E	NA

☑ Hide default values □ Hide identical rows

Description: (select one column)

Every alarm has a default profile. To create a new profile, clone the default profile in CTC, rename it, and choose the severity settings for the new profile. Activating and changing profiles are simple procedures in CTC.

Intermediate-Path Performance Monitoring

Release 3.0.x supports Intermediate-Path Performance Monitoring (IPPM), which is the transparent monitoring of a constituent channel of an incoming transmission signal by a node that does not terminate that channel. IPPM allows you to monitor near-end PM data on individual STS payloads and report the associated threshold crossing alerts (TCAs) for user-selected STS payloads passing through a Cisco ONS 15454 OC-N card. Far-end PM monitoring is not presently supported.

An ONS 15454 performing IPPM examines the overhead in the monitored path and derives all of the near-end PM parameters in the incoming transmission direction while allowing the path signal to pass bidirectionally through the NE completely unaltered.

IPPM parameters are derived as follows: a bidirectional path is cross-connected through the ONS 15454 (non-PTE equipped) and has path terminations at path terminating equipment (PTE) 1 and PTE 2. Four sets of PM parameters are accumulated when IPPM is activated. For the path signal received on facility 1, these include the near-end parameters monitored on the path from PTE 1 to the SONET Line Terminating Equipment (LTE). For the path signal received on facility 2, these include the near-end parameters.

Intermediate J1 and C2 Monitor and Report

Release 3.0.x provides intermediate monitoring of the SONET J1 and C2 bytes, which means the LTE NE can provide on-demand diagnostics to detect and report the contents of the STS Path Trace and Signal Label in non-terminated STS Paths designated by the user. The J1 Byte contains a repetitive 64-byte message used to verify continuity between STS PTEs transmitting the byte. The J1 byte reports when an expected 64-byte message is not received. The C2 Signal Label byte provides a similar functionality. The C2 byte contains binary values or codes that define a specific type of payload transmitted in the STS SPE. The C2 byte is provisioned at the PTE. It is used to both identify the SPE payload and support STS Payload Defect Indication (PDI-P). Release 3.0.x allows you to monitor these bytes at intermediate (LTE) nodes and monitor specific STS Paths or groups of STS paths. You can provision an expected J1 or C2 value so that the node reports when an expected value for either byte is not received at the intermediate node.

Section Performance Monitoring

The SONET Section PM feature enables the Cisco ONS 15454 to accumulate and report the section layer performance monitoring parameters on any OC-N card. The section layer deals with the transport of an STS-N frame across the physical medium. This layer handles framing, scrambling, and error monitoring. All types of SONET devices terminate the section layer. A SONET regenerator, however does not process beyond the physical and section layers. When a non-Cisco regenerator is used on the span between two ONS 15454s operating as LTEs, the ONS 15454 Section PM isolates the side of the regenerator that is causing any bit errors.

The ONS 15454 monitors the following section-layer parameters:

- Severely Errored Framing Seconds (SEFS-S): the number of seconds an SEF defect was present
- Errored Seconds (ES-S): the number of seconds during which at least 1 section BIP error was detected, or an SEF or LOS defect was present.
- Severely Errored Seconds (SES-S): the number of sections during which K or higher section BIP errors were detected or an SES or LOF was present (K is bit-rate dependent).
- Coding Violations (CV-S): a count of the number of section-layer BIP errors.

Auto-refresh PM Data

- You can auto-refresh PM data using a check box and pull-down menu providing valid options on the Performance Monitoring screen in the card view. When selected, the information auto refreshes the screen every *x* seconds (where *x* is selected from the valid options or manually configured). The auto-refresh only works while the selected card is in card view. When you are not viewing this card in card view, PM data is not auto-refreshed. However, when you return to the card, the auto-refresh option has not changed. This parameter can be specified and remembered for each card individually and for each node separately.

BLSR Enhancements

Support for Two 2-Fiber BLSRs

A single ONS 15454 supports two distinct 2-fiber OC-12 or OC-48 BLSR logical nodes within one physical node. Traffic from one BLSR can cross connect to the other BLSR at both the VT1.5 and STS-1 payload mappings.

- OC-12 BLSRs can be created using any traffic card slot; OC-48 BLSRs must reside in Slots 5, 6, 12, and 13.
- If more than one BLSR is supported per physical ONS 15454 node, each logical BLSR node will function as an independent ring unless traffic is interconnected between both logical nodes.

- The ONS 15454 allows two logical OC-12 BLSRs or two logical OC-48 BLSRs to operate on one physical node. It also allows one logical BLSR node to operate at OC-12 and one logical BLSR node to operate at OC-48 on one physical node.

Increased BLSR Node and Ring ID Support

Release 3.0.x will support up to 16 nodes in a BLSR. This includes pass-through nodes, regenerators, and add/drop nodes. The range of BLSR ring IDs has been expanded from 0 through 255 to 0 through 9999. You can provision greater than 16 nodes per BLSR, but you might experience switch times of greater than 50 ms with this configuration.

CTC Platforms

The Cisco Transport Controller runs on PC computers and Sun and H-P workstations. CTC can be launched by Netscape Navigator and Microsoft Internet Explorer on the following platforms: Netscape Navigator 4.x - Windows 95, Windows NT 4.0, Windows 98, Windows 2000, Solaris 2.6.x, Sun Solaris 2.5.x, Microsoft Internet Explorer 5.x - Windows 95, Windows NT 4.0, Windows 98, Windows 2000, Solaris 2.6.x, and Sun Solaris 2.5.x.

CTC supports the Java 2 platform on the following operating systems: Windows 95, Windows NT 4.0, Windows 98, Windows 2000, Solaris 2.6.x, Sun Solaris 2.5.x, (O) HP UX 11.x, and (O) HP UX 10.x.

CTC is optimized for laptop PC computers with the following specifications: Pentium II 300 MHz with 128 MB of RAM, and a 2 GB hard drive, with Windows NT Workstation 4.x, and Netscape Navigator 4.x.

CTC can manage 25 nodes concurrently. The 25 nodes can be on a single DCC or split across multiple DCCs. Four concurrent CTC sessions can interact with the same ONS 15454 node at the same time.

CTC Installation

First-time use of the Cisco Transport Controller requires a computer loaded with a CTC-compatible Internet browser, a CTC-compatible version of the Java Runtime Environment, a target ONS 15454, and TCP/IP DCN connectivity. The Java policy file required for first-time use of CTC is distributed with the CTC archive file(s) on the TCC+. The file can also be downloaded from the web, or installed automatically by the CTC Setup Wizard.

The CTC Setup Wizard guides the user through the first CTC download and installation. The setup wizard supports user input directory paths and custom installation, and guides user action when necessary to ensure smooth, continuous execution of the download and installation process.

Daylight Savings Time

Cisco Transport Controller supports all North American standard time zones (Atlantic, EST, CST, MST, PST, Alaska, Hawaii) as well as Universal (GMT). It also supports Daylight Savings time. CTC supports time zones with and without Daylight Savings; users can configure the time zone of a network element and opt for Daylight Savings or no Daylight Savings.

Port Naming

Release 3.0.x provides the ability to store a name with each ONS 15454 traffic card port. Right-click the port to view the name. Other port naming features include:

- Node and network alarm and history panels: when an alarm affects a named port, or a circuit that traverses a named port, the port name is displayed in the alarm.
- Circuit creation: if a port is named, CTC displays the port name and port number.
- Node and network circuit list: if either or both circuit end points are named, CTC displays the port name and port number.
- Node provisioning: if any port is named, CTC displays the port name and the port number (panes affected include line and threshold).
- Node maintenance: if any port is named, CTC displays the port name and the port number (loopback).
- Node performance data: if any port is named, CTC displays the port name and port number.

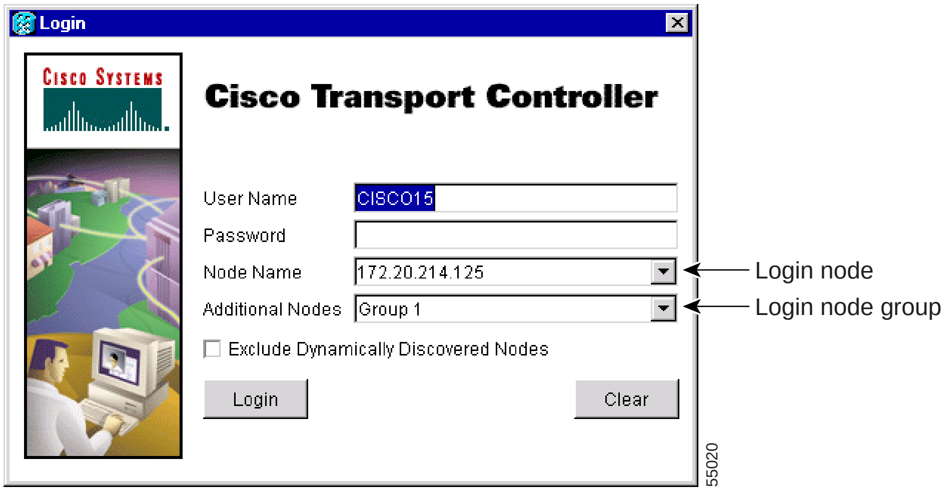
Search for Circuit by Name

Release 3.0.x allows you to search for circuits by circuit name, or by a substring included in the circuit name. The substring search allows you to jump down an alphabetically sorted list of circuits to those beginning with a particular letter. Enter the circuit name (or a substring included in the name) in the Circuit Name Search dialog box and click “Find Next.” You can search up or down the list of circuits. The search tool selects the circuit bearing the name you type. Once you have found the circuit, you can open it by double-clicking the selected row.

Limit DCC Autodiscovery at Login

A check box on the CTC Login dialog box allows you to limit DCC autodiscovery so you can open a single or selected group of ONS 15454s residing in a network.

Figure 3 Login Dialog Box



User Name: CISCO15

Password:

Node Name: 172.20.214.125

Additional Nodes: Group 1

□ Exclude Dynamically Discovered Nodes

Login node

Login node group

Multi-Circuit Operations

CTC allows you to modify selector settings on a set of circuits. If you select a set of circuits and make changes to selectors, the changes are applied end-to-end along each of the selected circuits.

Auto Range

CTC also provides an auto-range feature that eliminates the need to individually build circuits of the same type. Specify the number of circuits you need, create one circuit, and CTC automatically creates additional sequential circuits.

Baseline Button

In CTC Release 3.0 and higher, the Baseline button located on the far right of the Performance Monitoring screen clears the PM count displayed in the Current column, but does not clear the PM count on the card. When the current 15-minute or 24-hour time interval passes or the screen view changes, the total number of PM counts on the card and on the screen appear in the appropriate column.

Clear Button

The Clear button located on the far right of the Performance Monitoring screen clears certain PM counts depending on the option selected. When the Clear button is clicked, three options appear in the Clear Statistics menu: Selected interfaces, All interfaces on port x, and All interfaces on card.

When you clear selected interfaces, all PM counts associated with the selected radio buttons are erased. For example, if the "15 min" and the Near End buttons are selected and you click the Clear button, all near-end PM counts in the current 15-minute interval are erased from the card and the screen display.

When you clear all interfaces on port x, all PM counts associated with all combinations of the radio buttons on the selected port are erased from the card and the screen. This means the 15-minute near-end and far-end counts and 24-hour near-end and far-end counts are cleared from the card and the screen.

When you clear all interfaces on the card, PM counts for all data and ports on all interfaces are erased from the card and the screen.

⚠ **Caution** The Clear button can mask problems if used incorrectly. This button is commonly used for testing purposes.

✎ **Note** The Ethernet cards are the only cards without the Clear button option.

Active/Standby Indication

In node view, visual indication of the status (active vs. standby) of each card in an ONS 15454 node is provided. This allows you to view the status quickly, which is particularly helpful during a forced or automatic protection switch. This feature enhances (but does not replace) the current mouse roll-over indication.

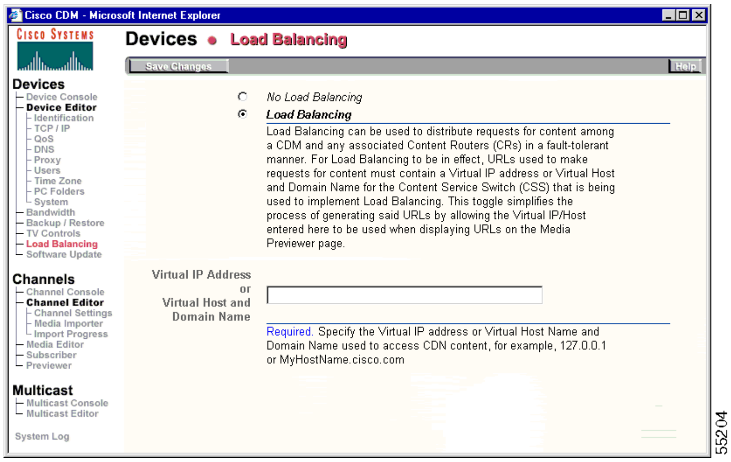
Filtering of Circuit View Window

In the CTC circuit window, you can filter circuits to the current network/node/card level. This option restricts the circuits listed to only those items meeting the filter criteria and associated with the current view (for example, the circuits on the node or card being viewed).

CTC Preferences

Release 3.0.x allows you to set CTC preferences from a new Preferences dialog box, shown in Figure 4.

Figure 4 Preferences Dialog Box



○ *No Load Balancing*

● ***Load Balancing***

Load Balancing can be used to distribute requests for content among a CDM and any associated Content Routers (CRs) in a fault-tolerant manner. For Load Balancing to be in effect, URLs used to make requests for content must contain a Virtual IP address or Virtual Host and Domain Name for the Content Service Switch (CSS) that is being used to implement Load Balancing. This toggle simplifies the process of generating said URLs by allowing the Virtual IP/Host entered here to be used when displaying URLs on the Media Previewer page.

Virtual IP Address or Virtual Host and Domain Name:

Required. Specify the Virtual IP address or Virtual Host Name and Domain Name used to access CDN content, for example, 127.0.0.1 or MyHostName.cisco.com

Change the CTC Network Image

The CTC Preferences dialog box allows you to change the image displayed in CTC network view. Any JPEG or GIF image accessible from a local or network drive can be used.

Limit History

The CTC Preferences dialog box allows you to modify the number of records shown in the CTC alarm history.

Access Non-DCC Connected ONS 15454 Networks

In previous CTC releases, access to non-DCC connected ONS 15454 networks required you to add the topology host IP address to the cms.ini file. In Release 3.0.x, you can add the IP address(es) for additional non-DCC connected networks to be managed by CTC. When you log into CTC, you can specify which groups you want to access.

Modify Span Colors

The CTC Preferences dialog box allows you to modify the background and foreground of active and standby spans. Span colors can be selected from color swatches on the Circuit pane of the Preferences dialog box.

Firewall Access

In Release 3.0.x, workstations can access the ONS 15454 using a firewall-compliant connection. Specify the port to connect through in the Firewall pane of the Preferences dialog box.

Loopback Indication

CTC provides a visual indication for ports, circuits, and circuit records that are involved in a loopback.

AutoDelete Cleared Alarms Checkbox

When you check AutoDelete Cleared Alarms, CTC remembers the setting between sessions.

Column Sizes

If you change the column width of table data in a CTC window, CTC will retain that width for the rest of the CTC session (unless you change it again). CTC Release 3.0.x allows the operator to save individual column widths for each type of table.

OSPF Support

Open Shortest Path First (OSPF) support allows OSPF hello notifications to be exposed through the LAN interface to external routers which automatically update their static route tables. OSPF can be configured so that OSPF routes are not displayed automatically. The default setting is off (not advertising OSPF).

Inhibit Switch to Protection Support

CTC reflects protection switches issued by TL1 commands. CTC also supports Lockout inhibition when set by TL1 or CTC.

Online Help

ONS 15454 Release 3.0 documentation can be viewed in an online help window accessed through the CTC Help menu. The help is installed from the ONS 15454 Release 3.0.x software CD or the documentation CD, using the new CTC Setup Wizard. The help window includes a table of contents and an index in frames adjacent to the body text. It also provides access to PDF versions of the manuals and a search tool.

GR-253 VT Renumbering

In accordance with Telcordia GR-253 Section 6.1.2 (R6-2), VT numbering within an STS-1 uses a two-level Group number and VT number convention. Port numbers associated with VTs are shown so that you do not need to look in the documentation for this mapping.

SONET/SDH Combination Card

CTC reflects each port’s mode configuration (SONET/SDH) visually in inventory and card view. Each port can be set to SDH or SONET. If a port is configured as SDH, CTC prevents VT and STS-1 cross connection.

For SDH, CTC functionally provides the same operation that was supported when the units were configured for SONET services only.

Each port on all OC-12 cards (OC12 IR 1310, OC12 LR 1310, OC12 LR 1550) can be provisioned as STM-4. Each port on all OC-48 cards (OC48 IR 1310, OC48 LR 1310, OC48 LR 1550) can be provisoned as STM-16.

All CTC fault management functions are provided for these cards.

Performance Management

All CTC performance management functionality:

- Provides for SDH
- Reports existing PM information (SONET and Async)
- Reports threshold crossing alarms

Configuration Management

- CTC graphically and visually designates the SDH/SONET combo card and each port's current mode (SONET or SDH mode).
- CTC supports the ability to cross connect an STM circuit to an appropriate size STS circuit (for example, STM1 to STS-3C).
- CTC circuit management functionality provides for SDH circuits.
- To provision an SDH circuit, an appropriate STS-N circuit is defined. The section and line information on the inbound signal will be terminated. The STS-N carries the SDH path information and SDH payload. At the SDH handoff, SDH section and line header information is reintroduced so that an SDH signal departs.

Node Diversity

Release 3.0.x supports node diversity as an option during automated circuit provisioning across UPSR segments in a mesh (PPMN) network. This option does not apply to 1:1, unprotected, and BLSR portions of the network. Node diversity means that, except for the source and destination, the circuit's working and protect paths do not traverse any of the same nodes. This feature ensures that the failure of a single node will not eliminate the benefit of SONET protection.

DHCP Pass-through Support

Release 3.0.x allows Dynamic Host Configuration Protocol (DHCP) requests/responses to traverse the ONS 15454 network. This allows craft PCs to request and receive appropriate IP addresses. In addition, the combination of DHCP pass-through and Proxy ARP allows the craft PC to work without any ONS 15454 or PC configuration in most subnetting environments. With the static route support introduced in Release 2.1, the craft PC can work with an ONS 15454 even when multiple nodes on the same DCC share a subnet and other crafts are connected. DHCP pass-through support includes support for User Datagram Protocol (UDP) and listening on Port 67 (the standard BOOTP/DHCP port). DHCP pass-through is configured as "on" or "off" in CTC; the default is "off."

Lamp Test

You can activate ONS 15454 lamp tests from CTC. When the test is invoked, all ONS 15454 LEDs illuminate at the same time for 10 seconds. Bicolored LEDs cycle from green to yellow.

Improved Management Routing

The following improvements have been made to management routing:

- Route advertisement over LAN interface: the surface mechanism (OSPF) eliminates the need to add to static route tables in an affiliate router when a Cisco ONS ring is deployed. Only the node IP address is sent to external systems via OSPF; IP addresses on cards are not sent. You can configure OSPF so that node IPs are not sent. The default configuration is off (not advertising OSPF).
- Craft attachment: Craft attachment and management of all nodes on a DCC (regardless of subnetting) without the addition of static routes to the craft PC is now possible. Proxy ARP or a similar mechanism over a LAN interface is supported to provide this capability. Multiple craft attachments to the same DCC can occur at the same time.
- Route learning and aging support: redundant physical connections to an ONS 15454 ring are supported, including rerouting messages through an alternate route and/or an alternate ONS 15454 gateway. Nodes can reroute messages (including the primary and secondary gateway nodes). This feature is not affected by subnet configuration (all nodes on one subnet, all nodes on different subnets, or any combination).

Improved GUI on Circuit Creation Wizard

A panel was added to the Circuit Creation Wizard to record entries from previous pages. This panel is visible during the selection process and displays user selections.

Network Topology Map

In Release 3.0.x, you can use a Zoom command to change the network topology map display:

- You can store a preferred zoom configuration as the default map view.
- When you zoom in or out, nodes are repositioned so that DCC spans do not overlap. DCCs are clearly delineated while nodes retain their geographic positions (as placed by the user or longitude/latitude coordinates).
- With zooming, it is possible to see and select one of up to ten DCC spans.
- The size of the ONS 15454 icon has been reduced to allow for more nodes in a view.

Common Security Profiles

CTC allows user security information (userid, password, permissions) to be shared across the nodes it manages:

- You can set SNMP community strings and access privileges.
- You can perform user management operations (such as creating a user or changing a password) at the network level. When a change is made on this screen, it applies to all CTC-managed nodes.

Multiple Circuit Creation

You can define multiple circuits between the same nodes in one easy step using the Number of Circuits field in the Circuit Provisioning Wizard.

CTC Managed Software Download

CTC Managed Software Download allows you to download CTC software to multiple nodes serially and in parallel.

Note Cisco advises that you limit concurrent software downloads to 3 nodes at once.

Directional Arrows on Circuit Maps

Arrowheads have been added to circuit lines displayed on the circuit map to distinguish unidirectional and bidirectional circuits.

TL1

CTAGs

In accordance with Telcordia GR-831, all TL1 commands must include a CTAG. Commands without CTAGs will be rejected by TL1 with the error Invalid Correlation Tag (IICT).

Password Enforcement

In accordance with Telcordia GR-815, TL1 functionality for Release 3.0.3 enforces password complexity as follows.

ONS 15454 TL1 enforces password complexity for TL1 and users. This rule only applies for new or changed passwords after Release 3.0.3 is installed; existing passwords do not need to be changed. A new password must have at least 1 numeric character (0 to 9) and at least one special character from the character set {plus-sign (+), pound-sign (#), percent-sign (%)}.

Note See the "DDTS # CSCdv62990" section on page 22 for a CTC caveat to these rules.

Test Access

TL1 Test Access enables you to monitor and test circuits. Commands to connect, disconnect and change the test access (TACC) and test access connections have been added to TL1 for Release 3.0. Refer to the *TL1 Command Guide, Release 3.0* for more information.

Gateway Network Element Topology

TL1 Gateway enables you to issue TL1 commands to multiple nodes using a single connection. Any node can serve as a Gateway Network Element (GNE), End-Point Network Element (ENE), or Intermediate Network Element (INE). A node becomes a GNE when a TL1 user connects to it and enters a command destined for another node. An ENE is an end node because it processes a TL1 command that is passed to it from another node. An INE is an intermediate node because of topology; it has no special hardware, software, or provisioning.

The GNE Session is the connection that multiplexes TL1 messages between the OSS/craftsperson and the GNE. The GNE demulitplexes incoming OSS TL1 commands and forwards them to the remote ENE. The GNE also multiplexes incoming responses and autonomous messages to the GNE Session. The ENE Session is the connection that exchanges messages between the GNE and the remote ENE.

Each GNE can support six (5+1) concurrent gateway communication sessions (connections from an OS to the GNE). Five of these sessions are via the LAN (wire-wrap, active TCC+ LAN port, or DCC) and the sixth session is reserved for the active TCC+ serial port.

New AIDs

TL1 supports the following new AIDs as of Release 3.0.

- BLSR
- ALL (added to the VT1_5 AID table)

Parameter Value Changes

TL1 supports the following parameter value changes as of Release 3.0.

- TMPER input/output value changed from 15MIN to 15-MIN
- SENDDONOTUSE changed to SENDDUS
- BLSR_MODE (new parameter)
- BLSR_TYPE (new parameter)
- MOD-TACC
- TACC-MODE

New Conditions

TL1 supports the following new conditions as of Release 3.0.

- NHSWPR - Inhibit switch to protect request on equipment
- NHSWWKG - Inhibit switch to working request on equipment

The following new BER alarm conditions have been added:

Condition	Alarm Description	Type
SD-L	BER Threshold exceeded for Signal Degrade	Line
SD-P	BER Threshold exceeded for Signal Degrade	Path
SF-L	BER Threshold exceeded for Signal Failure	Line
SF-P	BER Threshold exceeded for Signal Failure	Path

Conditions Replaced in Release 3.0

The SWFTDWN condition has been changed to SFTWDOWN.

Release 2.2.1 TL1 Commands Replaced in Release 3.0

Category	Command	Replacement
Equipment	RTRV-FFP-EQPT DLT-FFP-EQPT ED-FFP-EQPT ENT-FFP-EQPT	RTRV-EQPT DLT-EQPT ED-EQPT ENT-EQPT
	// Pre-provisioning cards ENT-<MOD2>	ENT-EQPT

	// Enable facility for service
	RST-<MOD2>
		RST-<MOD_PORT>
		// Setting attributes of port/facilities
		// including enable facility
		ED-<OCN_TYPE>
		ED-EC1
		ED-T1
		ED-T3

	// Un-provisioning cards DLT-<MOD2>	DLT-EQPT

	// Remove facility from service
	RMV-<MOD2>
		RMV-<MOD_PORT>
		// Setting attributes of port/facilities
		// including disable facility
		ED-<OCN_TYPE>
		ED-EC1
		ED-T1
		ED-T3

	OPR-PROTNSW-EQPT	SW-TOPROTN-EQPT SW-TOWKG-EQPT
System	ED-NE	ED-NE-GEN
	RTRV-NE	RTRV-NE-GEN
Testing	OPR-LPBK-<OCN_TYPE>	OPR-LPBK-<MOD2_IO>
	RLS-LPBK-<OCN_TYPE>	RLS-LPBK-<MOD2_IO>

Release 2.2.1 TL1 Commands Changed in Release 3.0

TL1 COMMAND	DESCRIPTION OF CHANGES
ALW-MSG-ALL INH-MSG-ALL	The two commas at the end of the command are not needed anymore.
ALW-SWDX-EQPT	Semi-colons after the CTAG field are not required anymore.
DLT-CRS-<STS_PATH> DLT-CRS-VT1	Trailing semi-colons after the CTAG are optional.
ED-BITS	Added support for the Sync Message field. An extra colon is needed after CTAG field. The colon after the PST field is not necessary. The Name string in Name/Value parameter changed.
ED-EC1	Added support for the Rx Equalization attribute for an EC1 port. The extra colon after the PST field is not required anymore.
ED-T1	Removed support for the ID field. Three colons after the CTAG field are now required, instead of two. The extra colon after the PST field is not required anymore. Added support for Test Access.
ED-T3	Three colons are needed after CTAG field, instead of two. The extra colon after the PST field is not required anymore. Added support for Test Access.
ED-<OCN_TYPE>	Added support for the send DUS and Synchronous Status Message fields. The extra colon after the PST field is not required anymore. Three colons are needed after the CTAG field instead of two.
ENT-CRS-<STS_PATH>	Cross-connect types are optional. The default is 2WAY. Supported Cross Connect types are now limited to 1WAY and 2WAY.
ENT-FFP-<OCN_TYPE> ED-FFP-<OCN_TYPE>	An extra colon after the CTAG field is required. Name field in name/value parameters have changed.
ED-EQPT ENT-EQPT RTRV-EQPT	This family of commands was functionally expanded to edit/enter/retrieve equipment attributes and electrical 1:1 and 1:N Protection Group. Use these commands instead of ED/ENT/RTRV-FFP-EQPT.
ED-USER-SECU	Added support for a NEW USER ID field. Fields are now positional instead of name/value pairs.
ENT-USER-SECU	An extra comma is needed after the PASSWORD field.
ED-<STS_PATH>	Added support for following fields: Revertive Mode, Revertive Time, Expected Path Trace, Path Trace Message, and Path Trace Mode. Added support for Test Access.
INIT-SYS	Phase Field (Level of Initialization) is not supported anymore.
OPR-LPBK-<MOD2_IO> RLS-LPBK-<MOD2_IO>	The Loopback Type field is now optional.

OPR-PROTNSW-<OCN_TYPE>	Added support for the SWITCH command field.
INIT-REG-<MOD2> RTRV-PM-<MOD2>	Added support for an optional Location field. Now only one comma is needed (instead of two) after the Time Period field.
REPT ALM BITS REPT ALM SYNCN	Output – The Condition description field is now optional.
REPT ALM <MOD2ALM> REPT ALM EQPT REPT EVT <MOD2ALM>	The Description and Equipment Type fields are now optional.
REPT ALM EVT	The positions of the Description and Equipment Type fields have changed.
REPT EVT SYNCN	Output – Condition and Condition Description are now optional. Requires 7 commas (instead of 6) after the Condition Effect field. Added support for the Aid Type field.
RTRV-ALM-BITS RTRV-ALM-SYNCN	Output – Added support for the Aid Type field.
RTRV-BITS	Output – Added support for the Sync Messaging field.
RTRV-COND-ALL	One less comma is needed after the Condition field.
RTRV-COND-BITS RTRV-COND-SYNCN	Requires two commas (instead of three) after the Condition field.
RTRV-CRS-<STS_PATH> RTRV-CRS-VT1	Semi-colons after the CTAG are no longer required.
RTRV-ALM-EQPT RTRV-COND-EQPT RTRV-ALM-MOD2 RTRV-COND-MOD2 RTRV-ALM-ALL	Use one less comma after the Service Affect field.
RTRV-EC1	The four colons after the CTAG field are now optional. Output – Added support for the Rx Equalization field.
RTRV-FFP-EQPT	Output – Name field in Name/Value parameters changed.
RTRV-INV	Output – Requires two colons (instead of one) after the Aid Type field.
RTRV-LOG	Requires an additional logname field.
RTRV-<OCN_TYPE>	The four colons after the CTAG field are now optional. Output – Added support for the following fields: Sync Status Messaging, Send DUS, Ring ID, and BLSR Type. Dropped support for Revertive Time.

RTRV-<STS_PATH>	Output – Added support for the following fields: Revertive Mode, Revertive Time, Expected Path Trace, Path Trace Message, Incoming Path Trace, Path Trace Mode and Test Access.
RTRV-SYNCN	Output – Replaced the Primary, Secondary, and Third fields with Rank of Synchronization Reference, Value of a Sync Ref, Quality of Sync Source, and Status of Signal Source.
RTRV-TOD	Output – Requires one comma (instead of two) after the Seconds field.
RTRV-T1 RTRV-T3	The four colons after the CTAG field are now optional. Output – Dropped support for the ID field.
SET-TOD	The Name string in the Name/Value parameter has been changed from USEDST to DST
SW-DX-EQPT	The comma after the optional Mode field is no longer necessary.

TL1 Commands New in Release 3.0

Note Refer to the TL1 Command Guide for new command descriptions.

CATEGORY	**COMMAND**
BLSR	ED-BLSR RTRV-BLSR
ENVIRONMENT	RTRV-ATTR-CONT RTRV-ATTR-ENV RTRV-EXT-CONT SET-ATTR-CONT SET-ATTR-ENV OPR-EXT-CONT RLS-EXT-CONT
EQUIPMENT	ALW-SWTOPROTN-EQPT ALW-SWTOWKG-EQPT INH-SWTOPROTN-EQPT INH-SWTOWKG-EQPT SW-SWTOPROTN-EQPT SW-SWTOWKG-EQPT ED-EQPT INH-SWDX-EQPT

FAULT	REPT ALM COM // Autonomous message
PERFORMANCE	RTRV-PMMODE-<STS_PATH> SET-PMMODE-<STS_PATH>
SECURITY	REPT EVT SECU // Autonomous message
	CANC // Autonomous message
SYNCHRONIZATION	OPR-SYNCSW RLS-SYNCSW
SYSTEM	ED-NE-GEN CHG-ACCMD-<MOD_TACC> CONN-TACC-<MOD_TACC> DISC-TACC
	RTRV-NE-GEN RTRV-NE-IPMAP
PORTS	RMV-<MOD_PORT> RST-<MOD_PORT>
STS & VT PATHS	RTRV-PHTRC-<STS_PATH> ED-VT1 RTRV-VT1
SYNCHRONIZATION	ED-NE-SYNCN RTRV-NE-SYNCN
UPSR SWITCHING	OPR-PROTNSW-<STS_PATH> OPR-PROTNSW-VT1 RLS-PROTNSW-<STS_PATH> RLS-PROTNSW-VT1 REPT SW // Autonomous message

Related Documentation

- *Cisco ONS 15454 Installation and Operations Guide, Release 3.0*
- *Cisco ONS 15454 Troubleshooting and Reference Guide, Release 3.0*
- *Cisco ONS 15454 TL1 Command Guide, Release 3.0*
- *Cisco ONS 15454 Product Overview, Release 3.0*
- *Release Notes for the Cisco ONS 15454*, Release 3.0.2
- *Upgrading Cisco ONS 15454 Release 2.2.x to 3.0.3*
- *Upgrading Cisco ONS 15454 Release 3.0.x to 3.0.3*

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including the *Cisco ONS 15454 Release Notes*, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM, a member of the Cisco Connection Family, is updated as required. Therefore, it might be more current than printed documentation. To order additional copies of the Optical Networking Product Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www.europe.cisco.com.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation, including the Optical Networking Product CD-ROM from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl
- 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 Cisco ONS 15454 User Documentation.