



Release Notes for Cisco ONS 15327

Release 4.1.8

October, 2007



Note

The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15327 SONET multiplexer. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to Release 4.1 of the *Cisco ONS 15327 Installation and Operations Guide*, *Cisco ONS 15327 Troubleshooting and Reference Guide*, and *Cisco ONS 15454 and Cisco ONS 15327 TLI Command Guide*. For the most current version of the *Release Notes for Cisco ONS 15327 Release 4.1.8*, visit the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/ong/15327/rnotes/index.htm>

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

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

Contents

- [Changes to the Release Notes, page 2](#)
- [Caveats, page 2](#)
- [Resolved Software Caveats for Release 4.1.8, page 9](#)
- [New Features and Functionality, page 14](#)
- [Related Documentation, page 22](#)
- [Obtaining Documentation, page 22](#)



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

Copyright © 2007 Cisco Systems, Inc. All rights reserved.

[Documentation Feedback, page 23](#)

[Cisco Product Security Overview, page 23](#)

[Obtaining Technical Assistance, page 24](#)

[Obtaining Additional Publications and Information, page 26](#)

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15327 Release 4.1.8* since the production of the Cisco ONS 15327 System Software CD for Release 4.1.8.

No changes have been added to the release notes for Release 4.1.8.

Caveats

Review the notes listed below before deploying the ONS 15327. Caveats with DDTS tracking numbers are known system limitations that are scheduled to be addressed in a subsequent release. Caveats without DDTS tracking numbers are provided to point out procedural or situational considerations when deploying the product.

Maintenance and Administration



Caution

VxWorks is intended for qualified Cisco personnel only. Customer use of VxWorks is not recommended, nor is it supported by Cisco's Technical Assistance Center. Inappropriate use of VxWorks commands can have a negative and service affecting impact on your network. Please consult the troubleshooting guide for your release and platform for appropriate troubleshooting procedures. To exit without logging in, enter a Control-D (hold down the Control and D keys at the same time) at the Username prompt. To exit after logging in, type "logout" at the VxWorks shell prompt.

DDTS # CSCee01779

A DBOSYNC alarm might be raised after circuit deletion, then creation, and subsequent (within 15 seconds) fiber pull on the same circuit. To recover from this, write the database once again with any provisioning change. This issue will be resolved in Release 5.0.

DDTS # CSCeb12993

When you perform a database restore initiated while the database is being saved, a DBOSYNC or BKUPMEMP alarm may be raised, accompanied by a silent restore failure. To avoid this issue, ensure no provisioning was changed within past 2 minutes before initiating a restore. This issue is resolved in Release 4.6.

DDTS # CSCeb09356

The CTC card level provisioning pane allows a different range of values for the PSC-W, PSC-S, and PSC-R thresholds from the range allowed in the defaults provisioning window. At the CTC card view for an OC-192 card, CTC will allow any values for the PSC-W, PSC-S, and PSC-R. When provisioning these same values using the CTC node view defaults pane, the range is restricted from 0 to 600. This issue is resolved in Release 4.6.

DDTS # CSCeb06071

Rarely, in the detailed circuit view for some VT circuits, a question mark may appear in the center of a port graphic. Ignore the question mark: it would indicate a problem with path trace functionality, but VT circuits do not have that functionality. This issue is resolved in Release 4.6.

DDTS # CSCdz84149

If a user is logged into CTC as a superuser (or other higher level security type), and then another superuser changes the first user's security level to "retrieve" (or another lower level security type) without first logging the user out, the lower level user is then still able to perform some actions authorized only for the original login security level. For example, a "provisioning" level user demoted to "retrieve" level in this manner can still provision and edit MS-SPRings (BLSRs) while logged into the current session, though the same user may no longer provision DCCs. To ensure that a user's level is changed completely, the superuser must log the user out prior to changing the security level. This issue is resolved in Release 4.6.

DDTS # CSCdz90753

In the Maintenance > Cross Connect Resource Pane, the VT matrix port detail is inconsistent with the general VT matrix data. This can occur when a 1+1 protection scheme is in place. To avoid confusion, note that the VT matrix data counts the VTs for both the working and protect card, while the detail data counts the VTs only for the working card. This issue is resolved in Release 4.6.

DDTS # CSCdy10030

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

DDTS # CSCdy71653

A change of the alarm profile while alarms are present on a DS3 card is not correctly applied. The behavior is specific to DS3 ports on an ONS 15327 node. This issue will be resolved in Release 5.0.

DDTS # CSCdy49608

A node connection might fail during bulk circuit creation, causing the circuit creation to also fail. For example, this has been seen while creating 224 VT 1.5 protected circuits, on a path protection consisting of eight ONS 15327 nodes. If you experience a bulk circuit creation failure of this type, cancel the circuit creation batch, then delete any incomplete circuits. Restart the batch from the last successful circuit. This issue will be resolved in Release 5.0.

DDTS # CSCdx35561

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

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

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

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

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

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

This issue will not be resolved.

DDTS # CSCdy11012

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

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

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

If a firewall is enabled on any node in the network, then CTC will be unable to contact nodes outside of the initial OSPF areas. This issue will not be resolved.

DDTS # CSCdy37198

On Cisco ONS 15327 platforms equipped with XTC cross-connect cards, Ethernet traffic may be lost during a BLSR protection switch, with no accompanying alarm or condition raised. Possible affected circuits will be between Ethernet cards (E100T-4) built over Protection Channel Access (PCA) bandwidth on BLSR spans. When BLSR issues the switch, the PCA bandwidth is preempted. Since there is no longer a connection between the ends of the Ethernet circuit, traffic is lost. Further, in nodes equipped with XTC cards, the E100T-4 cards do not raise an alarm or condition in CTC. This issue will be resolved in a future release.

DDTS # CSCdw43896

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

Upgrades from Release 1.0

If you wish to upgrade from Release 1.0 to Release 4.1.x, you must first upgrade to maintenance Release 1.0.2. If you are already running maintenance Release 1.0.1 or better, you do not have to perform the intermediate upgrade.

DDTS # CSCds23552

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

Line Cards

DDTS # CSCef13110

DS1 and DS3 PMs on the XTC card are not marked Invalid for node time changes greater than ten seconds. Telcordia GR-253 requires that current PMs be marked invalid when the time change is over ten seconds. This issue is resolved in Release 4.6.

DDTS # CSCef40117

DS1 and DS3 PMs on the XTC card are not marked Invalid when the node time changes to midnight. The current interval should be changed to a yellow color to indicate that this interval is invalid once the node time changes. This issue is resolved in Release 4.6.

DDTS # CSCef40042

On an ONS 15327 the 1 day current interval for DS1 and DS3 PMs does not scroll over to the “Prev” interval if DST (Daylight Savings Time) is enabled on the node, the time is changed, and the date rolls over. This issue is resolved in Release 4.6.

DDTS # CSCef43718

Under the conditions listed below, the DS1 card does not raise Loss of Frame for a Mismatched Frame Format. This can happen when you change from the correct frame format to an incorrect frame format, where the correct format is Unframed and the incorrect format is D4, and you switch from the incorrect, to correct, and back to the incorrect format. This issue is resolved in Release 5.0.

DDTS # CSCef18088

A DS1 AINS circuit might change to IS state after two-fiber BLSR switch on a mixed-node network with one ONS 15327 and two ONS 15454s. This issue will be resolved in a future release.

DDTS # CSCed03215

The ONS 15327 XTC card allows soft reset immediately after a database change. After making any database change (for example, changing some provisioning) it is possible to soft reset the XTC card before the database change has been written to non-volatile memory. The result is that the most recent provisioning change might be lost. To avoid this issue, before soft resetting the XTC card, wait 2 minutes from the last provisioning change. This issue is resolved in Release 4.6.

DDTS # CSCec66218

A hard reset of the active XTC in a 1+1 configuration causes CTNEQPT-PBPROT to be raised in OC-3 trunk cards and OC-12 line cards. The hard reset also causes UNEQ-P to be raised in the OC-12 line cards. This issue is resolved in Release 4.6.

DDTS # CSCeb23183

On the ONS 15327 XTC, the j1 path trace values for the DS1 are incorrect. The table shows 28 entries, all with identical (but wrong) values, when an STS-1 (the only type that supports path trace on the XTC's DS1) only should have one entry. This can occur with an STS-1 circuit terminating at the XTC's DS1, in the DS1 maintenance card view of the XTC. To find the actual path trace values for the DS1 circuit, open the detailed circuit map for that circuit, right-click on the port image of the DS1, and select “j1 path trace.” This issue will be resolved in Release 4.6.

E Series and G Series Cards

DDTS # CSCdy41135

When using a G1000-2 card, TIM-P can be mistakenly raised on a PCA circuit after a protection switch. This occurs when path trace is enabled on a PCA circuit that is no longer in use after a protection switch. To work around this issue, either disable path trace or use alarm profiling to filter out the unwanted alarm. This issue will not be resolved.

DDTS # CSCdy63172

With E100/E1000 cards, a CARLOSS alarm present, and port alarms suppressed from CTC, Manual Alarm Suppression does not correctly suppress CARLOSS alarms. This issue is resolved in Release 4.6.

DDTS # CSCdy47038

G1000-2 path alarm profiles applied on port 2 are not updated to reflect the correct alarm severities. This issue will be resolved in Release 5.0.

DDTS # CSCdy13035

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

Path Protection Functionality

DDTS # CSCeb37707

With a VT path protection circuit, if you inject signals with a thru-mode test set into one path of the circuit in a particular order, you may not see the appropriate alarms. This can occur when you first inject LOP-P, then clear, then inject LOP-V. This issue will be resolved in Release 6.0.

BLSR Functionality

DDTS # CSCeb24331 and CSCeb40119

If you create a four-fiber BLSR with a VT circuit on it, then delete the circuit and the ring, then created a two-fiber BLSR on the same ports, you may see an unexpected AIS-V on the path, even before any additional circuit is created. A soft switch of the XTC will clear the AIS-V condition. This issue is resolved in Release 4.6.

DDTS # CSCdz35479

Rarely, CTC Network view can freeze following the deletion or addition of a node from or to a BLSR. This can result in the CTC Network view no longer updating correctly. If this occurs, restart CTC. This issue is resolved in Release 4.6.

DDTS # CSCdw66416

Traffic along a running ring segment cannot be restored while a participating node is rebooting. To see this problem, in a two fiber BLSR with circuits created along a given ring segment, you must isolate that ring segment by powering down two or more nodes where one of the nodes powered down is at the edge of the segment and the others are outside of the segment. Then power up and reboot the node at the edge of the segment. The circuits along this segment will not be restored even though the nodes on the segment are both up and running. You must restore power to all nodes before the traffic is restored. This issue will be resolved in Release 5.0.

BLSR Support for Mixed Node Networks

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

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 # CSCdz86121

In one rare case, the ONS 15454/15327 times out a user session without communicating the timeout to TL1. If this happens, the TL1 user remains logged in, although the session is actually timed out. This can occur when you log into the node with a timeout of X minutes. If the user session sits idle for all but 5 seconds of the X minutes, then you have only 5 seconds to type in a command to notify the node that the session is active. If you try this, you will likely miss the five second window, in which case the node will respond as though the session is inactive and deny access. However, because you have typed a key, irrespective of the five second window, TL1 responds as though the session is active and does not log you out (time out). You will not have access to the node and will receive a “DENY” response to TL1 commands. The error message may vary depending on commands issued. To recover from this situation, log out and log back in to TL1. This issue is resolved in Release 4.6.

DDTS # CSCdz26071

The TL1 COPY-RFILE command, used for SW download, database backup, and database restore, currently does not allow a user-selected port parameter to make connections to the host. The command expects the default parameter of Port 21 and will only allow that number. This issue will be resolved in Release 5.0

Performance Monitoring

DDTS # CSCdt10886

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

Documentation

G-Series Notes

The following two notes on page 5-30 of the Cisco ONS 15454 Reference Manual, R4.1 and R4.5 should be replaced.



Note

G-Series cards manufactured before August 2003 do not support DWDM GBICs. G1000-4 cards compatible with DWDM GBICs have a CLEI code of SNP8KW0KAB. Compatible G1K-4 cards have a CLEI code of WM5IRWPCAA.



Note

All versions of G1000-4 and G1K-4 cards support CWDM GBICs.

Resolved Software Caveats for Release 4.1.8

The following items are resolved in Release 4.1.8.

Maintenance and Administration

DDTS # CSCed76192

If a host on the same Ethernet as a given NE sends ARP requests to the NE, with a source address that is in a restricted address range (see below), the NE might reboot and other cards in the shelf reset. The NE might become unmanageable under these circumstances. The NE will install an ARP entry for the illegal IP address, with the MAC supplied in the ARP request, thereby misrouting important addresses.

Restricted addresses are those in the loopback network, 127.0.0.0/8, in the multicast networks, 224.0.0.0/4, and in the cell bus network, 192.168.100.0/24.

The workaround is to ensure that no legitimate hosts have addresses in the illegal networks, and that no compromised hosts that might generate ARP attacks are on the Ethernet. This issue is resolved in Releases 4.0.3, 4.6.2, 4.1.5, and 5.0.

DDTS # CSCee55443

In Releases 4.1.4 and 2.3.5, when TCC-B is the active shelf controller card, the NE will not send SNMP traps to the provisioned trap destinations. When TCC-A is the active shelf controller card, SNMP traps will be sent. This only occurs in software Releases 2.3.5 and 4.1.4. To work around this issue, make TCC-A the active shelf controller card. This issue is resolved in all releases other than Releases 4.1.4 and 2.3.5.

DDTS # CSCec86969

VT1 circuits might incur excessive traffic hits (greater than 50 ms) following a manual switch of the XTC. This issue is resolved in Release 4.1.4.

DDTS # CSCeb05404

PWR-A/B alarms can become stuck for an ONS 15327 node in the event of a transient power failure. The alarms will clear after resetting both XTCs. This issue is resolved in Release 4.6, and Maintenance release 4.1.4.

DDTS # CSCeb63327

The High Temperature Alarm is raised at 50 degrees Celsius. This is, however, not optimal on an Itemp rated system, which can tolerate up to 65 degrees Celsius. To work around this issue, the alarm can be downgraded or suppressed, but note that this will result in no temperature alarm provided at all. Alternatively, Cisco TAC provides a method of retrieving the temperature from the node, which can thus be monitored periodically for temperature-related problems. This issue is resolved in Release 4.6, and Maintenance release 4.1.3.

DDTS # CSCec84338

With multiple unnamed circuits (circuit name listed as “Unknown”) on a node, where at least one is a path protection circuit, a cross-connect from one of these unnamed circuits will incorrectly appear on the Circuit Edit > Path Protection Selectors, and Circuit Edit > Path Protection Switch Counts tabs of the other unnamed circuits. Also, the State tab will show paths in the wrong column (for example, both source and destination in the CRS End B column).

This issue can manifest anytime you create multiple unnamed circuits (via TL1 or from CTC using the TL1-like option) on a node, where at least one is a path protection circuit. This issue is resolved in Release 4.6 and maintenance Releases 4.1.1 and 4.1.3.

DDTS # CSCec20521

After addition and deletion of a static route that overlaps with the internal IP addresses range, all cards in the shelf reboot. This can also happen after the node learns a similar route through OSPF or RIP updates. This issue is present in all releases through 4.1 and 4.5. To avoid this issue, do not provision static routes with a destination address in the subnet range 192.168.190.x, and avoid overlap between IP addresses in the network and the internal subnet range 192.168.190.x. If the issue does occur, reset your TCCs. This issue is resolved in Release 4.6 and in maintenance Release 4.1.3.

DDTS # CSCec16812

UNEQ-V alarms are incorrectly raised prior to connecting a TAP to a TACC, and also after disconnecting the TAP from the TACC. This issue is resolved in Releases 4.1.3 and 4.6.

DDTS # CSCdy38603

VT Cross-connects downstream from a DS1 can automatically transition from the OOS-AINS state to the IS state even though the DS1 signal is not clean (for example, when there is an LOS present). This can occur when you have created a VT circuit across multiple nodes with DS1s at each end, and you have not yet applied a signal to the DS1 ports, and then you place the DS1 ports in OOS-AINS, OOS-MT, or IS. When you then place the circuit in OOS-AINS, the circuit state changes to IS (within one minute). This issue is resolved in Release 4.1.

Line Cards

DDTS # CSCeg52788

When a DS1 port on the XTC card (ONS 15327) or the on the DS1 card (ONS 15454) is configured as ESF frame format, and is connected to external DS1 equipment that transmits a malformed Performance Report Message (PRM) on the Facility Data Link (FDL), the XTC or DS1 card cannot manage the malformed PRM and will reset each time it receives one (so the symptom of this issue is multiple repeated resets on an XTC or DS1 card configured for ESF). To avoid this issue, change the frame format from ESF to Unframed on the DS1 ports on the ONS 15327 or ONS 15454. This allows you to keep your settings on the external DS1 equipment and not lose traffic. Some functionality of alarms, such as LOF, or of any line PMs that look into the DS1 header for information will be lost, however, in this method of avoiding an XTC/DS1 reset. This issue is resolved in Releases 4.1.7 and 5.0.

DDTS # CSCed06531

Malformed IP packets can potentially cause the XTC, TCC/TCC+/TCC2 and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to reset at the same time. This issue is resolved in Release 5.0, and maintenance Releases 4.1.4, 2.3.5, 4.0.3, and 4.6.2.

DDTS # CSCed86946

Malformed ICMP packets can potentially cause the XTC, TCC/TCC+/TCC2 and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to reset at the same time. This issue is resolved in Release 5.0, and maintenance Releases 4.1.4, 2.3.5, 4.0.3, and 4.6.2.

DDTS # CSCec88426, CSCec88508, CSCed85088

Malformed TCP packets can potentially cause the XTC, TCC/TCC+/TCC2, and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to reset at the same time. This issue is resolved in Release 5.0, and maintenance Releases 4.1.4, 2.3.5, 4.0.3, and 4.6.2.

DDTS # CSCec59739, CSCed02439, CSCed22547

The XTC, TCC/TCC+/TCC2 and TCCi/TCC2 control cards are susceptible to a TCP-ACK Denial of Service (DoS) attack on open TCP ports. The controller card on the optical device will reset under such an attack.

A TCP-ACK DoS attack is conducted by withholding the required final ACK (acknowledgement) for a 3-way TCP handshake to complete, and instead sending an invalid response to move the connection to an invalid TCP state. This issue is resolved in maintenance Releases 4.1.4, 2.3.5, 4.0.3, and 4.6.2.

DDTS # CSCec88402, CSCed31918, CSCed83309, CSCec85982

Malformed UDP packets can potentially cause the XTC, TCC/TCC+/TCC2, and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to reset at the same time. This issue is resolved in Release 5.0, and maintenance Releases 4.1.4, 2.3.5, 4.0.3, and 4.6.2.

DDTS # CSCea16455, CSCea37089, CSCea37185

Malformed SNMP packets can potentially cause the XTC, TCC/TCC+/TCC2 and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to reset at the same time. This issue is resolved in Release 4.6, and maintenance Releases 4.0.1, 4.0.3, and 4.1.3.

DDTS # CSCed05846

In Releases 4.0, 4.0.1, and 4.1 the standby TCC+, TCC2, or XTC card might reset automatically. This can occur at any time, but only rarely. This issue is resolved in Release 4.6, and maintenance Releases 4.1.1 and 4.1.3.

BLSR Functionality**DDTS # CSCdy48872**

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

To see this issue, on a node participating in a two fiber BLSR with PCA circuits terminating at the node over the two fiber BLSR, cause an SF-R by failing the receive fiber in one direction (say, west). Then, issue a lockout span in the other direction (in our example, east). Since the lockout span has higher priority than the SF-R, the ring switch should clear and PCA traffic should be restored on spans without a fiber fault. The ring switch does clear, but PCA traffic does not restore. To correct this issue, clear the fiber fault. All traffic restores properly. This issue is resolved in Release 4.1.

DDTS # CSCdy65890

If you have PCA circuits over two-fiber or four-fiber BLSR protect channels, an incorrect auto-inservice transition occurs after traffic preemption. You may place the circuit back into the OOS-AINS state after the BLSR has returned to the unswitched mode, using the Circuit Editing pane of the CTC. This issue is resolved in Release 4.1.

Path Protection Functionality

DDTS # CSCec04550

In a path protection configuration, upon detecting a double-path failure with UNEQ-P, the UNEQ-P on the protect path is not reported. This issue is resolved in Release 4.1.3.

DDTS # CSCec14995

In a non-revertive path protection configuration, when a double failure is detected on both paths with UNEQ-P or AIS-P, upon clearing the protect path defect, the UNEQ-P or AIS-P alarm may remain stuck on the working path for the node. The most reliable way to remove the alarm is a TCC side switch. This issue is resolved in Release 4.1.3.

DDTS # CSCea23862

After you perform a force switch on one of the spans of a DRI or IDRI topology with path protection-DRI circuits present, if you then apply a clear on the same span, the state will not show up immediately in CTC. This issue is resolved in Release 4.1.

TL1 Functionality

DDTS # CSCed10618

If the TL1 craft port is disconnected while a retrieve level user (or a user with no timeout) is logged in, and there is a currently active CTC session, then the active TCC will reset. To avoid this, log the craft access user out before disconnecting the TL1 craft port. This issue is resolved in Release 4.6 and in maintenance Release 4.1.4.

DDTS # CSCed22816

The TL1 "COPY-RFILE" command fails when executed on an ENE through an ONS 15454 GNE. This issue occurs when a Checkpoint firewall is between the FTP server and the GNE. The 'COPY-RFILE' will work properly when executed on the GNE but fails when executed on the ENE with an ONS 15454 GNE. The workaround is to stop FTP protocol monitoring on the

Checkpoint firewall when the FTP client is a GNE and the FTP server is the COPY-RFILE server. This issue is resolved in Release 4.1.4.

DDTS # CSCec21039

Rarely, the TL1 craft port on the ONS 15327 XTC card may not respond to data sent to the port after a power cycle. A reset initiated from CTC may clear the problem. This issue is resolved in Releases 4.1.3 and 4.6.

DDTS # CSCdz79471

The default state, when no PST or SST inputs are given for The TL1 command, RMV-<MOD2_IO>, is OOS instead of OOS-MT. Thus, if you issue a RMV statement, followed by maintenance-state-only commands, such as OPR-LPBK, the maintenance state commands will not work, since the port will be in the out-of-service state (OOS), instead of the out-of-service maintenance state (OOS-MT). To work around this issue, place ports in the OOS-MT state, by specifying the primary state as OOS and a secondary state of MT in either the RMV-<MOD2_IO> command or the ED-<MOD2_IO> command.

Scripts that depend on the RMV-<MOD2_IO> command defaulting to OOS-MT without specifying the primary and secondary states should be updated to force the primary and secondary state inputs to be populated. This issue will be resolved in Release 4.1.

DDTS # CSCea03186

The TL1 command, INH-USER-SECU, does not disable the userid appropriately. The command should disable the userid until the corresponding ALW-USER-SECU command is issued; however, the userid is automatically re-enabled after the user lock-out period expires. The user lockout period is set from the CTC. This issue will be alleviated in Release 4.1 by removal of the ALW-USER-SECU and INH-USER-SECU commands. The commands are reinstated correctly in Release 4.1.

New Features and Functionality

This section highlights new features and functionality for Release 4.1.x. For detailed documentation of each of these features, consult the user documentation.

New Software Features and Functionality

Open Ended Path Protection

In previous releases, you could create an end-to-end path protection circuit on any Cisco ONS 15XXX network using A-Z provisioning of CTC/CTM. This feature requires you to specify one source node and one destination node of a path protection circuit. CTC/CTM requires these nodes to be part of the network that is discovered by CTC/CTM.

With Release 4.1.x you can create an open ended path protection circuit in addition to a regular path protection. An open ended path protection circuit is a partial path protection circuit. This feature helps you create end-to-end path protection circuits where a part of the given path protection circuit is on a Cisco 15XXX network, while the other part of the circuit is on another vendor's equipment. The circuit may consist of one source point and two end points. There are two paths from the source; one path is from the source to one end point and the other path is from the source to the other end point. The source has a bridge that sends the traffic on both paths. The end points do not have any selectors and may hand off the traffic to another vendor's equipment. For bidirectional circuits, the source also contains a selector for the reverse traffic from end points to source. Alternatively, open ended path protection can be used to create a circuit with two sources and one destination. In the unidirectional case, the destination node has a selector, and the source nodes have one-way connections.

NE Defaults

The NE defaults pane user interface is changed in Release 4.1.x as follows:

- The NE defaults pane now has a highlighted title at the top of the pane, indicating the last action taken by the user.
- If you import or export a file, the title shows the file name and the time of the action.
- If you load or apply a file to the node, the changes and the time of the action will be displayed.

User Privileges

As of Release 4.1.x, The following user privileges have changed:

- A Maintenance level user can back up the database and transfer a software package to the node.
- A Provisioning level user can delete and reset cards.

Protect Threshold Crossing Alarms

As of Release 4.1.x, BLSR/MS-SPR and path protection/SNCP protect thresholds at both the card and port level are inherited from the working card/port.

C-bit framing

To be compatible with certain legacy deployments, the DS3-12E card C bit detection algorithm has changed conjunction with Release 4.1.x through an FPGA change in the DS3-12E modules.

Gigabit Ethernet Transponder

The Gigabit Ethernet Transponder is a software enhancement to existing G-series Ethernet cards that allows these cards to support transponder functionality.

The following features support Gigabit Ethernet Transponder functionality for Release 4.1.x.

Facility Loopback

Facility Loopback is supported for Release 4.1.x transponder functionality.

This applies to all G-series cards (G1000-4 and G1K-4 on the ONS 15454 and G1000-2 on the ONS 15327).

Provisionable Flow Control Watermarks

Provisionable flow control watermarks are supported for Release 4.1.x. This capability enables the user to tune the flow control mechanism on the G-Series cards for some network applications.

This applies to all G-series cards (G1000-4 and G1K-4 on the ONS 15454 and G1000-2 on the ONS 15327).

Changed Alarms

The following alarms have changed as of Release 4.1.x.

**Note**

For SONET alarms that apply the ONS 15327, refer to the Alarm Troubleshooting chapter of the user documentation.

SONET CRITICAL Alarms

LOC is added in Release 4.1.x.

SONET MAJOR Alarms

OTUK-IAE is dropped in Release 4.1.x.

PLM-V is added in Release 4.1.x.

SQUELCHED is MJ in Release 4.0 but changed to NA in Release 4.1.x.

FEC-MISM is added in Release 4.1.x.

SONET MINOR Alarms

OTUK-TIM is MN in Release 4.0 but changed to NA in Release 4.1.x.

SONET NA/NR Conditions

ERFI-P-CONN is added in Release 4.1.x

ERFI-P-PAYLD is added in Release 4.1.x

ERFI-P-SRVR is added in Release 4.1.x

EXERCISE-RING-FAIL is added in Release 4.1.x

EXERCISE-SPAN-FAIL is added in Release 4.1.x

INTRUSION-PSWD is added in Release 4.1.x

LPBKFACILITY (G-Series) is added in Release 4.1.x

New TL1 Features

The following TL1 features are new for release 4.1.x. For detailed instructions on using TL1 commands, consult the TL1 Command Guide for Release 4.1.

Removed Commands

The following commands were dropped from Release 4.0.

REPT^ALM^SECU

ALW-USER-SECU

INH-USER-SECU

New Commands

The following command was added in Release 4.1.x.

CLR-COND-SECU

New Support

The following new support has been added for Release 4.1.x.

- Facility loopbacks on G1000 are supported in Release 4.1.x.
- Escaped double quotes (“\””) was introduced in Release 4.1.x for Inner Strings (See Telcordia GR-831-CORE, Section 2.2.10) for GR compliance.
- In the command COPY-RFILE, DB backup and DB Download can be done by a MAINT user in Release 4.1.x (in addition to SUPERUSER).
- Negative MonLevels are accepted in Release 4.1.x.
- The command RTRV-COND-SYCN can be used with the ALL AID to suppress conditions with the same root cause. This behavior is enhanced in Release 4.1.x to display all Synchronization related conditions.
- The ED-BITS and RTRV-BITS commands now support the AIDs SYNC-BITS1 and SYNC-BITS2 for setting and retrieving the BITS-OUT port state.
- The parameter VOATTN, in ED/RTRV-OCH, has a range of -40 to +30.

The following BLSR ringid alarms are changed in Release 4.1.x to report on the OCn port.

- BLSROSYNC, MN, NSA, “BLSR Out Of Sync”—Always reported against the East working OCn facility of the BLSR.
- APSCNMIS, MN, NSA, “Node Id Mismatch”—Always reported against the working OCn facility that detects the mismatch.
- RING-MISMATCH, MN, NSA, “Far End Of Fiber Is Provisioned With Different Ring ID”—Always reported against the East working OCn facility of the BLSR.

Command Request changes

In the following command requests, the Release 4.0 request syntax appears first, followed by the new Release 4.1.x syntax.

ED-G1000 In Release 4.0:

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

ED-G1000 In Release 4.1.x:

ED-G1000:<TID>:<aid>:<CTAG>:::[MFS=<mfs>],[FLOW=<flow>],[LOWMRK=<lowmrk>],[HIWMRK=<hiwmrk>],[<pst>],[<sst>];

ED-T1 in Release 4.0:

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

ED-T1 in Release 4.1.x:

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

ED-T3 in Release 4.0:

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

ED-T3 in Release 4.1.x:

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

ED-EC1 in Release 4.0:

ED-EC1:[<TID>]:<aid>:<CTAG>:::[PJMON=<pjmon>],[LBO=<lbo>],[SOAK=<soak>]:[<pst>],[<sst>];

ED-EC1 in Release 4.1.x:

ED-EC1:[<TID>]:<aid>:<CTAG>:::[PJMON=<pjmon>],[LBO=<lbo>],[SOAK=<soak>],[SFBER=<sfber>],[SDBER=<sdber>]:[<pst>],[<sst>];

Command Response changes

In the following command responses, the Release 4.0 response syntax appears first, followed by the new Release 4.1.x syntax.

RTRV-USER-SECU response in Release 4.0:

“<uid>:,<uap>”

RTRV-USER-SECU response in Release 4.1.x:

“<uid>:,<uap>:LOGGEDIN=<loggedin>[,NUMSESSIONS=<numsess>],LOCKEDOUT=<lockedout>”

RTRV-G1000 response in Release 4.0:

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

RTRV-G1000 response in Release 4.1.x:

“<aid>::[MFS=<mfs>],[FLOW=<flow>],[LAN=<lan>],[OPTICS=<optics>],[TRANS=<trans>],[TPORT=<tport>],[LOWMRK=<lowmrk>],[HIWMRK=<hiwmrk>]:[<pst>],[<sst>]”

RTRV-T1 response in Release 4.0:

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

RTRV-T1 response in Release 4.1.x:

“<aid>::[LINECDE=<linecde>],[FMT=<fmt>],[LBO=<lbo>],[TACC=<tap>],[SOAK=<soak>],[SOAKLEFT=<soakleft>],[SFBER=<sfber>],[SDBER=<sdber>]:[<pst>],[<sst>]”

RTRV-T3 response in Release 4.0:

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

RTRV-T3 response in Release 4.1.x:

“<aid>::[LINECDE=<linecde>],[FMT=<fmt>],[LBO=<lbo>],[TACC=<tap>],[SOAK=<soak>],[SOAKLEFT=<soakleft>],[SFBER=<sfber>],[SDBER=<sdber>]:[<pst>],[<sst>]”

RTRV-OCH response in Release 4.0:

```
“<aid>:.,,[<status>]:[RDIRN=<rdirn>],[OPTYPE=<opticalPortType>],[OPWR=<power>],[EXPWLEN=<expWlen>],[ACTWLEN=<actWlen>],[ILOSS=<iloss>],[VOAMODE=<voamode>],[VOAATTN=<voaattn>],[VOAPWR=<voapwr>],[VOAREFATTN=<voarefattn>],[VOAREFPWR=<voarefpwr>],[REFOPWR=<refopwr>],[CALOPWR=<calopwr>],[NAME=<portname>],[SFBER=<sfber>],[SDBER=<sdber>],[ALSMODE=<alsmode>],[ALSRCINT=<alsrcint>],[ALSRCPW=<alsrcpw>],[COMM=<comm>],[GCCRATE=<gccrate>],[DWRAP=<dwrap>],[FEC=<fec>],[OSFBER=<osfber>],[OSDBER=<osdber>],[MACADDR=<macaddr>],[SYNCSMSG=<syncmsg>],[SENDDUS=<senddus>],[LSRSTAT=<lsrstat>],[SOAK=<soak>]:<pst>,<sst>”
```

RTRV-OCH response in Release 4.1.x:

```
“<aid>:.,,[<status>]:[RDIRN=<rdirn>],[OPTYPE=<opticalPortType>],[OPWR=<power>],[EXPWLEN=<expWlen>],[ACTWLEN=<actWlen>],[ILOSS=<iloss>],[VOAMODE=<voamode>],[VOAATTN=<voaattn>],[VOAPWR=<voapwr>],[VOAREFATTN=<voarefattn>],[VOAREFPWR=<voarefpwr>],[REFOPWR=<refopwr>],[CALOPWR=<calopwr>],[NAME=<portname>],[SFBER=<sfber>],[SDBER=<sdber>],[ALSMODE=<alsmode>],[ALSRCINT=<alsrcint>],[ALSRCPW=<alsrcpw>],[COMM=<comm>],[GCCRATE=<gccrate>],[DWRAP=<dwrap>],[FEC=<fec>],[OSFBER=<osfber>],[OSDBER=<osdber>],[MACADDR=<macaddr>],[SYNCSMSG=<syncmsg>],[SENDDUS=<senddus>],[LSRSTAT=<lsrstat>],[SOAK=<soak>],[SOAKLEFT=<soakleft>]:<pst>,<sst>”
```

RTRV-CLNT response in Release 4.0:

```
“<aid>:.,,<role>,<status>:[NAME=<portname>],[COMM=<comm>],[SFBER=<sfber>],[SDBER=<sdber>],[ALSMODE=<alsmode>],[ALSRCINT=<alsrcint>],[ALSRCPW=<alsrcpw>],[SYNCSMSG=<syncmsg>],[SENDDUS=<senddus>],[LSRSTAT=<lsrstat>],[CLEI=<clei>],[PN=<partnum>],[SN=<serialnum>],[VENDOR=<vendor>],[VENDORREV=<vendorrev>],[PLGTYPE=<plgtype>],[MACADDR=<macaddr>],[SOAK=<soak>]:<pst>,<sst>”
```

RTRV-CLNT response in Release 4.1.x:

```
“<aid>:.,,<role>,<status>:[NAME=<portname>],[COMM=<comm>],[SFBER=<sfber>],[SDBER=<sdber>],[ALSMODE=<alsmode>],[ALSRCINT=<alsrcint>],[ALSRCPW=<alsrcpw>],[SYNCSMSG=<syncmsg>],[SENDDUS=<senddus>],[LSRSTAT=<lsrstat>],[CLEI=<clei>],[PN=<partnum>],[SN=<serialnum>],[VENDOR=<vendor>],[VENDORREV=<vendorrev>],[PLGTYPE=<plgtype>],[MACADDR=<macaddr>],[SOAK=<soak>],[SOAKLEFT=<soakleft>]:<pst>,<sst>”
```

RTRV-OCN response in Release 4.0:

```
“<aid>:.,,<role>,<status>:[DCC=<dcc>],[TMGREF=<tmgref>],[SYNCSMSG=<syncmsg>],[SENDDUS=<senddus>],[PJMON=<pjmon>],[SFBER=<sfber>],[SDBER=<sdber>],[MODE=<mode>],[WVLEN=<wvlen>],[RINGID=<ringid>],[BLSRTYPE=<blsrtype>],[MUX=<mux>],[UNIC=<unic>],[CCID=<ccid>],[NBRIX=<nbrix>],[SOAK=<soak>]:<pst>,<sst>”
```

RTRV-OCN response in Release 4.1.x:

```
“<aid>:.,,<role>,<status>:[DCC=<dcc>],[TMGREF=<tmgref>],[SYNCSMSG=<syncmsg>],[SENDDUS=<senddus>],[PJMON=<pjmon>],[SFBER=<sfber>],[SDBER=<sdber>],[MODE=<mode>],[WVLEN=<wvlen>],[RINGID=<ringid>],[BLSRTYPE=<blsrtype>],[MUX=<mux>],[UNIC=<unic>],[CCID=<ccid>],[NBRIX=<nbrix>],[SOAK=<soak>],[SOAKLEFT=<soakleft>]:<pst>,<sst>”
```

RTRV-EC1 response in Release 4.0:

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

RTRV-EC1 response in Release 4.1.x:

```
“<aid>:.[PJMON=<pjmon>],[LBO=<lbo>],[RXEQUAL=<rxequal>],[SOAK=<soak>],[SOAKLEFT=<soakleft>],[SFBER=<sfber>],[SDBER=<sdber>]:<pst>,<sst>”
```

ENUM changes

The following enum items have changed for Release 4.1.x.

ALS_RESTART enum items added to Release 4.1.x:

ALS_RESTART_AUTO => "AUTO-RESTART"
 ALS_RESTART_MAN => "MAN-RESTART"
 ALS_RESTART_MAN_TEST => "MAN-TEST-RESTART"

MOD2 enum items added to Release 4.1.x:

MOD2_M2_G1000 => "G1000"

OPTICS enum items dropped from Release 4.0:

OPTICS_OP_IR => "IR"
 OPTICS_OP_LR => "LR"
 OPTICS_OP_SR => "SR"
 OPTICS_OP_VLR => "VLR"

OPTICS enum items added to Release 4.1.x:

OPTICS_OP_1000_BASE_CX => "1000_BASE_CX"
 OPTICS_OP_CWDM_1470 => "CWDM_1470"
 OPTICS_OP_CWDM_1490 => "CWDM_1490"
 OPTICS_OP_CWDM_1510 => "CWDM_1510"
 OPTICS_OP_CWDM_1530 => "CWDM_1530"
 OPTICS_OP_CWDM_1550 => "CWDM_1550"
 OPTICS_OP_CWDM_1570 => "CWDM_1570"
 OPTICS_OP_CWDM_1590 => "CWDM_1590"
 OPTICS_OP_CWDM_1610 => "CWDM_1610"
 OPTICS_OP_ITU_100G_1530_33 => "ITU_100G_1530_33"
 OPTICS_OP_ITU_100G_1531_12 => "ITU_100G_1531_12"
 OPTICS_OP_ITU_100G_1531_90 => "ITU_100G_1531_90"
 OPTICS_OP_ITU_100G_1532_68 => "ITU_100G_1532_68"
 OPTICS_OP_ITU_100G_1534_25 => "ITU_100G_1534_25"
 OPTICS_OP_ITU_100G_1535_04 => "ITU_100G_1535_04"
 OPTICS_OP_ITU_100G_1535_82 => "ITU_100G_1535_82"
 OPTICS_OP_ITU_100G_1536_61 => "ITU_100G_1536_61"
 OPTICS_OP_ITU_100G_1538_19 => "ITU_100G_1538_19"
 OPTICS_OP_ITU_100G_1538_98 => "ITU_100G_1538_98"
 OPTICS_OP_ITU_100G_1539_77 => "ITU_100G_1539_77"
 OPTICS_OP_ITU_100G_1540_56 => "ITU_100G_1540_56"
 OPTICS_OP_ITU_100G_1542_14 => "ITU_100G_1542_14"
 OPTICS_OP_ITU_100G_1542_94 => "ITU_100G_1542_94"

OPTICS_OP_ITU_100G_1543_73 => "ITU_100G_1543_73"
 OPTICS_OP_ITU_100G_1544_53 => "ITU_100G_1544_53"
 OPTICS_OP_ITU_100G_1546_12 => "ITU_100G_1546_12"
 OPTICS_OP_ITU_100G_1546_92 => "ITU_100G_1546_92"
 OPTICS_OP_ITU_100G_1547_72 => "ITU_100G_1547_72"
 OPTICS_OP_ITU_100G_1548_51 => "ITU_100G_1548_51"
 OPTICS_OP_ITU_100G_1550_12 => "ITU_100G_1550_12"
 OPTICS_OP_ITU_100G_1550_92 => "ITU_100G_1550_92"
 OPTICS_OP_ITU_100G_1551_72 => "ITU_100G_1551_72"
 OPTICS_OP_ITU_100G_1552_52 => "ITU_100G_1552_52"
 OPTICS_OP_ITU_100G_1554_13 => "ITU_100G_1554_13"
 OPTICS_OP_ITU_100G_1554_94 => "ITU_100G_1554_94"
 OPTICS_OP_ITU_100G_1555_75 => "ITU_100G_1555_75"
 OPTICS_OP_ITU_100G_1556_55 => "ITU_100G_1556_55"
 OPTICS_OP_ITU_100G_1558_17 => "ITU_100G_1558_17"
 OPTICS_OP_ITU_100G_1558_98 => "ITU_100G_1558_98"
 OPTICS_OP_ITU_100G_1559_79 => "ITU_100G_1559_79"
 OPTICS_OP_ITU_100G_1560_61 => "ITU_100G_1560_61"

TRANS enum items added to Release 4.1.x:

TRANS_NONE => "NONE"
 TRANS_ONE_PORT_BI => "ONE-PORT-BI"
 TRANS_TWO_PORT_BI => "TWO-PORT-BI"
 TRANS_TWO_PORT_RX_ONLY => "TWO-PORT-RX-ONLY"
 TRANS_TWO_PORT_TX_ONLY => "TWO-PORT-TX-ONLY"

Alarms, Conditions, and Errors Changed in Release 4.1.x

The following conditions have been added for Release 4.1.x.

ERFI-P-CONN—Enhanced Remote Failure Indication, Path, Connectivity
 ERFI-P-PAYLD—Enhanced Remote Failure Indication, Path, Payload
 ERFI-P-SRVR—Enhanced Remote Failure Indication, Path, Server

The following error has changed for Release 4.1.x.

IDMS has changed from "Loopback Type Missing" to "Missing Internal Data."

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15327, Release 4.1.7*
- *Release Notes for the Cisco ONS 15454, Release 4.1.8*
- *Release Notes for the Cisco ONS 15454 SDH, Release 4.1.8*
- *Cisco ONS 15327 Software Upgrade Guide, Release 4.1*

Platform-Specific Documents

- *Cisco ONS 15327 Procedure Guide, Release 4.1*
- *Cisco ONS 15327 Reference Manual, Release 4.1*
- *Cisco ONS 15327 Troubleshooting Guide, Release 4.1*
- *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide, Release 4.1*
- *Cisco ONS 15327 Product Overview, Release 4.1*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2007 Cisco Systems, Inc. All rights reserved.