



Release Notes for Cisco ONS 15454 SDH Release 7.2

May 2006

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15454 SDH multiplexer. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to the “Release 7.2” version of the *Cisco ONS 15454 DWDM Installation and Operations Guide*; and the “Release 7.2” version of the *Cisco ONS 15454 SDH Procedure Guide*; *Cisco ONS 15454 SDH Reference Manual*; *Cisco ONS 15454 SDH Troubleshooting Guide*; and *Cisco ONS 15454 SDH TL1 Command Guide*. For the most current version of the *Release Notes for Cisco ONS 15454 Release 7.2*, visit the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/ong/15454sdh/sdhrelnt/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 Caveats for Release 7.2, page 28](#)
- [New Features and Functionality, page 30](#)
- [Related Documentation, page 39](#)
- [Obtaining Documentation, page 40](#)
- [Documentation Feedback, page 41](#)
- [Cisco Product Security Overview, page 41](#)
- [Obtaining Technical Assistance, page 42](#)
- [Obtaining Additional Publications and Information, page 44](#)



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

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15454 SDH Release 7.2* since the production of the Cisco ONS 15454 SDH System Software CD for Release 7.2.

The following changes have been added to the release notes for Release 7.2.

Changes to Caveats

The following caveat has been added.

[CSCsd92505](#)

[CSCse85355](#)

[CSCsd52665](#)

[CSCsd56328](#)

Changes to New Features and Functionality

The following caution has been added:

[LMP Caution on page 35.](#)

Caveats

Review the notes listed below before deploying the ONS 15454 SDH. Caveats with tracking numbers are known system limitations that are scheduled to be addressed in a subsequent release. Caveats without tracking numbers are provided to point out procedural or situational considerations when deploying the product.

Hardware

CSCed18803

Rarely, the non-enhanced Muxponder unit does not pass Jitter Tolerance test from Trunk port to client port as per ITU-T G.825, 2 Mb/s mask, at the 10 Hz specific setpoint. The Muxponder should be configured with G.709 Off, FEC Off and Trunk signal provided by external Jitter test box, and the unit client port output monitored for errors, to see this issue. This issue will not be resolved. Note, however, that in normal network configurations the muxponder is operated with G.709 and FEC turned on, and the jitter tolerance tests pass.

CSCuk48503

Under specific conditions the non-enhanced MXPDP does not pass the Telcordia GR-253/G.825 Jitter generation mask test on 10G TX Trunk port. The 2.5 G TX Client jitter generation is always within mask and does not exhibit this issue. This occurs only when, in SONET mode, there is no FEC, no G.709, and

client interfaces are looped back, with non-synchronous clocking, and the jitter testbox TX connected to Trunk RX port, while the jitter testbox RX is connected to the Trunk TX port. The jitter testbox TX clock recovers from RX with an additional 5 ppm offset added. This issue will be resolved in a future hardware release.

CSCea78210

The TXP_MR_2.5G and TXPP_MR_2.5G cards do not support TX Optical power performance monitoring on the trunk port. To see this, go to the Optics Performance Monitoring tab of the TXP_MR_2.5G or TXPP_MR_2.5G card, and select the trunk port. TX Optical Pwr is not shown. This is as designed.

CSCdw92634

SDH DS3-I and E3 electrical cards only support a VC4 J1 trace string setting for all VC4s together. You cannot set the J1 byte for individual VC4s. This issue is a limitation of hardware.



Note

VC3 J1 strings can be set individually, but the optical cards cannot monitor the VC3 J1 string.

CSCdw14501

Interconnection Equipment failure alarms may be generated at 55 degrees C, and 72 volts. When the operating environment is at 55 degrees C and 72 volts, interconnection equipment failure alarms for the following cards can occur:

- STM16SH
- STM64LH
- STM16LH

The alarms could potentially occur on any of these boards, as well: OC48AS, GigE, OC192 or OC192LR. This issue will not be resolved.

Upgrades

CSCec42769 Database Corruption with ONS 15454 SDH Release 4.0, 4.0.1, 4.1



Caution

Before you upgrade to Release 7.x from Release 4.0, 4.0.1, or 4.1, you must read this caveat and run the SDH Circuit Repair Utility (VcCheck) provided on the software CD (also available on CCO).

The XCVXL card on the ONS 15454 SDH allows the intermixing of VC12 and VC3 payloads within a single VC4. When a VC4 contains only one VC12 tributary and at least one VC3 tributary and the VC12 is deleted, the database becomes corrupt.

The database load process on the ONS 15454 SDH occurs during a TCC2/TCC2P reboot, TCC2/TCC2P protection switch, software activation, or database restore. When the database is loaded containing this corruption the load process fails, causing the corrupt database to be deleted from the TCC2/TCC2P flash

memory. The previous saved database is then loaded instead. When all saved databases on a TCC2/TCC2P contain the corruption, the TCC2/TCC2P will load with the default provisioning, and all existing provisioning will be lost.

If this issue occurs you will see a loss of either some or all provisioning after a TCC2/TCC2P switch or reset.

To ensure that your network is not vulnerable to this issue, you must first determine if the issue already exists within your network, and if so, correct it. You can detect the issue by using the SDH Circuit Repair Utility (VcCheck) provided on the ONS 15454 SDH Release 4.1.3, 4.6.x, 5.x, 6.x, or 7.x software CDs. The VcCheck tool is also available for download from CCO. Once you have alleviated immediate risk from the issue, you must upgrade to Release 7.x, Release 6.x, Release 5.x, Release 4.6.1, or maintenance Release 4.1.3 (or any later release) to avoid further risk.

The VcCheck utility and its associated README file (in the same directory with the tool) provide details on how to temporarily alleviate this issue before upgrading to a release in which the issue is resolved.

This issue is resolved in Releases 4.6 and later, and in maintenance Releases 4.1.3 and later (caveated herein because of the upgrade issue).

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.



Note

In releases prior to 4.6 you could independently set proxy server gateway settings; however, with Release 4.6.x and forward, this is no longer the case. To retain the integrity of existing network configurations, settings made in a pre-4.6 release are not changed on an upgrade to Release 7.x. Current settings are displayed in CTC (whether they were inherited from an upgrade, or they were set using the current GUI).

CSCsd47626

Bulk deletion of Low Order Server Trails can cause a TCC card to reset. To avoid this delete low order server trails one by one. This issue will be resolved in Release 8.0.

CSCsc64015

Rarely, in an STM 1+1 configuration with VC3 traffic from one E3 to another where the source node has a 1:1 protection group, if you perform a parallel upgrade from Release 5.0.2 to 7.0, E3 traffic might incur a 13.2 ms hit. This issue will be resolved in a Release 8.0.

CSCeh84908

A CTC client session can disconnect from an ONS node during simultaneous deletion of large numbers of VT level circuits (3000+). Connectivity to the node will recover without any user action. If the condition persists, restart the CTC session to reconnect. This issue is under investigation.

CSCin92246

When one of the underlying connections of a circuit moves to the Unlocked-disabled, failed state, CTC treats the Unlocked-disabled, failed state as out of service and interprets part of the circuit to be out of service, or Locked. However, this is incorrect, as none of the underlying connections is in a Locked state. The result is that the circuit state is displayed as Locked[Partial], even though all of the underlying connections are technically Unlocked. This issue will be resolved in Release 8.0.

CSCin90057

A signal degrade or signal failure is not reported when you inject bit errors into the line for an E3 card. To see the SD or SF, inject a code violation error instead. This issue will not be resolved.

CSCeh92201

When you create a bidirectional MS-SPRing-SNCP IDRI circuit using autorouting and select the PCA option for secondary spans, the circuit is created over working MS-SPRing spans and does not use PCA spans. To enforce the use of the PCA option, provision the circuit using manual routing. This issue will not be resolved.

CSCef53317

A traffic hit can occur during a clock reference switch. To see this issue, complete the following steps.

-
- Step 1** Set up two ONS 15454 SDH nodes with STM16 SNCP (call the nodes STM16-1 and STM16-2).
 - Step 2** Set up two ONS 15454 SDH nodes with MXP_MR_2.5G_10G (call the nodes MXP-1 and MXP-2).
 - Step 3** Place MXP-1 and MXP-2 in Transparent Termination Mode.
 - Step 4** Ensure that STM16-1 is connected to MXP-1 client 1.
 - Step 5** Ensure that STM16-2 is connected to MXP-2 client 1.
 - Step 6** Ensure that MXP-1 trunk is connected to MXP-2 trunk.
 - Step 7** Connect a traffic generator to MXP_MR_2.5G_10G Port 3 (client) of MXP-1 and feed a PRC clock.
 - Step 8** Set MXP-1 Clock Reference 1 to MXP_MR_2.5G_10G Port 3, leaving the other two clock references as INTERNAL.
 - Step 9** Provision circuits such that a combination of VC4-4C, VC12, VC3 and VC4 traffic flows between STM16-1 and STM16-2 through MXP-1 and MXP-2.
 - Step 10** Gradually inject increasingly negative frequency offset through the traffic generator, in steps of 3 ppm, where you perform the next decrement step only when the node returns to NORMAL state.
-

When the clock offset reaches around 17 ppm, Clock Reference 1 fails and MXP-1 switches to Clock Reference 2. During the clock switch a traffic hit might occur for less than one second. The same is behavior can occur when injecting positive frequency offset. This issue will not be resolved.

CSCuk49106

The amplifier gain set point shown by CTC and the actual measured amplifier gain differ. The following steps illustrate this issue.

-
- Step 1** Reduce the insertion loss of the span just before the amplifier.
 - Step 2** Execute the APC procedure.
-

The APC procedure does not check consistency between the gain set point and the real gain, but rather only verifies the amplifier total output power. As a workaround, manual setting can be performed to align these values, although the discrepancy does not impact the normal functioning of the amplifier. This issue will not be resolved.

CSCef54670

The SQUELCHED condition is not raised when a non-enhanced MXP card is in MS termination mode. To see this issue perform the following steps.

-
- Step 1** Set up one ONS 15454 SDH node with MXP_2.5G_10G (MXP-1).
 - Step 2** Provision MXP-1 Port 1 (client) with any payload.
 - Step 3** Set MXP-1 Port 1 (client) and Port 5 (trunk) to the UNLOCKED state.
-

LOS and LOS-P alarms are reported on MXP-1 Port 1 (client). The SQUELCHED condition is not reported on MXP-1 Port 1 (client) because AIS is sent out the client port instead. This is as designed.

CSCef05162

Clearing the displayed statistics for a port will also clear the displayed history for that port. Clearing the displayed statistics for all ports will also clear the displayed history for all ports. There is no warning message from the TCC2. If History information is to be retained, do not clear displayed statistics for any port without first documenting the displayed history information for the associated port. This issue will not be resolved.

CSCef29516

The ALS pulse recovery min value is 60 instead of 100. If this occurs, increase the value to 100. This issue will not be resolved.

CSCeb36749

In a Y-Cable configuration, if you remove the client standby RX fiber; a non-service affecting LOS is raised, as expected. However, if you then remove the trunk active RX fiber; a non-service affecting LOS-P is raised, but the previously non-service affecting LOS on the client port is now escalated to a service affecting alarm, in spite of no traffic having been affected. This issue will not be resolved.

CSCee82052

After setting the node time (either manually or via NTP) you must wait for the endpoint of the interval to be reached before the end time will reflect the recently-set node time. Until this has occurred, the date time stamp for the end of the retrieved interval remains 12/31/69. This issue will not be resolved.

CSCeb39359

When changing NE timing from External or Mixed to Line timing, a Transient IEF alarm might be reported against the standby XC10G. This issue will be resolved in a future hardware release.

CSCdz62367

When replacing a failed working E1-42 card in a 1:1 or 1:N protection configuration with the protect card carrying the switched traffic, bit errors, less than 50ms in duration, are possible on the activated protection card. This issue will not be resolved.

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. This issue will not be resolved.

CSCdx35561

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

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

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

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

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

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.

CSCdy57891

An LOP-P alarm can be inadvertently cleared by an LOS that is raised and cleared. On older STM-N cards, when an LOP condition and an LOS condition are both present on the input, an LOS will be raised. However, upon clearing the LOS with the LOP still present, the LOP alarm is not raised. An AIS-P condition will be visible. This issue will not be resolved.

CSCdw38283

If a node has one good BITS reference and is running in a normal state, and you configure a second BITS reference, then reconfigure the second reference within 30 seconds of applying the first configuration, the node will enter FAST START SYNC mode. To avoid this problem, wait a minute before configuring the second reference a second time. This issue is a hardware limitation, and there are no current plans to resolve it.

CSCdw23208

[Table 1](#) summarizes B1, B2, and B3 error count reporting for SDH optical cards. Note that not all reporting is done according to ITU specifications. In particular, ITU specifies error counts for B1 and B3 as the number of blocks with errors (refer to ITU-T G.826 for paths and ITU-T G.829 for RS and MS).

Table 1 Error Count Reporting

Specification/Card Comparison	B1	B2	B3
ITU Specification	block	bit	block
STM1	block	bit	block
STM4	bit	bit	bit
STM16 trunk	bit	bit	bit
STM16 AS	block	bit	bit
STM64	block	bit	bit
STM1-8	bit	bit	bit
STM4-4	bit	bit	bit

CSCdw82689

After creating 509 VLANs and provisioning many Ethernet circuits, Ethernet circuit provisioning can become very slow, or possibly fail. Ethernet traffic may also incur an outage of a few minutes. To avoid this problem, delete any VLANs that are created but not used, and do not recreate them. There is no resolution planned for this issue.

CSCdv10824: Netscape Plugins Directory

If you use CTC, JRE, and the Netscape browser with a Microsoft Windows platform, you must ensure that any new installation of Netscape uses the same Netscape directory as the previous installation did, if such an installation existed. If you install Netscape using a different path for the plugins directory, you will need to reinstall JRE so that it can detect the new directory.

“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.

Common Control and Cross Connect Cards

CSCec82148

Rarely, traffic hits can occur on TCC2/TCC2P card removal. To avoid this issue, remove the card quickly. To recover from this issue, soft reset the TCC2/TCC2P card. This issue will not be resolved.

Ethernet Polarity Detection

The TCC2/TCC2P does not support Ethernet polarity detection. The TCC+ and TCCI both support this feature. If your Ethernet connection has the incorrect polarity (this can only occur with cables that have the receive wire pairs flipped), the TCC+/I will work, but the TCC2/TCC2P will not. In this event, a standing condition, “LAN Connection Polarity Reverse Detected” (COND-LAN-POL-REV), will be raised (a notification will appear on the LCD, and there will be an alarm raised). This issue will most

likely be seen during an upgrade or initial node deployment. To correct the situation, ensure that your Ethernet cable has the correct mapping of the wire wrap pins. For Ethernet pin mappings, consult the user documentation.

Active Cross Connect or TCC2/TCC2P Card Removal

Active cross connect or TCC2/TCC2P cards should not be removed. If the active cross connect or TCC2/TCC2P card must be removed, to minimize network interruption you can first perform an XCVXL side switch and then remove the card once it is in standby, or you can perform a lockout on all circuits that originate from the node whose active cross connect or active TCC2/TCC2P will be removed (performing a lockout on all spans will also accomplish the same goal).



Caution

If you mistakenly remove an active cross connect or TCC2/TCC2P card and you subsequently lose traffic on some interface cards, you may need to physically reset these cards if they fail to regain traffic.

Optical IO Cards

CSCee17695 and CSCed26246

Rarely, an STM1-8 card might fail to read MFG EEPROM and will show MEA in CTC. This issue can be reproduced by power cycling the node several times, by quickly removing and reinserting a fuse, or when the fuse is removed for several minutes and then replaced; however, the issue is not likely to be due to the power cycling. If a card enters this state, remove and reseal it, or cycle power again to recover STM1-8 operation. This issue will not be resolved.

CSCdw44431

Cisco ONS 15454 optical cards are not provisioned for particular path labels (C2 bytes). Consequently, they cannot raise a PLM condition. However, the ONS 15454 electrical card that terminates traffic ensures that the C2 byte is correct for the type of traffic carried. If the C2 byte is incorrect, this card raises a PLM condition that is reported against the optical port of ingress. An optical card will not raise a PLM against traffic that passes through a node, though it will appear to raise a PLM against traffic with the wrong C2 byte that is terminated on an electrical card within the node. This issue will not be resolved.



Note

Optical cards do ensure that the C2 byte is nonzero (Equipped), and will raise a UNEQ condition if the C2 byte is 0 (Unequipped).

Electrical IO Cards

CSCse96077

On an IO port false TCAs that indicate line or traffic problems might be raised every 15 min after the 15 min pm report. There are no alarms with the associated ports. Traffic is not affected.

In Release 7.2, during a very short period when the defect is present (less than 1 sec), false TCAs might be raised. This can be reproduced by either removing and then reinserting the card, or by a small burst of defects.

The cards affected are: DS3i, DWDM, E1, E1_42, STM1-8, STM4-4, MRC-12, STM64XFP

There are two workarounds:

Place the affected ports in locked,disabled and then back to Unlocked. This clears the problem for the specific port on the card, but the traffic will be down during the period of locked,disabled.

Soft reset the card with problem ports. This clears the problem on all ports on the card.

Soft reset might cause a protection switch if any circuit path on the card, or any port on the card or the card itself is in a protection group. Note that the protection switch itself might cause a defect burst, which might introduce false TCAs. Before resetting the card, check if any circuit, port, or card is in a protection group. If there is SNCP, MSSP, 1+1 LMSP or 1:1/1:N protection on the card, lock the protection using a switch command (for example, LOCKOUT/LOCKON) available to users before you reset the card ensuring that no protection switch occurs during soft reset, and that traffic will not be affected. For a card with no protection type, simply soft reset the card and traffic will not be affected.

This issue will be resolved in a future release.

CSCsd71602

On a four node STM16 SNCP with E1-42 cards set up in a 1:N protection group on a single node, if slots 1, 2, and 4 are designated as working cards, with slot 3 as the protect card, and with circuits provisioned on slot 1 ports, and then you fail the working card on slot 1 and the protect card takes over, and finally you alter the protection group by first removing and then replacing the working card in slot 2, CTC might fail to deny on a subsequent attempt to delete the entire protection group, in spite of the need for the protect card to continue to manage the traffic for the failed card in slot 1. Deletion of the protection group should be denied, because it can result in a loss of traffic. This issue will be resolved in a future release.

CSCeg80233

Long traffic hits can occur on E1-42 when using cross connect FIT cards. This can occur when, on the FIT card, you toggle the 155 mhz clock going to the E1-42 cards to the off position. This issue cannot be resolved.

CSCeg81428

Rarely, a long traffic hit (117 ms) can occur on E1-42 after an XC side switch. In multinode BLSR setups, switching the cross connect cards repeatedly might cause traffic hits greater than 60 ms. To avoid this issue side switch the XC only when needed (and not repeatedly). This issue will not be resolved.

CSCeg19255

Rarely, DS3I VC3 traffic takes a hit greater than 60 ms during a cross connect card soft reset. This issue will not be resolved.

CSCef67059

Bit errors can occur on E1-42 line cards passing traffic, when other E1-42 line cards are initially inserted into adjacent slots. Specifically, inserting line cards into adjacent slots or 1:N protect slots (Slots 3 and 15) can cause hits on Ports 1-14. Also, when the card in the 1:N protection slot is passing traffic, inserting E1-42 line cards into adjacent slots can cause bit errors. The bit errors characteristically last less than 5 ms. After the card is inserted, no further bit errors occur. Ports 15-42 behave differently. No bit errors occur on a line card residing in a non-1:N slot if adjacent line cards are inserted. Bit errors will only occur for these ports if line cards are inserted into the 1:N protection slots (Slots 3 and 15). Bit errors might also occur if traffic passes through the 1:N protected slot, and you insert a line card into any other working slot. A future version of E1-42 hardware will resolve this issue.

Interoperability with SONET DS3i-N-12

When provisioning circuits in SDH to interoperate with SONET DS3i-N-12, you must create a VC4 containing VC3s as a payload in the exact order in which they will attach to port groups on the SONET side.

CSCea52722

With DS3-I cards in a 1:2 protection group, when the protect card is active and in the WTR condition, removing another working card from the protection group clears the WTR condition. To work around this issue, remove the working card from the protection group when the protect card is in the standby state. This issue will be resolved in a future release.

CSCdw80652

When one traffic card in a DS3I 1:N protection group is reset, and then another card is reset, there will be a loss of traffic on the second card, after the first card completes its reset, lasting until the second card completes its reset. This only occurs when the protect card tries to handle the traffic of a card that is resetting, and that card is carrying traffic because when it reset the protect card was carrying traffic for another card. This loss of traffic occurs because the protect card attempts to set its relays to handle the traffic of the working card, but the relays on the working card are also set to carry the traffic, and since the card is resetting, no software is running to switch its relays. This issue most frequently presents itself when testing a double-failure scenario: resetting two cards in a protection group. Wait until the first card completes its reset sequence before resetting the second card to prevent this problem. Configuring cards in 1:1 instead of 1:N protection should also avoid the problem. This issue will not be resolved.

DWDM Cards

CSCsd92505

Traffic hits of 100 ms to 300 ms might occur during an OPT-PRE or OPT-BST card software reset or firmware upgrade. This occurs only with cards displaying the vendor ID 1025 in the CTC node level inventory tab when the following conditions are present for the affected card.

- OPT-PRE
 - WorkingMode is set to Output Power and the Input Com Power value is less than -33dBm.
- OPT-BST

- WorkingMode is set to Gain with a Gain value of greater than 17 dB, and Input Com Power is less than -10 dBm (three channels at approximately -14 dBm).

This issue is resolved in Release 7.0.1 and all subsequent releases except for Release 7.2.

CSCeh22604

When an MXP_MR_2.5G card is in MIXED or ESCON mode, TCA and alarm optical thresholds of Tx power for laser bias are configurable for ESCON payload, though not supported. This issue will be resolved in the future release.

CSCei19148

When a port is placed in-service while the conditions necessary to squelch the port are present, as in when the trunk port on a DWDM card is OOS,DSBLD and a client port is placed in-service, the client will momentarily enable, emitting light, before squelching due to the trunk OOS,DSBLD condition. The pulse is approximately 500 ms. This issue will not be resolved.

CSCei87554

When using a 1GE payload over the TXP_MR_2.5G the IfInErrors counter does not report oversized, undersized, or CRC errored frames, but rather, reports frame coding only. This issue will not be resolved.

CSCsb47323

For MXP_MR_10DME-C and MXP_MR_10DME-L cards, an unexpected RFI condition might be raised along with an OTUK-BDI. When there is an LOS downstream, the node receives OTUK-BDI. Because of the placement of dual OTN and SONET wrappers, it can also receive an RFI. This issue will not be resolved.

CSCsb79548

A long traffic hit can occur when an active TCC2/TCC2P resets while an MXP_MR_10DME-C or MXP_MR_10DME-L card is rebooting.

This issue can be reproduced as follows:

-
- | | |
|---------------|---|
| Step 1 | 1. Set up two MXP_MR_10DME-C or MXP_MR_10DME-L cards, connected back-to-back in two different nodes, A and B. |
| Step 2 | 2. Ensure that Node A has two TCC2 cards; one is active, and the other is standby. |
| Step 3 | 3. Set up any kind of traffic between the two MXP_MR_10DME-C or MXP_MR_10DME-L cards. |
| Step 4 | 4. Soft reset the MXP_MR_10DME card in Node A, then soft reset the active TCC2/TCC2P. |
-

OTUK/ODUK-SD, FEC Uncorrected word alarms are raised on the trunk port. Traffic goes down and does not recover until the MXP_MR_10DME card is able to come up. It is not known when or if this issue will be resolved.

CSCsb94736

After a fault condition (trunk LOS or Y-cable switch) an MXP_MR_10DME card might fail to detect the login message and traffic might not start for some minutes (after multiple login trials). This can occur in an N-F configuration with MDS switch and MXP_MR_10DME distance extension on, where test equipment traffic is set to 2G Fibre channel (FC) full bandwidth occupancy and started. Stop traffic or keep bandwidth occupancy below 80% during the login phase to work around this issue. This issue will not be resolved.

CSCsb95918

All GFP related alarms are raised with their active severities on the standby card after a Y-Cable protection switch. When a DWDM card (with GFP support) in a Y-Cable protection group becomes standby as a result of a Y-Cable protection switch, the GFP alarms raised when the card was active retain their severities instead of assuming standby severities. The alarms can be seen in the alarm pane if not suppressed, or in the condition pane if suppressed. This issue will be resolved in a future release.

CSCsc36494

Manual Y cable switches with squelching turned off can cause a Fibre channel link with brocade switches to go down.

This issue can be reproduced as follows:

-
- Step 1** Set up MXP_MR_10DME cards so that they are Y cable protected. Squelching is provisioned to be off. Distance extension is turned on.
 - Step 2** The path between the working pair of Y cable protected cards, has no distance introduced. But the protect path has a delay of 800 km introduced.
 - Step 3** Start Fibre channel traffic with brocade switches.
 - Step 4** Perform user-initiated manual Y cable switches from CTC.
-

After a few switchovers, the FC link will go down. SIGLOSS and GFP-CSF alarms are seen on the CTC. Cisco recommends you provision squelching to be on when interworking with brocade switches. If for some reason, squelching must be off with brocade switches, Cisco recommends you use a FORCE command to perform Y cable switches. It is not known when or if this issue will be resolved.

CSCsc60472

CTC is not able to discover a TL1 OCHCC circuit provisioned over an ITU-T line card (ITU-T OC48/STM16 and ITU-T OC192/STM64). This issue can occur when, using the TL1 client interface, you create the OCHNC layer that will be used by the OCHCC circuit, then create the OCHCC connections that involve the ITU-T line cards. The result is an OCHNC and two OCHCC partial circuits, instead of an OCHNC and a single OCHCC complete circuit. This issue will not be resolved.

CSCsc14290

LOW communication between two nodes equipped with TXP-MR-10E and AIC-I cards does not work with TXP-MR-10E cards in line termination mode, G.709 enabled, GCC present on the trunk port, and LOW circuits created between the transponders and AIC-I; Cisco recommends that you use EOW instead. This issue will be resolved in a future release.

CSCsc58941

Trunk ports of the TXPP_MR_2.5G and MXPP_MR_2.5G can be in facility and terminal loopback at the same time. This can occur if you provision terminal loopback on the protected trunk port after putting the trunk ports in facility loopback. You can clear this condition by removing loopback provisioning on the trunk ports. This issue will be resolved in a future release.

CSCeh94567

Setting a Terminal loopback on an MXP-2.5G-10G trunk port causes OTUK alarms.

This can occur under the following conditions.

1. Two MXP-2.5G-10G cards are connected via the trunk ports.
2. The client ports are connected to respective STM16 line cards.
3. SDCC is enabled on the client ports and the line cards' STM16 port.
4. A terminal loopback is set on the MXP-2.5G-10G trunk port.

This terminal loopback causes OTUK-LOF and OTUK-IA alarms to be reported on both MXP-2.5G-10G trunk ports. This issue will not be resolved.

CSCef15415

RMON TCAs are not raised on the TXPP_MR_2.5G client port after a hardware reset. To see this issue, provision two nodes with TXPP_MR_2.5G (TXP-1 and TXP-2) as follows.

-
- Step 1** Connect the TXP-1 DWDM-A trunk to the TXP-2 DWDM-A trunk.
 - Step 2** Connect the TXP-1 DWDM-B trunk to the TXP-2 DWDM-B trunk.
 - Step 3** Create an external fiber loopback on the TXP-1 client.
 - Step 4** Connect the TXP-2 client to a traffic generator.
 - Step 5** Provision 1G FC payload on the TXP-1 and TXP-2.
 - Step 6** Ensure that traffic is running smoothly.
 - Step 7** Provision RMON thresholds using TL1 for all TXPP_MR_2.5G ports (client and trunks).
 - Step 8** Apply a hardware reset to the TXPP_MR_2.5G.
-

After the card reboots, only DWDM-A and DWDM-B (trunk) port RMON TCAs are raised in the CTC History pane. RMON TCAs for port 1 (client) are not raised. This issue will not be resolved.

CSCef15452

RMON TCAs are not raised when the RMON history is cleared on TXPP_MR_2.5G card. To see this issue, provision two nodes with TXPP_MR_2.5G (TXP-1 and TXP-2) as follows.

-
- Step 1** Connect the TXP-1 DWDM-A trunk to the TXP-2 DWDM-A trunk.
 - Step 2** Connect the TXP-1 DWDM-B trunk to the TXP-2 DWDM-B trunk.
 - Step 3** Create an external fiber loopback on the TXP-1 client.
 - Step 4** Connect the TXP-2 client to a traffic generator.
 - Step 5** Provision 1G FC payload on the TXP-1 and TXP-2.
 - Step 6** Ensure that traffic is running smoothly.
 - Step 7** Provision RMON thresholds using TL1 for all TXPP_MR_2.5G ports (client and trunks).
 - Step 8** While the traffic is running reset the RMON history by clicking the Clear button in the CTC Payload PM pane.
-

RMON TCAs are not raised for any port. This issue will not be resolved.

CSCef50726

Receive client fiber removal can cause a switch from the protect to the active in a TXPP_MR_2.5G. To see this issue, perform the following steps.

-
- Step 1** Set up two nodes with TXPP_MR_2.5G (call the nodes TXP-1 and TXP-2).
 - Step 2** Ensure that TXP-1 DWDM-A trunk is connected to TXP-2 DWDM-A trunk with a 100 Km span.
 - Step 3** Ensure that TXP-1 DWDM-B trunk is connected to TXP-2 DWDM-B trunk with a 0 Km span.
 - Step 4** Ensure that TXP-1 client has an external fiber loopback.
 - Step 5** Connect the TXP-2 client to a traffic generator.
 - Step 6** Provision TXP-1 and TXP-2 with FICON 1G payload.
 - Step 7** Ensure that traffic is running smoothly on the protected span.
 - Step 8** Remove the receive client fiber at the near end.
-

This causes the far end trunk to switch from protect to working span. Similarly, removal of the receive Client fiber at far end causes the near end trunk to switch from the protect to the working span. (Note that the traffic is already lost due to the receive client fiber pull.) To work around this issue, manually switch via CTC from the working to the protect span. This issue will not be resolved.

CSCef13304

Incorrect ALS initiation causes a traffic outage on an FC payload. This issue can be seen by performing the following steps.

-
- Step 1** Set up two nodes with TXPP_MR_2.5G (call these nodes TXP-1 and TXP-2).
 - Step 2** Connect the TXP-1 DWDM-A trunk to the TXP-2 DWDM-A trunk.
 - Step 3** Connect the TXP-1 DWDM-B trunk to the TXP-2 DWDM-B trunk.
 - Step 4** Provision the TXP-1 client with an external fiber loopback.
 - Step 5** Connect the TXP-2 client to a traffic generator.
 - Step 6** Ensure that TXP-1 and TXP-2 have 1G FC payload provisioned.
 - Step 7** Enable ALS on TXP-1 trunk port and set it to “Manual Restart.”
 - Step 8** When traffic is running, remove the receive and transmit fibers on TXP1 port 1 (client). Traffic goes down and shutdown on TXP-1 port 2 (trunk) displays “No.”
 - Step 9** Reconnect the fibers for TXP-1 port 1 (client).
-

ALS is now initiated on TXP-1 port 2 (trunk) and the laser shuts down. Traffic never comes back.



Note This issue is restricted to the TXPP_MR_2.5G card.

To recover from this situation, perform a manual restart or disable the ALS in this configuration. This issue will not be resolved.

CSCuk51184

When downloading Release 4.7 to nodes with Release 4.6 installed, The 15454-32MUX-O and 15454-32DMX-O report an AWG Temperature fail low alarm that subsequently clears. This also occurs when downgrading from Release 4.7 to Release 4.6, where the AWG Temperature alarm fail is high. This issue cannot be resolved.

CSCec22885

AS-MT is not enabled in Port 3 when a loopback is applied. To see this issue, on the TXPP card, make the following 3 changes before clicking Apply:

-
- Step 1** Change Port 2 to OOS-MT from IS.
 - Step 2** Change Port 3 to OOS-MT from IS.
 - Step 3** Change Port 2 to facility or terminal loopback.
-

Now, when you click Apply, CTC issues the error message: “Error applying changes to row2 peer trunk port must not be IS.” Port 3 is still IS and the loopback changes are not applied. You must place Port 3 in the OOS-MT state, apply the changes, and then change the loopback to recover.

This error occurs only when all three of the above changes are attempted at the same time.

To avoid this issue, first change both the trunk ports to OOS-MT, click Apply, and then place port 2 in loopback and click Apply again. This issue will not be resolved.

CSCed76821

With Y-cable provisioned for MXP-MR-2.5G cards, if you remove the client receive fiber on one side, the far end takes greater than 100 ms to switch away from the affected card. This issue will not be resolved.

CSCef44939

Under certain conditions you may be unable to provision an Express Order Wire (EOW) circuit using an MXP_2.5G_10G or TXP_MR_10G card trunk port. This can occur as follows.

-
- Step 1** Provision an MXP_2.5G_10G or TXP_MR_10G card within a node.
 - Step 2** Disable OTN.
 - Step 3** Provision DCC on both client and trunk ports.
 - Step 4** Go to the Network view **Provisioning > Overhead Circuits** tab.
-

During the EOW circuit provisioning only the MXP/TXP client ports are listed for the selection. This issue will not be resolved.

CSCuk51185

After a soft reset of an OSCM or OSC-CSM card, a CONTBUS-IO alarm is raised. This issue will not be resolved.

CSCuk50144

Neither E1 nor E2 circuits are available for EOW circuits on TXP_MR_2.5 TXT in Section and Line Termination mode. This issue will not be resolved.

CSCee45443

When the FICON bridge does not receive the expected number of idle frames between data packets it will transition to SERV MODE. The MXP-MR-2.5G should not be used in scenarios where there is a FICON Bridge in place. This issue will not be resolved.

CSCec40684

After a database restore TXPP trunk ports might report SF, resulting in a traffic outage. The SF occurs when you restore the database and then put the port OOS for DWDM cards; then the operating mode in the database is different from the current operating mode. To avoid this issue, either put the DWDM port OOS before restore the database, or, after restoring the database, reset the DWDM cards. This issue will not be resolved.

CSCec51270

Far end traffic does not switch in line termination mode with .G709 off. This can occur with non-revertive Y-cable, and DCC enabled, under certain specific conditions. To avoid this issue, turn on .G709 when in line mode. This issue will not be resolved.

CSCuk42668

TXP-MR-2.5G F1-UDC may not be passed through in a line-terminated configuration with OTN off. This can occur with clean, OC-3/STM-1, line-terminated traffic, with OTN disabled, when you create a D1-D3 tunnel, a D4-D12 tunnel, and an F1-UDC from client to client. This issue will not be resolved.

CSCuk42752

If you go to the Overhead Circuits Tab in network view and select any User Data, F1 or User Data D4-D12 circuit type, no nXP cards are available for selection in the Endpoints. However, user Data type circuits can still be made end-to-end (where “end-to-end” refers to external cards, such as AIC to AIC) if the nXP cards are put in Transparent mode. This issue will not be resolved.

CSCeb49422

With TXPP cards, a traffic loss up to six seconds can occur during a DWDM protection switch. This behavior may be exhibited during protection switches by certain third-party fiber channel switches due to loss of buffer credits resulting in a reconvergence of the fiber channel link. This issue will not be resolved.

CSCeb53044

The 2G Fiber Channel (FC) payload data type in the TXP_MR_2.5G and TXPP_MR_2.5G cards does not support any 8B/10B Payload PM monitoring. This is by design.

CSCeb32065

Once engaged, the ALR will not restart on the trunk lines of a TXP or TXPP card. This occurs whenever ALR engages on the trunk lines of a TXP or TXPP card and the recover pulse width is provisioned to less than 40 seconds. This is a function of the trunk laser turn-on time, and the limiting recovery pulse width will vary by card. To avoid this issue, provision the pulse width to 40 seconds or more. This issue will not be resolved.

CSCeb37346

Near end and far end PMs might increment simultaneously on TXPP-2.5G cards. This can occur when two nodes have TXPP-2.5G cards and two nodes have STM16 cards in a four node network, where both TXPP-2.5G cards have STM16 SFPs on them, and are in MS (Line Termination) mode. By default, the TXPP-2.5G cards are in Splitter protection: the first DWDM port is working and the second is protect. If you remove the receive fiber of the first DWDM port on one TXPP-2.5G card, both near and far end counts begin to increment. The far end counts should not increment in this case. This issue is seen only when the Txpd cards have G709 and FEC on. If the cards have G709 and FEC off, only the near end counts will increment, as expected.

CSCeb26662 and CSCea88023

With TXP-MR-2.5G cards, when the current 1 day Optics PM rolls over, the information is inaccurate. This issue will not be resolved.

CSCuk42588

With ALS mode configured as “Auto Restart” or “Manual Restart,” it is possible the ALS Pulse Duration Recovery time can be set to values out of ITU-T recommendation G.664. You can use values out of the range defined in ITU-T recommendation G.664 only in order to interoperate with equipment that lasers cannot turn on or off within the required pulse time. To stay within the specification, you can set this value to 2 seconds and up to 2.25 seconds.

CSCea81219

On the TXPP, the default value for Tx Power High for TCAs & Alarms is too high for the trunk ports. Since Tx Power TCA and Alarm are not supported for trunk ports, this caveat is for informational purposes only.

CSCeb24815

With TXP-MR-2.5G cards, ratios are calculated incorrectly after clearing statistics. This is because after you clear statistics the entire time period becomes invalid. Once the time period rolls over again, values will be reliable for the new period.

CSCeb27187

During a Y-Cable protection switch, the client interface sends 200,000 to 300,000 8B/10B errors towards the attached Catalyst 3550 switch. The switch reacts to this large amount of 8B/10B errors by reinitializing the interface and spanning tree. The end result is that a protection switch can lead to a 30-45 second traffic hit if the switch is running spanning tree (default mode). This is expected behavior.

CSCea87290

In a Y-Cable protection group, if GCCs are defined on both cards, both cards' active LEDs will be green. This is by design.

CSCeb12609

For the TXPP, attenuating Port 2 Rx signal, SD, and SF alarms are not declared before LOS-P is raised. This is due to the intrinsic design of the optical interface, which allows required BER performances with dispersion and OSNR penalties.

This can occur when Port 2 is in back to back or has low dispersions and high OSNR.

CSCea68773

The ACTV/STBY LED shows AMBER when a 2.5G transponder is first connected. The DWDM cards introduced a new design: When all the ports are OOS on a card, the card is considered to be in standby mode.

Data IO Cards

SONET and SDH Card Compatibility

Tables 2, 3, and 4 list the cards that are compatible for the ONS 15454 SONET and ONS 15454 SDH platforms. All other cards are platform specific.

Table 2 *SDH Data Cards that are SONET Compatible*

Product Name	Description
15454E-G1000-4	4 port Gigabit Ethernet Module - need GBICs
15454E-E100T-12	12 port 10/100BT Ethernet Module
15454E-E1000-2	2 port Gigabit Ethernet Module - need GBICs
15454E-ML100T-12	10/100 Mbps Ethernet card, 12 ports, RJ-45, L2/L3 switching, SDH/ETSI system, includes console cable
15454E-ML1000-2	1000 Mbps Ethernet card, 2 SFP slots, L2/L3 switching, SDH/ETSI system

Table 3 *SONET Data Cards that are SDH Compatible*

Product Name	Description
CE-1000-4	4 port 1000-Mbps Gigabit Ethernet module
CE-100T-8	8 port 10/100FE Ethernet Module
15454-G1000-4	4 Port Gigabit Ethernet
15454-E100T-G	10/100BT, 12 circuit, compatible w/ XC, XCVT and XC10G
15454-E1000-2-G	Gigabit Ethernet, 2 circuit, GBIC - G
15454-ML100T-12	10/100 Mbps Ethernet card, 12 ports, RJ-45, L2/L3 switching, SONET/ANSI system, includes console cable
15454-ML1000-2	1000 Mbps Ethernet card, 2 SFP slots, L2/L3 switching, SONET/ANSI system

Table 4 *Miscellaneous Compatible Products*

Product Name	Description
15454-BLANK	Empty slot Filler Panel
15454-GBIC-LX	1000Base-LX, SM or MM, standardized for 15454/327
15454-GBIC-SX	1000Base-SX, MM, standardized for 15454/327
15454-FIBER-BOOT=	Bag of 15 90 degree fiber retention boots

Table 4 *Miscellaneous Compatible Products (Continued)*

Product Name	Description
15454-SFP-LC-SX	1000BASE, SX, short-reach, multimode, small form factor pluggable (SFP), LC connectors
15454-SFP-LC-LX	1000BASE, LX, long-reach, single mode, SFP, LC connectors
15454-CONSOLE-02	Cable, console, ML-Series, RJ-11 plug to RJ-45 jack, 22in/55.9cm long, SONET/ANSI system
15454E-CONSOLE-02	Cable, console, ML-Series, RJ-11 plug to RJ-45 jack, 22in/55.9cm long, SDH/ETSI system

E1000-2/E100T

Do not use the repair circuit option with provisioned stitched Ethernet circuits. It is not known at this time when or if this issue will be resolved.

Single-card EtherSwitch

Each E100/E1000 card can be configured as a single-card EtherSwitch configuration to allow VC4-4c of bandwidth to be dropped at each card. The following scenarios for provisioning are available:

- VC4-4c
- VC4-2c, VC4-2c
- VC4-2c, VC4, VC4
- VC4, VC4, VC4, VC4

When configuring scenario 3, the VC4-2c must be provisioned before either of the VC4 circuits.

Multicard EtherSwitch

When deleting and recreating Ethernet circuits that have different sizes, you must delete all VC4 circuits provisioned to the EtherSwitch before you create the new circuit scenario. (See the preceding “Single-card EtherSwitch” section on page 6 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.

CSCed96068

If an ML-Series card running Software Release 4.6.2 or later is interoperating with an ML-Series card running Software Release 4.6.0 or 4.6.1, then the `pos vcat resequence disable` command must be added to the configuration of the ML-Series card running R4.6.2 or later.

CSCec52443

On an ML-series RPR ring circuit deletion or creation causes an approximately 200 ms traffic loss. Traffic loss is expected to be less than 50 ms for RPR. To avoid this issue, from the ML-series CLI, perform a “shutdown” on both ends of the circuit prior to circuit changes. This issue will not be resolved.

CSCec52372

You must issue a “shut” command to both ends of a POS circuit before placing the circuit OOS, and issue IS before a “no shut” command. Placing a POS circuit OOS without shutting down can cause long traffic hits. This issue will not be resolved.

CSCec51252

You must issue a “shut” on both ends of affected POS circuits before performing a maintenance action on those circuits. If a POS circuit is restored without first issuing the shut commands, traffic loss is greater than 50 ms. When a maintenance action is taken, one end of the circuits could come up before the other. During that time, traffic is lost because the other end is not up yet. This issue will not be resolved.

CSCeb25778

When a MAC-SA is seen for the first time, it is learned, but may age out in less than 5 minutes. If the same MAC-SA is seen again before the first ages out, the entry will age out after 5 minutes, as expected. This issue will not be resolved.

CSCin43669

Timer expiration can cause a system crash when you attempt to remove 250 Shared Packet Ring (SPR) subinterfaces using the “no int spr1” command, while Cisco Discovery Protocol (CDP) is also enabled. To avoid this issue, either turn off CDP, issue the command, and then turn CDP back on; or remove the SPR subinterfaces explicitly. This issue will not be resolved.

CSCea36829

The broadcast packet count is always 0 for the SPR interface. The ML100 and ML1000 hardware does not support counting broadcast packets. This issue will not be resolved.

CSCeb21996

When the POS interface is removed from SPR due to a defect, while SPR is configured in immediate mode, the defect type may not be reported. This only occurs if the defect is set and clears in less than 50 ms.

CSCdz49700

ML-series cards do not appear in the Cisco Discovery Protocol (CDP) adjacencies and do not participate in the Spanning-Tree Protocol. All packets are counted as multicast.

The ML-series cards always forward Dynamic Trunking protocol (DTP) packets between connected devices. If DTP is enabled on connected devices (which might be the default), DTP might negotiate parameters, such as ISL, that are not supported by the ML-series cards. All packets on a link negotiated to use ISL are always counted as multicast packets by the ML-series card, and STP and CDP packets are bridged between connected devices using ISL without being processed. To avoid this issue, disable DTP and ISL on connected devices. This functionality is as designed.

CSCdz68649

Under certain conditions, the flow-control status may indicate that flow control is functioning, when it is not. Flow-control on the ML-series cards only functions when a port-level policer is configured. A port-level policer is a policer on the default and only class of an input policy-map. Flow-control also only functions to limit the source rate to the configured policer discard rate, it does not prevent packet discards due to output queue congestion.

Therefore, if a port-level policer is not configured, or if output queue congestion is occurring, policing does not function. However, it might still mistakenly display as enabled under these conditions. To avoid this issue, configure a port-level policer and prevent output queue congestion. This issue will not be resolved.

CSCdz69700

Issuing a **shutdown/no shutdown** command sequence on an ML1000 port clears the counters. This is a normal part of the startup process and there are no plans to change this functionality.

CSCea01675

Packets without an 802.1q VLAN tag are classified as COS 0. This issue will not be resolved.

CSCin29274

When configuring the same static route over two or more interfaces, use the following command:

```
ip route a-prefix a-networkmask a.b.c.d
```

Where *a.b.c.d* is the address of the outgoing gateway, or, similarly, use the command:

```
ip route vrf vrf-name
```

Do not try to configure this type of static route using only the interface instead of the address of the outgoing gateway. This issue will not be resolved.

CSCin32057

If no BGP session comes up when VPN Routing/Forwarding (VRF) is configured and all interfaces have VRF enabled ensure that at least one IP interface (without VRF) is configured and add an IP loopback interface on each node. This issue will not be resolved.

CSCdy55437

The maximum MAC Address Learn Rate for the ML-Series cards is 1300 MAC addresses per second. This number varies based on the ML-Series control and forwarding plane loads. If the forwarding and control planes are heavily loaded, the maximum MAC Address Learn Rate could be as low as 100 MAC addresses per second. To correct a situation where an ML-Series card has stopped learning MAC addresses, reduce the load on these cards. This load limit is by design.

CSCdy47284

Oversize frames are not supported on ML100 Fast Ethernet ports. Oversize frames cause egress traffic to incur CRC, line, and fragment errors on these ports. To avoid this issue, do not send jumbo packets to ML far end ports. This is as designed.

Alarms

CSCed28167

When a VC_LOW_PATH_TUNNEL only contains unidirectional circuits, an AU-LOP critical alarm is raised. This can occur when a bidirectional tunnel goes through at least three nodes, and the AU-LOP alarm is shown on the intermediate node on the direction not used. Tunnels are bidirectional. If a tunnel does not have traffic in both directions, it will be alarmed. The alarm will be cleared when a bidirectional circuit is added to the tunnel. This issue will not be resolved.

CSCef63240

Rarely, an LP TIM alarm displays its severity as NR instead of MJ in CTC. This can occur when a VC3 circuit is created on Port 5 and IO has detected a VC4 PLM alarm. This issue will not be resolved.

CSCee29901

A CARLOSS alarm can take up to 3 minutes to be reported depend of the number of VLANs configured on a node. When the alarm does appear, if you clear this major alarm, the severity changes to minor, but then the alarm disappears. The alarm severity behavior will not be changed.

CSCse85355

The NE should report alarms or conditions on ingress port not on any internal ports. Alarm detected at the internal ports (TERM) side will be ingress map to the MON side. So the NE raises the STS-MON/VT-MON and STS-TERM/VT-TERM alarms or conditions on the STS-MON/VT-MON ports, irrespective of the actual detection port (MON or TERM). If the user wants the customized severity to be reflected for a specific STS/VT alarms, the alarm profile entities of both STS-MON and STS-TERM, if available, should be changed to the same severity.

CSCsd52665

The NE should report alarms or conditions on ingress port not on any internal ports. Alarm detected at the internal ports (TERM) side will be ingress map to the MON side. So the NE raises the STS-MON/VT-MON and STS-TERM/VT-TERM alarms or conditions on the STS-MON/VT-MON ports, irrespective of the actual detection port (MON or TERM). If the user wants the customized severity to be reflected for a specific STS/VT alarms, the alarm profile entities of both STS-MON and STS-TERM, if available, should be changed to the same severity.

CSCsd56328

The NE should report alarms or conditions on ingress port not on any internal ports. Alarm detected at the internal ports (TERM) side will be ingress map to the MON side. So the NE raises the STS-MON/VT-MON and STS-TERM/VT-TERM alarms or conditions on the STS-MON/VT-MON ports, irrespective of the actual detection port (MON or TERM). If the user wants the customized severity to be reflected for a specific STS/VT alarms, the alarm profile entities of both STS-MON and STS-TERM, if available, should be changed to the same severity.

MS-SPRing Functionality

CSCdz66275

When creating a MS-SPRing from the network view, the node default values for reversion are not initially used. To see this, starting with no preferences file, log into a node with CTC, and set the node default values for MS-SPRing reversion. Now, in Network view, use the MS-SPRing wizard to create a MS-SPRing. The node level default values are initially ignored while the wizard is still in operation. If you encounter this issue, you may need to change values as appropriate for your network while you are still using the MS-SPRing wizard. Once the wizard is finished, these values are saved to a preferences file and will be used henceforth. This issue will not be resolved.

CSCdw53481

Two MS-SPRings are not allowed to coexist. If you execute a manual ring switch command on one side of an MS-SPRing node and apply another manual ring switch command on other side of the node, the second manual ring switch command is rejected. This works as designed. The implementation complies with Telcordia GR-1230, R6-102.

CSCdx45851

On a four fiber MS-SPRing, restoring the database for all nodes at the same time could cause VC4-16c traffic to fail to switch. Do not restore the database for multiple nodes simultaneously. The proper procedure for restoring the database for multiple nodes is to restore one node at a time. This procedure is documented in the user documentation.

CSCdx19598

A rare hardware failure on an STM16AS card transmitter can trigger SEF on the receiving STM16AS card in a four fiber MS-SPRing (or BLSR) configuration. The BER calculations are suspended when SEF is detected, so SD or SF is never raised. Likewise SEF is not considered a signal failure condition like LOS or LOF, so a protection switch will not occur. If this occurs, use the CTC GUI to force a protection switch on the MS-SPRing (or BLSR). This issue will not be resolved.

CSCdv53427

In a two ring, two fiber MS-SPRing (or BLSR) configuration (or a two ring MS-SPRing or BLSR configuration with one two fiber and one four fiber ring) it is possible to provision a circuit that begins on one ring, crosses to a second ring, and returns to the original ring. Such a circuit can have protection vulnerabilities if one of the common nodes is isolated, or if a ring is segmented in such a way that two non-contiguous segments of the circuit on the same ring are each broken. There are two possible workarounds for this issue:

1. Manually route the circuit to avoid the “one circuit over two ring” routing scenario.
2. When routing the circuit automatically, select the Using Required Nodes/Spans option in the Circuit Routing Preference screen, then select the appropriate spans to avoid the “one circuit over two ring” routing scenario.

This issue will be resolved in a future release.

Database Restore on an MS-SPRing

When restoring the database on an MS-SPRing, follow these steps:

-
- | | |
|---------------|---|
| Step 1 | To isolate the failed node, issue a force switch toward the failure node from the adjacent east and west nodes. |
| Step 2 | If more than one node has failed, restore the database one node at a time. |
| Step 3 | After the TCC2/TCC2P has reset and booted up, ensure that the “MS-SPRing Multi-Node Table update completed” event has occurred for all nodes in the ring. |
| Step 4 | Release the force switch from each node. |
-

SNCP Functionality

CSCee53579

Traffic hits can occur in an unprotected to SNCP topology upgrade in unidirectional routing. If you create an unprotected circuit, then upgrade the unprotected circuit to a SNCP circuit using Unprotected to SNCP wizard, selecting unidirectional routing in the wizard, the circuit will be upgraded to a SNCP circuit. However, during the conversion, traffic hits on the order of 300 ms should be expected. This issue will not be resolved.

CSCeb37707

With a VT SNCP 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 not be resolved.

Active XCVXL or TCC2/TCC2P Card Removal

As in MS-SPRing, you must perform a lockout on SNCP before removing an active cross connect or TCC2/TCC2P card. The following rules apply to SNCP.

Active XCVXL cards should not generally be physically removed. If the active cross connect or TCC2/TCC2P card must be removed, you can first perform an XCVXL side switch or TCC2/TCC2P reset and then remove the card once it is in standby, or you can perform a lockout on all circuits that originate from the node whose active cross connect card or active TCC2/TCC2P will be removed (performing a lockout on all spans will also accomplish the same goal). No lockout is necessary for switches initiated through CTC or through TL1.

Performance Monitoring

CSCef28522

When you inject errors on a splitter protection card in the node's working port, CVL and ESL are incremented for the working and protect far end ports. This issue will not be resolved.

SNMP

SNMP Attribute Changes

The following SNMP attributes will be replaced in future releases, and will no longer be supported after Release 7.x.

- cMsDwdmIfMultiplexSectionRingDirection
- cMsDwdmIfTransportRingDirection
- cMsDwdmIfChannelRingDirection

Resolved Caveats for Release 7.2

This section highlights resolved caveats for Release 7.2.

Maintenance and Administration

CSCsc62845

When you try delete a provisionable patchcord (PPC) from the CTC Provisioning > PPC tab, sometimes CTC fails to refresh the screen and the PPC deletion appears to have failed. The workaround is to restart into CTC. This issue is resolved in a Release 7.2.

CSCsd65791

.Authentication fails with “Illegal Registry” error when you try to authenticate from Multi Layer Card to Server using TACACS+. This issue is resolved in this Release.

DWDM Cards

CSCsc56015

Extracting an MSTP card and inserting a different type of card in the same slot will result in an MEA alarm and APC DISABLE condition being raised. The APC DISABLE condition will not clear even if you insert the correct card. The workaround is to send a software reset to the active TCC. This issue is resolved in Release 7.2.

CSCsc55771

When two MXP_MR_10DME cards are interconnected through OC-192/STM-64 cross connects and traffic is up, if you hard reset one of the MXP_MR_10DME cards, the traffic might fail to recover. To recover traffic flow, place the client port in OOS,DSBLD state, delete the PPM then recreate it, and reprovision the port. This issue is resolved in Release 7.2.

CSCsc62581

A T-TX-PWR-MIN TCA is raised and a wrong receive optical power value (of -40 dB) is displayed after a card is reset. The alert and incorrect Rx value both clear in the next 15 min sample period. This issue is resolved in Release 7.0.1 and Release 7.2.

CSCsc54518

The OPT-BST amplifier card is in a LASER OFF state, even if input power is provided to all input ports. This issue only occurs with Release 7.0 and can be reproduced on a card with the amplifier turned on, in operating conditions (with lasers on) as follows.

-
- Step 1** From the card-level **Maintenance** tab set ALS Mode to **Manual Restart** and click **Apply**.
 - Step 2** Set **OSRI** to **ON** and click **Apply**. The amplifier turns off.

- Step 3** Set **OSRI** to **OFF** and click **Apply**. The amplifier stays turned off (this is expected, since in Manual Restart the lasers are turned back on by means of a Request Laser Restart command issued in CTC).
- Step 4** Select the **Request Laser Restart** check box in the **Maintenance** tab and click **Apply**.
-

The amplifier goes into APR for 9 seconds (correct), but after this it turns off; it should go into LASER ON state (State 4 at module level). If this issue occurs, change the card from manual restart to auto restart, then toggle OSRI ON and OFF. This issue is resolved in Release 7.2.

SNMP

CSCsc62801

For nodes configured in multishelf mode using the default LAN configuration, SNMP traps are not sent to the management system. To avoid this issue, provision any the DCN-connected node as “Socks proxy,” then, on such nodes add the following static route:

- Destination: 0.0.0.0
- Next hop: DCN Router
- Cost: 10
- Provision any non-DCN connected node as ENE.

A white paper/application note is in progress and can be requested from Cisco TAC. A documented solution is available in the *ONS 15454 DWDM Procedures Guide*.

TL1

CSCsc62784

The Calibration Tilt is not properly changed using the TL1 interface. The reference tilt is changed instead. This issue can be seen when you try to change the CALTILT parameter on amplifier cards using the ED-OTS command. To avoid this issue, use CTC. This issue is resolved in Release 7.2.

New Features and Functionality

This section highlights new features and functionality for Releases 7.0.x. For detailed documentation of each of these features, consult the user documentation.

New Hardware

Radio Access Network Support


Note

Release 7.2 software and TL1 documentation support the RAN-SVC card; however, the card itself is not yet available. Additional documentation for this card type, as well as an update to the release notes, will become available when the card is released in the future.

Release 7.2 adds support for the Cisco Radio Access Network (RAN) Optimization solution with the new Cisco ONS 15454 RAN-SVC card, which implements aggregation node functionality in a RAN.

A typical Radio Access Network (RAN) is composed of Base Transceiver Stations (BTSs) or Node Bs, of Base Station Controllers (BSCs) or Radio Network Controllers (RNCs), and of Mobile Switching Centers (MSCs). The traffic generated by a BTS or Node B is transported to the corresponding BSC or RNC across a network, referred to as the backhaul network. The interface between a BTS and a BSC in Global System for Communication (GSM) and Code Division Multiplex Access (CDMA) systems is called the Abis interface. The interface between a Node B and an RNC in a Universal Mobile Telecommunication System (UMTS) is called the Iub interface.

In RAN Optimization, the Cisco MWR 1941-DC-A router extends IP connectivity to a cell site and a BTS. The router provides bandwidth-efficient IP transport of GSM and UMTS voice and data bearer traffic, as well as maintenance, control, and signaling traffic, over a leased line backhaul network between the BTS and leased line termination and the aggregation node via compression (cRTP/cUDP) and packet multiplexing (PPP mux and Multilink PPP).

In the Cisco ONS 15454, the RAN-SVC card transmits and receives E1/T1 data streams (for Abis) and OC-3 data streams (for UMTS) via the cross-connect cards.

RAN-SVC Card

The RAN-SVC card performs circuit emulation and optimization on traffic from 3rd Generation Partnership Project (3GPP) RAN nodes and provides IP-based backhaul of the optimized traffic to other peer nodes. The RAN-SVC card, when combined with the T1-56 and OC-3 cards, provides a high-rack-density aggregation function for the Cisco RAN optimization solution. When the RAN-SVC is used along with a Cisco MWR-1941-DC-A, it provides transparent RAN aggregation and optimization services.

Optimized traffic is received by the RAN-SVC card from peer cell site routers on VT1.5 circuits via a cross connect card or from native GE ports on the RAN-SVC card. Optimized traffic can also be received on the Cisco ONS 15454 node over the OC-3 through OC-192 range of rate interfaces. The RAN-SVC reconstructs higher-rate data onto VT1.5 circuits and sends it back through the cross connect card. Reconstructed traffic is externally delivered to the 3GPP RAN nodes over DS1 and OC-3 interfaces.

The RAN-SVC card is a multiprocessor card. It consists of three traffic-forwarding CPUs and one service CPU, which performs the control plane function for the card. Each traffic forwarding processor is equipped with one front-side 10/100/1000 Gigabit Ethernet (GE) port, two OC-3 Packet over SONET (POS), two STM-1 backplane interfaces, and 42 T1 backplane interfaces. The service CPU is equipped with a Gigabit Ethernet, one ATM and one POS interface.

In the Cisco ONS 15454, the RAN-SVC card transmits and receives T1 data streams (for GSM applications) and OC-3 data streams (for UMTS applications) via the cross connect cards. For T1 connections (GSM and/or backhaul), up to 126 T1 interfaces from multiple T1-56 cards can be aggregated by the cross connect card to form two STS-1 data streams, which are directed to and

terminated on the RAN-SVC card. For OC-3 interfaces (POS and/or ATM), up to eight OC-3 interfaces from multiple OC-3 cards can be aggregated by the cross connect cards to form two STS-4 data streams, which are directed to and terminated on the RAN-SVC card as well.

The RAN-SVC card supports 1:N protection. This allows a single RAN-SVC protect card to protect up to nine working RAN-SVC cards. A RAN-SVC protect card can be installed in any slot and can protect working cards on either side of the shelf.

The RAN-SVC card supports SNMP version 1 and SNMP version 2c. It supports standard ONS MIBS, standard Cisco IOS MIBs, and the CISCO-IP-RAN-BACKHAUL-MIB.

For RAN-SVC slots, connectors, card-level indicators, and port-level indicators consult the user documentation.

New Software Features and Functionality

IEEE 802.17b Based Resilient Packet Ring (RPR)

With Release 7.2 the ML-Series card supports IEEE 802.17b based RPR (RPR). RPR, as described in IEEE 802.17, is a metropolitan area network (MAN) technology supporting data transfer among stations interconnected in a dual-ring configuration. The IEEE 802.17b spatially aware sublayer amendment adds support for bridging to IEEE 802.17.

RPR is well suited for transporting Ethernet over a SONET/SDH ring topology and enables multiple ML-Series cards to become one functional network segment. RPR overcomes the limitations of earlier schemes, such as IEEE 802.1D Spanning Tree Protocol (STP), IEEE 802.1W Rapid Spanning Tree Protocol (RSTP), and SONET/SDH, when used in this role.

In Release 7.2 and later, the ML-Series card supports IEEE 802.17b based RPR in addition to Cisco proprietary RPR. Some of the advantages of IEEE 802.17b based RPR over Cisco proprietary RPR include:

- Steering. Ring protection is accomplished through steering instead of wrapping. Steering is a more efficient way of routing around a failure.
- Dual-transit queues. Dual-transit queues offer more control in handling transit traffic.
- Best-effort traffic classifications. “Best Effort” and “EIR” traffic classifications improve distribution of traffic across a best-effort service class.
- Interoperability. Conformance to the IEEE 802.17b standard increases interoperability with third-party vendors.
- Built-in service provider support. RPR provides built-in operations, administration, and maintenance (OAM) support for service provider environments.

The following IEEE 802.17b based Resilient packet ring (RPR) features are supported for ML-series cards.

- Multiple data path features are supported:
 - Bridging is supported, as specified in the IEEE 802.17b spatially aware sublayer amendment.
 - Shortest path forwarding through topology discovery is supported.
 - Addressing. unicast, multicast, and simple broadcast data transfers are supported.
 - Bi-directional multicast frames flood around the ring using both east and west ringlets.
 - The time to live (TTL) of the multicast frames is set to the equidistant span in a closed ring and the failed span in an open ring.

- Multiple service qualities are supported:
 - Per-service-quality flow-control protocols regulate traffic introduced by clients.
 - Class A allocated or guaranteed bandwidth has low circumference-independent jitter.
 - Class B allocated or guaranteed bandwidth has bounded circumference-dependent jitter. This class allows for transmissions of excess information rate (EIR) bandwidths (with class C properties).
 - Class C provides best-effort services.
- Efficient design strategies increase effective bandwidths beyond those of a broadcast ring:
 - Clockwise and counterclockwise transmissions can be concurrent.
 - Bandwidths can be reallocated on non-overlapping segments.
 - Bandwidth reclamation. Unused bandwidths can be reclaimed by opportunistic services.
 - Spatial bandwidth reuse. Opportunistic bandwidths are reused on non-overlapping segments.
 - Temporal bandwidth reuse. Unused opportunistic bandwidth can be consumed by others.
- Fairness features ensures proper partitioning of opportunistic traffic:
 - Weighted fairness allows a weighted fair access to available ring capacity.
 - Aggressive fairness is supported.
 - Single Choke Fairness Supports generation, termination and processing of Single Choke Fairness frames on both spans.
- Plug-and-play automatic topology discovery and advertisement of station capabilities allow systems to become operational without manual intervention.
- Multiple features support robust frame transmissions:
 - Service restoration time is less than 50 milliseconds after a station or link failure.
 - Queue and shaper specifications avoid frame loss in normal operation.
 - Fully distributed control architecture eliminates single points of failure.
 - Operations, administration, and maintenance support service provider environments.

The following IEEE 802.17b based RPR features are not supported on the ML-series cards.

- EoMPLS
- IP forwarding
- Wrapping, the optional IEEE 802.17b protection scheme (Steering, the protection scheme mandated by the standard, is supported)
- Layer 3 routing

Advantages with SONET/SDH Circuits

The ML-Series cards in an RPR must connect directly or indirectly through point-to-point STS/STM circuits. The point-to-point STS/STM circuits are configured on the ONS node through CTC or TL-1 and are transported over the ONS node's SONET/SDH topology on either protected or unprotected circuits.

On circuits unprotected by the SONET/SDH mechanism, RPR provides resiliency without using the capacity of the redundant protection path that a SONET/SDH protected circuit would require. This frees this capacity for additional traffic. RPR also utilizes the bandwidth of the entire ring and does not block segments like STP or RSTP.

Redundant Interconnect Support

Ring interconnect (RI) is a mechanism to interconnect RPRs for protection from node failure. Protection is accomplished through redundant pairs of back-to-back Gigabit Ethernet connections that bridge RPR networks. One connection is the active node and the other is the standby node. During a failure of the active node, link, or card, the detection of the failure triggers a switchover to the standby node.

RI on the ML-Series Card

RI on the ML-Series card is supported only on Gigabit Ethernet. RI on ML-series is provisioned by identifying peer RPR MACs or station IDs as either primary or standby, and uses an OAM frame to flush the SAS table and MAC table at the add stations. RI on ML-series provides card-level redundancy when connected to a switch running EtherChannel. It also provides protection between individual RPRs, including:

- Two RPRs
- Two Cisco proprietary RPRs
- A Cisco proprietary ring and an 802.17 ring

For RPR and RI configuration applications and details consult the user documentation.

Network Circuit Automatic Routing Overridable NE Default

The Network Circuit Automatic Routing Overridable NE default makes it possible to set by default whether or not a user creating circuits can change (override) the automatic circuit routing setting (also provisionable as a default).

The new NE default supporting this feature is:

```
CTC.circuits.RouteAutomaticallyDefaultOverridable
```

This default works in combination with the existing circuit routing default:

```
CTC.circuits.RouteAutomatically
```

The overridable option enables network administrators to manage how circuits are created on a network-wide basis. For example, if the Automatic Circuit Routing default is set to FALSE (the check box is unchecked by default), then setting the Network Circuit Automatic Routing Overridable default to FALSE ensures that manual circuit routing is enforced for all users creating circuits (the default is not overridable by the user). When the Network Circuit Automatic Routing Overridable default is set to TRUE (the factory configured setting) users can click in the Automatic Routing check box to change the automatic routing setting if they wish.

When the Route Automatically check box is not selectable during circuit creation, the following automatic routing sub-options will also be unavailable:

- Using Required Nodes/Spans
- Review Route Before Creation

Like the Automatic Circuit Routing default, the Network Circuit Automatic Routing Overridable default applies to all nodes in the network. The Route Automatically check box is either overridable or not depending on how the default is set for the node you are logged into through CTC. To ensure correct behavior after setting the default, propagate the chosen default setting to all nodes through which users might log into the network to perform provisioning. For more information on NE defaults and their provisioning consult the user documentation.

Fibre Channel and FICON Interface Interoperability Enhancements

Release 7.2 enhanced card mode interoperability features add string (port name) provisioning for each fiber channel and FICON interface on the FC_MR-4 to allow the Cisco Metadata Server (MDS) Fabric Manager to create a link association between a SAN port on a Cisco MDS 9000 switch and the FC_MR-4 SAN port.

Link Management Protocol



Caution

LMP is a leading edge feature, requiring specific equipment and network topology to function successfully. Contact Cisco Optical Product Line Marketing for an initial network needs evaluation and specific recommendations before deploying the LMP feature.

Release 7.2 supports Link Management Protocol (LMP). LMP is used to establish traffic engineering (TE) links between Cisco ONS 15454 nodes or between Cisco ONS 15454 nodes and selected non-Cisco nodes that use vendor-specific hardware.

LMP manages TE links between nodes through the use of control channels. TE links are designed to define the most efficient paths possible for traffic to flow over a network and through the Internet. Traffic engineering encompasses traffic management, capacity management, traffic measurement and modeling, network modeling, and performance analysis. Traffic engineering methods include call routing, connection routing, quality of service (QoS) resource management, routing table management, and capacity management.

LMP manages TE links between peer nodes, such as two optical cross-connect (OXC) nodes. Peer nodes have equivalent signaling and routing. LMP also manages TE links between a node such as an OXC and an adjacent optical line system (OLS) node. An example of an OLS node is an ONS 15454 DWDM node.

Networks with routers, switches, OXC, DWDM optical line systems (OLS), and add-drop multiplexers (ADM) use a common control plane such as Generalized Multiprotocol Label Switching (GMPLS) to provision resources and provide network survivability using protection and restoration techniques. LMP is part of the GMPLS protocol suite.

A single TE link can be formed from several individual links. Management of TE links can be accomplished with in-band messaging, as well as with out-of-band methods. For a pair of nodes that manage TE links, LMP accomplishes the following:

- Maintains control channel connectivity
- Verifies the physical connectivity of the data links
- Correlates the link property information
- Suppresses downstream alarms
- Localizes link failures for protection/restoration purposes in multiple types of networks

DWDM networks often use MPLS and GMPLS as common-control planes to control how packets are routed through the network. LMP manages the control channel that must exist between nodes for routing, signaling, and link management. For a control channel to exist, each node must have an IP interface that is reachable from the other node. Together, the IP interfaces form a control channel. The interface for the control messages does not have to be the same interface as the one for the data.

The LMP protocol is specified in an Internet-Draft, draft-ietf-ccamp-lmp-10.txt, which was published as a Proposed Standard, RFC 4204, (<http://www.ietf.org/rfc/rfc4204.txt>), on 2005-10-28.

For details about LMP network implementation, configuration, applications, troubleshooting, and procedures, consult the user documentation.

TL1

TL1 Command Changes

New Commands

The following new TL1 commands are added for Release 7.2.

- ED-LMP
- LMP-CTRL
- LMP-DLINK
- LMP-TLINK
- RTRV-PATH-OCH-TYPE

Command Syntax Changes

The syntax of the following commands is changed in Release 7.2.

ED-OTS syntax:

```
ED-OTS[:<TID>]:<aid>:<CTAG>[::RDIRN=<rdirn>],[VOAATTN=<voaattn>],[VOAPWR=
<voapwr>],[OFFSET=<offset>],[CALTILT=<caltilt>],[OSRI=<osri>],[AMPLMODE=<ampl
mode>],[CHPOWER=<chpower>],[EXPGAIN=<expgain>],[NAME=<name>],[SOAK=<soak
>],[CMDMDE=<cmdmde>][:<pst>[,<sst>]];
```

Is changed to:

```
ED-OTS[:<TID>]:<aid>:<CTAG>[::RDIRN=<rdirn>],[VOAATTN=<voaattn>],[VOAPWR=
<voapwr>],[OFFSET=<offset>],[REFTILT=<reftilt>],[CALTILT=<caltilt>],[OSRI=<osri>],[
AMPLMODE=<amplmode>],[CHPOWER=<chpower>],[EXPGAIN=<expgain>],[NAME=<n
ame>],[SOAK=<soak>],[CMDMDE=<cmdmde>][:<pst>[,<sst>]];
```

Command Response Changes

The following TL1 responses have changed in Release 7.2.

ED-POS response:

```
<aid>::[<adminstate>],[<linkstate>],[<mtu>],[<encap>],[<name>],[<soak>],[<soakleft>]:[<ps
t>],[<sst>]
```

Is changed to:

```
<aid>::[<adminstate>],[<linkstate>],[<mtu>],[<encap>],[<name>],[<soak>],[<soakleft>],[<rp
span>],[<edge>],[<jumbo>]:[<pst>],[<sst>]
```

TL1 ENUM Changes

TL1 ENUM Items Added or Removed

The following section, including [Table 5](#) through [Table 13](#), highlights ENUM items changed (added or removed) for Release 7.2, by ENUM type.

Table 5 *CARDMODE enum items added to Release 7.2*

Enum Name	Enum Value
CARDMODE_ML_IEEE_RPR	"ML-IEEE-RPR"

CARDMODE is used in the following commands:

- ED-EQPT
- ENT-EQPT
- RTRV-EQPT

Table 6 *DATALINK enum items added to Release 7.2*

Enum Name	Enum Value
DATALINK_COMPONENT	"COMPONENT"
DATALINK_PORT	"PORT"

DATALINK is used in the following command:

- LMP-DLINK

Table 7 *ENCAP enum items added to Release 7.2*

Enum Name	Enum Value
ENCAP_RPR_GFP_F	"RPR-GFP-F"

ENCAP is used in the following commands:

- ED-G1000
- ED-POS
- RTRV-FC
- RTRV-G1000

Table 8 *MOD2ALM enum items added to Release 7.2*

Enum Name	Enum Value
MOD2ALM_M2_LMP	"LMP"
MOD2ALM_M2_RPRIF	"RPRIF"

MOD2ALM is used in the following commands:

- RTRV-ALM-MOD2ALM
- RTRV-COND-MOD2ALM

Table 9 *MOD2B enum items added to Release 7.2*

Enum Name	Enum Value
MOD2B_M2_RPRIF	"RPRIF"

MOD2B is used in the following commands:

- ALS
- RTRV-ALM-ALL
- RTRV-ALM-BITS
- RTRV-ALM-EQPT
- RTRV-ALM-SYNCN
- RTRV-COND-ALL
- RTRV-COND-BITS
- RTRV-COND-EQPT
- RTRV-COND-SYNCN
- RTRV-PM-MOD2
- RTRV-TH-ALL
- RTRV-TH-MOD2

Table 10 MUXCAP enum items added to Release 7.2

Enum Name	Enum Value
MUXCAP_FIBER	"FIBER"
MUXCAP_LAMBDA	"LAMBDA"
MUXCAP_LAYER2	"LAYER2"
MUXCAP_PKTSWITCH1	"PKTSWITCH1"
MUXCAP_PKTSWITCH2	"PKTSWITCH2"
MUXCAP_PKTSWITCH3	"PKTSWITCH3"
MUXCAP_PKTSWITCH4	"PKTSWITCH4"
MUXCAP_TDM	"TDM"

MUXCAP is used in the following command:

- LMP-TLINK

Table 11 OPSTATE enum items added to Release 7.2

Enum Name	Enum Value
OPSTATE_ACTIVE	"ACTIVE"
OPSTATE_ACT_FAILED	"ACT-FAILED"
OPSTATE_CFG_RCV	"CFG-RCV"
OPSTATE_CFG_SND	"CFG-SND"
OPSTATE_DEGRADED	"DEGRADED"
OPSTATE_DOWN	"DOWN"
OPSTATE_GOING_DOWN	"GOING-DOWN"
OPSTATE_GOING_UP	"GOING-UP"
OPSTATE_INIT	"INIT"

Table 11 *OPSTATE enum items added to Release 7.2 (Continued)*

Enum Name	Enum Value
OPSTATE_TESTING	“TESTING”
OPSTATE_UNKNOWN	“UNKNOWN”
OPSTATE_UP	“UP”
OPSTATE_UP_ALLOC	“UP-ALLOC”
OPSTATE_UP_FREE	“UP-FREE”

OPSTATE is used in the following commands:

- ED-LMP
- LMP-CTRL
- LMP-DLINK
- LMP-TLINK

Table 12 *RPRSPAN_DIRN enum items added to Release 7.2*

Enum Name	Enum Value
RPRSPAN_EAST	“EAST”
RPRSPAN_WEST	“WEST”

RPRSPAN_DIRN is used in the following command:

- ED-POS

Table 13 *WDM_ROLE enum items added to Release 7.2*

Enum Name	Enum Value
ROLE_OLS	“OLS”
ROLE_PEER	“PEER”

WDM_ROLE is used in the following command:

ED-LMP

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15454 SDH, Release 7.0*
- *Release Notes for the Cisco ONS 15454, Release 7.2*
- *Release Notes for the Cisco ONS 15327, Release 7.2*
- *Release Notes for the Cisco ONS 15600, Release 7.2*

- *Release Notes for the Cisco ONS 15310-CL, Release 7.2*
- *Cisco ONS 15454 SDH Software Upgrade Guide, Release 7.2*

Platform-Specific Documents

- *Cisco ONS 15454 SDH Procedure Guide*
Provides installation, turn up, test, and maintenance procedures
- *Cisco ONS 15454 SDH Reference Manual*
Provides technical reference information for SONET/SDH cards, nodes, and networks
- *Cisco ONS 15454 DWDM Installation and Operations Guide*
Provides technical reference information for DWDM cards, nodes, and networks
- *Cisco ONS 15454 SDH Troubleshooting Guide*
Provides a list of SONET alarms and troubleshooting procedures, general troubleshooting information, and hardware replacement procedures
- *Cisco ONS SDH TL1 Command Guide*
Provides a comprehensive list of TL1 commands

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_inpk/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 © 2006, Cisco Systems, Inc.
All rights reserved.