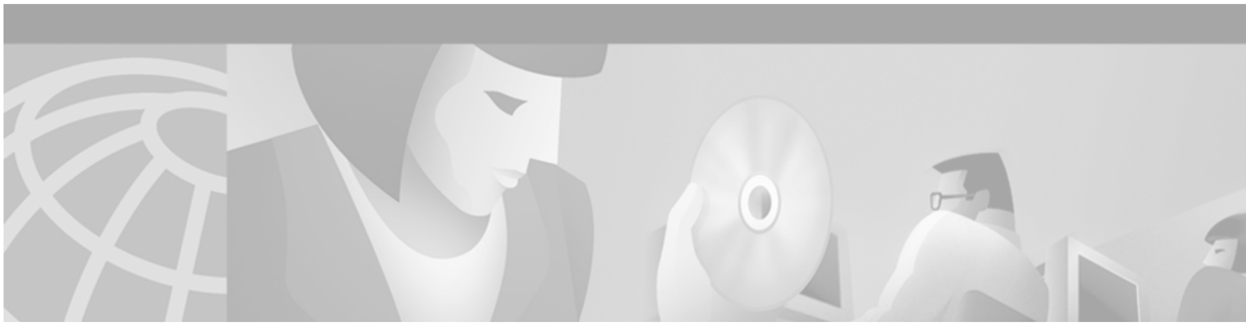

Release Notes for Cisco ONS 15454 Release 4.1.1

October 2007

Note

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

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15454 SONET multiplexer. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to the “Release 4.1.x and 4.5” version of the *Cisco ONS 15454 Procedure Guide*; *Cisco ONS 15454 Reference Guide*; *Cisco ONS 15454 Troubleshooting Guide*; *and Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide.* For the most current version of the *Release Notes for Cisco ONS 15454 Release 4.1.1*, visit the following URL:

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

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

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

Contents

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

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15454 Release 4.1.1* since the production of the Cisco ONS 15454 System Software CD for Release 4.1.1.

The following changes have been added to the release notes for Release 4.1.1.

Changes to Caveats

The following caveat has been added.

JRE Updates, page 12

Transmission Control Protocol Specification, page 12

Caveats

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

Hardware

CWDM and DWDM GBIC Compatibility with G1000-4 Cards and G1K-4 Cards

Existing G1000-4 cards are expected to support CWDM and DWDM GBICs, but final qualification testing was not complete at press time. The online version of the 4.1.x user documentation and release notes will be updated to reflect the final qualification status of CWDM and DWDM GBICs on the G1000-4 card, when this information is available.

Existing G1K-4 cards do not support CWDM or DWDM GBICs.

G1K-4 cards with the CLEI code of WM5IRWPCAA (manufactured after August 2003) are expected to support CWDM and DWDM GBICs, but final qualification testing was not complete at press time. The online version of the 4.1.x user documentation and release notes will be updated to reflect the final qualification status of CWDM and DWDM GBICs on the G1K-4 card with the CLEI code of WM5IRWPCAA, when this information is available.

Note Operating temperature of the DWDM GBICs is -5 degrees C to 40 degrees C.

DDTS # CSCdy48478 Fan Tray Assembly Fan Fail Lamp Test Failure

A user-initiated lamp test does not illuminate the fan fail LED on the fan tray assembly for the ONS 15454 or the ONS 15454 SDH. The lamp test successfully lights the LEDs for major, minor, and critical alarms on the fan tray, and for all cards in the chassis, but does not light the fan fail LED. An actual fan failure, however, will light the fan fail LED.

DDTS # CSCdw57215

In a configuration with OC-48 Any Slot cards and an STS-24c circuit, provisioned between G1000-4 cards with traffic going over the OC-48 span, extracting the G1000-4 card at one end of the STS-24c circuit before deleting the circuit will result in a traffic hit on all existing SONET circuits defined over that same span. This only occurs when the STS-24c is provisioned on timeslot 25.

In the *Cisco ONS 15454 Procedure Guide*, Release 4.1.x, refer to the "NTP-77 Delete Circuits" procedure to delete the 24c circuit before removing the card. Once you have deleted the circuit, refer to the "DLP-191 Delete a Card from CTC" task (also in the procedure guide) to delete the G1000-4 card. This issue will be resolved in Release 5.0.

Line Cards

Note Rarely, when the active TCC2 is removed, small traffic errors of 2 to 30 ms can sometimes occur. To avoid this issue, switch to the protect TCC2 before removing the working TCC2.

DDTS # CSCeb45064

Terminal loopback on DS3XM-6 card may not work properly. AIS-P may be transmitted towards the system (away from the line side) direction. A VT circuit newly created to the DS3XM-6 with no valid input signal to the port can cause this. A terminal loopback will not work because AIS-P is being transmitted towards the system direction. To avoid this issue, apply a valid signal to the input port for the DS3XM card for at least 10 seconds with no terminal or facility loopback applied to that particular port. After receiving a valid signal for this time period, the terminal loopback will function properly even if the input signal is disconnected from the DS3XM port. This issue will be resolved in Release 6.0.

DDTS # CSCdz49928

When using KLM type fuses with specific types of fuse and alarm panels, the PWR-REDUN alarm may not be displayed once the fuse is blown. A KLM fuse does not have a blown fuse indicator build into it. As a result, the blown fuse detection circuitry on the FAP may continue to provide voltage on its output despite a blown fuse.

Ethernet Polarity Detection

The TCC2 does not support polarity detection & correction on the LAN Ethernet port. This is a change from prior common control cards, such as the TCC+. If your LAN Ethernet connection has the wrong polarity (due to incorrect wiring on the backplane wire-wrap pins), the connection will work when using a TCC+, but not with a TCC2. To avoid possible problems, ensure that your Ethernet cable has the correct mapping of the backplane wire-wrap pins. For Ethernet pin mappings, consult the "DLP-A 21 Install LAN Wires on the Backplane" procedure in the user documentation.

If you are using a TCC+, the Release 4.0 or 4.1.x software will report the polarity issue (previous releases do not), by raising the standing condition: LAN Connection Polarity Reverse Detected (COND-LAN-POL-REV). Also, notification will appear on the fan tray LCD, which will display "BP LAN POL. NEG." The issue will typically be reported during the software upgrade process, but can also be raised during a new installation when using TCC+ and Release 4.0 or 4.1.x.

If this is a new installation with a TCC2 and you have the Ethernet polarity reversed, the TCC2 will not communicate over the LAN Ethernet interface (no polarity correction will occur), and no condition will be reported, nor will the fan tray LCD indicate an issue.

SONET and SDH Card Compatibility

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

Table 1 SDH Data Cards that are SONET Compatible

Product Name	Description
15454E-G1000-4	4 port Gigabit Ethernet Module - need GBICs
15454E-E100T-12	12 port 10/100BT Ethernet Module
15454E-E1000-2	2 port Gigabit Ethernet Module - need GBICs
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 2 SONET Data Cards that are SDH Compatible

Product Name	Description
15454-G1000-4	4 Port Gigabit Ethernet
15454-E100T-G	10/100BT, 12 circuit, compatible w/ XC, XCVT and XC10G
15454-E1000-2-G	Gigabit Ethernet, 2 circuit, GBIC - G
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 3 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
15454-SFP-LC-SX	1000BASE, SX, short-reach, multimode, small form factor pluggable (SFP), LC connectors

Table 3 Miscellaneous Compatible Products

Product Name	Description
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, 22Ý/55.9cm long, SONET/ANSI system
15454E-CONSOLE-02	Cable, console, ML-Series, RJ-11 plug to RJ-45 jack, 22Ý/55.9cm long, SDH/ETSI system

DDTS # CSCdw27380

Performing cross connect card switches repeatedly might cause a signal degrade condition on the lines or paths that can trigger switching on these lines or paths. If you must perform repeated cross connect card switches, lock out the corresponding span (path protection, BLSR, or 1+1) first. This issue will be resolved in Release 6.0.

LOS Behavior

When an OC-N card is seeing LOS and the problem is resolved (for example, the pulled fiber is reinserted) the LOS will normally clear quickly, and any other errors seen on the signal will be raised. However, in the special case where the restored signal is unframed, the LOS will remain raised (that is, the LOS will not be replaced by an LOF). This is standard SONET behavior per Telcordia GR-253 R6-57, Method 1, where to clear LOS the signal must also contain valid framing alignment patterns.

DDTS # CSCdw66444

When an SDH signal is sent into an ONS 15454 OC-12/STM-4 (IR, 1310 LR and 1550 LR) or an OC-48/STM-16 high-speed (IR and LR) port which has been configured to support SDH, an SD-P (Signal Degrade) alarm will appear as soon as the circuit is created. This alarm will continue to exist until the circuit is deleted.

To avoid this problem, when provisioning an OC-12/STM-4 (IR, 1310 LR and 1550 LR) or an OC-48/STM-16 high-speed (IR and LR) port to support SDH, disable the signal degrade alarm at the path level (SD-P) on the port.

Also, PM data at the path level will not be reliable. You must set associated threshold values to 0 in order to avoid threshold crossing alerts (TCA) on that port. The path threshold values to set to zero are CV-P, ES-P, SES-P, and UAS-P.

These issues are the result of a hardware limitation, and there are no current plans to resolve them.

DDTS # CSCdw09604

If you are using an XC10G with OC-48, you must use either OC-48AS or OC-48 cards with a revision number higher than 005D.

Jitter Performance with XC10G

During testing with the XC10G, jitter generation above 0.10 UI p-p related to temperature gradient testing has been observed. This effect is not expected to be seen under standard operating conditions. Changes are being investigated to improve jitter performance in a future release. DDTS numbers related to this issue include CSCdv50357, CSCdv63567, CSCdv68418, CSCdv68441, CSCdv68389, CSCdv59621, and CSCdv73402.

Active Cross Connect (XC/XC10G/XCVT) or TCC+/TCC2 Card Removal

You must perform a lockout in BLSR, path protection, and 1+1 before physically removing an active cross connect (XC/XC10G/XCVT) or TCC+/TCC2 card. The following rules apply.

Active cross connect (XC/XC10G/XCVT) cards should not generally be physically removed. If the active cross connect or TCC+/TCC2 card must be removed, you can first perform an XC/XCVT/XC10G side switch or TCC+/TCC2 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 or active TCC+/TCC2 will be removed (performing a lockout on all spans will also accomplish the same goal). No lockout is necessary for switches initiated through CTC or through TL1.

DDTS # CSCdv62565, CSCdv62573

In a 1:N protection group, traffic loss could occur if a DS-N card is preprovisioned and then added to the group while another working card in the group is removed from its slot. To avoid this, before adding slots to a protection group ensure that:

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

This issue will be resolved in Release 6.0.

E Series and G Series Cards

Note When using ONS 15327s as passthrough nodes with Release 3.2, you cannot create 9c or 24c gigabit Ethernet circuits through any 15327.

DDTS # CSCdy37198

On Cisco ONS 15454s equipped with XC or XCVT cross-connect cards, neither the E100T-12 nor the E1000-2 cards raise an alarm or condition in CTC when Ethernet traffic is predictably lost due to the following circumstances:

Circuits exist between Ethernet cards (E100T-12 and/or E1000-2) built over Protection Channel Access (PCA) bandwidth on BLSR spans. When BLSR issues a switch, the PCA bandwidth is preempted. Since there is no longer a connection between the ends of the Ethernet circuit, traffic is lost.

Note In nodes equipped with XC10G, these Ethernet cards will raise an AIS-P condition.

This issue will be resolved in a future release.

DDTS # CSCdr94172

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

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

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

Note A workaround for this issue is to use the port-mapped mode of the E-series cards.

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

Table 0-1 Protocols Added to the MAC Address Table

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

E1000-2/E100T

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

Single-card EtherSwitch

Starting with Release 2.2.0, each E100/E1000 card can be configured as a single-card EtherSwitch configuration to allow STS-12c of bandwidth to be dropped at each card. The following scenarios for provisioning are available:

1. 12c
2. 6c, 6c
3. 6c, 3c, 3c
4. 6c, six STS-1s
5. 3c, 3c, 3c, 3c
6. 3c, 3c, six STS-1s
7. Twelve STS-1s

When configuring scenario 3, the STS-6c must be provisioned before either of the STS-3c circuits.

Multicard EtherSwitch

When deleting and recreating Ethernet circuits that have different sizes, you must delete all STS circuits provisioned to the EtherSwitch before you create the new circuit scenario. (See the preceding "Single-card EtherSwitch" section on page 9 for details on the proper order of circuit creation.) Enable front ports so that the VLANs for the ports are carried by the largest circuit first. A safe approach is to enable the front port before you create any circuits and then retain the front port VLAN assignment afterwards. If you break the rules when creating a circuit, or if you have to delete circuits and recreate them again, delete all circuits and start over with the largest first.

DDTS # CSCds02031 E1000-2/E100

Whenever you drop two 3c multicard EtherSwitch circuits onto an Ethernet card and delete only the first circuit, you should not provision STS-1 circuits to the card without first deleting the remaining STS-3c circuit. If you attempt to create an STS-1 circuit after deleting the first STS-3c circuit, the STS-1 circuit will not work and no alarms will indicate this condition. To avoid a failed STS-1 circuit, delete the second STS-3c prior to creating any STS-1 circuit.

ML-Series

DDTS # CSCeb56287

When an ML-series circuit's state is provisioned from In-Service (IS) to Out-of-Service (OOS), and then back to IS, data traffic does not recover. To avoid this issue, prior to changing the state from IS, set the POS port to shut down on the CLI. After the state is changed back to IS from OOS, set the POS port to "no shutdown." This issue will be resolved in Release 4.6.

DDTS # CSCeb24757

Disconnecting a transmit fiber on an ML1000 port causes only the neighboring port to take the link down. Ideally, both ports should identify that the link went down so upper layer protocols can reroute the traffic to a different port. To work around this situation, issue “shutdown” and “no shutdown” to the port that has the disconnected or faulty transmit fiber. This issue will be resolved in Release 4.6.

DDTS # CSCea46580

SPR input counters do not increment on a BVI with an SPR interface. This issue is under investigation.

DDTS # CSCea35971

A monitor command may disappear from the configuration after a TCC reboots. To avoid this issue, use the exec command, “terminal monitor,” instead (a minor drawback is that this command applies to all VTYs), or, alternatively, reapply the monitor command after connection is lost. This is as designed.

DDTS # CSCdy31775

Packets discarded due to output queue congestion are not included in any discard count. This occurs under either of the following conditions:

- Traffic on ML-series cards between Ethernet and SONET ports, with oversubscription of available circuit bandwidth configured, leading to output queue congestion.
- Traffic from SONET to Ethernet, with oversubscription of the available Ethernet bandwidth.

This issue will be resolved in a future release.

DDTS # CSCdz49700

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.

DDTS # 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 be resolved in a future release.

DDTS # 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.

DDTS # CSCdz87944

Error messages indicating "Stuck Ucode" and "MDA_INTERNAL_ERROR" occur when routing 64-byte VLAN tagged frames at line rate. For VLANs, use bridging instead of routing. This issue will be resolved in a future release.

DDTS # CSCea11742

When a circuit between two ML POS ports is provisioned OOS, one of the ports might erroneously report TPTFAIL. This issue exists for both ML100T-12 and ML1000-2 cards. If this occurs, open a console window to each ML card and configure the POS port to shutdown. This issue will be resolved in Release 5.0.

DDTS # CSCea20962

No warning is displayed when applying OOS to ML drop ports on the circuit provisioning window. This issue will be resolved in Release 5.0.

DDTS # CSCea26847

An unexpected card reload can occur when a card is configured to route IP-Multicast traffic and subsequently sends IP-Multicast frames larger than 1649 bytes. To prevent this, avoid routing IP-Multicast frames larger than 1649 bytes. This issue is under investigation.

DDTS # 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 in Release 4.0. This issue will be resolved in a future release.

DDTS # CSCin32057

If no BGP session comes up when 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 be resolved in a future release.

DDTS # CSCin35960

POS ingress classification based on IP precedence does not match the packets when inbound policy map classifying based on IP precedence is applied to the POS interface, which is configured for HDLC or PPP encapsulation. To avoid this issue, use LEX encapsulation (default) or, at the Ethernet ingress point, mark the COS based on an IP precedence classification, then classify based on the COS during POS ingress. This issue will be resolved in a future release.

DDTS # CSCdy47284

ML-100 FastEthernet MTU is not enforced. However, frames larger than 9050 bytes may be discarded and cause Rx and Tx errors.

DDTS # CSCdz74432

Issuing a “clear IP route *” command can result in high CPU utilization, causing other processes to be delayed in their execution. To avoid this issue do not clear a large number of route table entries at once, or, if you must use the “clear IP route *” command, do not install more than 5000 EIGRP network routes.

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 CTC does not support adding/creating more than 5 STS or 28 VT circuits in auto-ranged provisioning. This is as designed.

JRE Updates

Cisco ONS platforms ship with a Java Runtime Environment (JRE) from Sun Microsystems. Occasionally Sun releases maintenance releases to the JRE. The Sun Microsystems website lists JRE maintenance releases and the issues resolved for each. Cisco recommends that you review these listings to determine if the issues resolved in any given JRE maintenance release warrant a JRE upgrade for your particular network. Cisco tests only with the specific JRE actually shipped with the ONS software CD.

Transmission Control Protocol Specification

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection might be automatically reestablished. In other cases, a user must repeat the action (for example, open a new Telnet or SSH session). Depending on the attacked protocol, a successful attack might have consequences beyond terminated connection that also must be considered. This attack vector is only applicable to those sessions that terminate on a device (such as a router, switch, or computer) and not to those sessions that only pass through the device (for example, transit traffic that is being routed by a router). Also, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products that contain TCP stack are susceptible to this vulnerability.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and describes the vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes the vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

This issue is resolved in Releases 2.3.5, 4.1.4 and 4.6.2.

DDTS # CSCec66884

Telnet access to the underlying VxWorks operating system, by default, is restricted to Superusers only. Due to this vulnerability a superuser whose account is locked out, disabled, or suspended is still able to log in (Telnet) to the VxWorks shell, using the previously configured password.

To work around this issue, use access control lists on routers and firewalls that are installed in the network to allow only valid network management workstations to gain login (Telnet) access to the TCC+/TCC2 control cards.

A Cisco Security Advisory for Cisco ONS 15327, ONS 15454, ONS 15454 SDH, and ONS 15600 vulnerabilities was released on 2004 February 19 at 1700 UTC (GMT) and applies to this issue. That advisory is located at the following URL:

http://www.cisco.com/warp/public/707/cisco-sa-20040219-ONS.shtml

This issue is resolved in Release 4.6.1 and maintenance Release 4.1.3.

DDTS # CSCec17308

The TFTP service on UDP port 69 is enabled by default to allow both GET and PUT commands to be executed without any authentication. Using a TFTP client, it is possible to connect to the optical device and upload or retrieve ONS system files to, or from the current active TCC in the /flash0 or /flash1 directories. It is not possible to upload or retrieve any user data files.

To work around this issue, use access control lists on routers and firewalls that are installed in the network to allow only valid network management workstations to gain TFTP access to the TCC+/TCC2 control cards.

A Cisco Security Advisory for Cisco ONS 15327, ONS 15454, ONS 15454 SDH, and ONS 15600 vulnerabilities was released on 2004 February 19 at 1700 UTC (GMT) and applies to this issue. That advisory is located at the following URL:

http://www.cisco.com/warp/public/707/cisco-sa-20040219-ONS.shtml

This issue is resolved in Release 4.6.1 and maintenance Release 4.1.3.

DDTS # CSCec31352

It is possible to set up the IP address of a node to an address that is in the subnet range 192.168.190.x. Such an address, however, should not be used, as its use might cause the node to reboot. This issue is resolved in Release 4.6.

DDTS # CSCeb63327

The High Temperature Alarm is raised at 50 degrees Celsius. This is, however, not optimal on an Itemp rated system, which can tolerate up to 65 degrees Celsius. To work around this issue, the alarm can be downgraded or suppressed, but note that this will result in no temperature alarm provided at all. Alternatively, Cisco TAC provides a method of retrieving the temperature from the node, which can thus be monitored periodically for temperature-related problems. This issue will be resolved in Release 4.6, and in a future maintenance release of Release 4.1.

DDTS # CSCeb45149

A 1+1 non-revertive system in which the protect card is reseated while the working card is present and active reverts back to working after you clear a Force to Protect or Manual to Protect. Affected cards are OC-3 8 port and OC-12 4 port. To work around this issue, soft-reset the working card with the protect card present and active. This issue will be resolved in Release 4.6.

Changed Default Alarm Severities

The following alarm severities have changed for Release 4.1.x.

Table 4 Changed Alarm Severities

Alarm	New Severity
VT-MON::AUTOSW-LOP	NSA-Minor
VT-MON::AUTOSW-UNEQ	NSA-Minor
VT-TERM::PLM-V	SA-Major

DDTS # CSCeb20996

While using the orderwire capability of the AIC-I, you must not input a station number with less than 4 digits. If you enter, for example, 123, CTC will display 0123; however, you will not be able to ring the node by dialing either *123, or *0123. This issue will be resolved in Release 4.6.

DDTS # CSCea93638

Path level alarms are displayed on the CTC conditions pane for deleted circuits. This issue may occur on any circuit deletion case. The conditions may be cleared by a TCC side switch. This issue will be resolved in Release 5.0.

DDTS # CSCea61887

Terminal loopback is provisionable even if the card is in transponder mode.

To see this, in the provisioning tab for a G1000 or G1K-4 card pick a pair of ports and set them to transpond with each other. The condition also holds true by picking one port and setting it to transpond with itself (one-port unidirectional). Once the transponder setting is provisioned, go to the Maintenance tab and attempt to provision terminal loopback on any of the ports that were previously provisioned for transponder functionality. CTC allows terminal loopback to be provisioned even though the setting has no effect due to the fact that the ports are performing transponder functions. If terminal loopback is truly intended, you should remove the transponder settings. A warning stating that terminal loopback has no effect if transponders are present will be displayed in Release 4.6.

DDTS # CSCea74000

Rarely, a PLM-P alarm on an OC-12 card might remain after deleting the affected STS-1 circuit. This condition persists even after deleting the affected card. If this occurs, you can reset the TCC2s to remove the stuck alarm. This issue will be resolved in Release 4.6.

DDTS # CSCea71675

Rarely, when nodes appear gray in CTC and you view the BLSR tab at the network level, the tab may be blank. When this occurs, all tabs on the same level will also become blank. To avoid this issue, do not enter into the BLSR tab at the network view until all of the nodes are some color other than gray. This issue will be resolved in Release 4.6.

DDTS # CSCea92969

The switch indicator does not clear on the Maintenance > Protection tabs when a revertive 1:1 protection group is provisioned to be non-revertive. If this occurs, from the Maintenance > Protection tabs, select the slot with the “Switch” indicator. Click the “Clear” button. This issue will be resolved in Release 4.6.

DDTS # CSCea78364

Simultaneous failure of working and protect cards in 1:N protection groups may not be alarmed as service affecting. This can occur when the working card of the protection group has been removed from the chassis, and the protect card of the protection group is subsequently issued a Manual Reset. Since the working and protect facilities are impaired, the Improper removal alarm should clear and be reissued as a Critical and service affecting condition. This issue will be resolved in Release 5.0.

DDTS # CSCea81001

When a fault condition exists against a circuit or port that is in the OOS-MT or OOS-AINS state (or when you are using the “Suppress Alarms” check box on the CTC Alarm Behavior pane), the alarm condition is not assigned a reference number. If you were to place the circuit or port in service at this time, in the absence of the reference number, the CTC alarm pane would display the condition with a time stamp indicating an alleged, but incorrect, time that the autonomous notification was issued. Clicking the CTC alarm “Synchronize” button at this stage will correct the alarm time stamp. There is no way to remedy the lack of reference number. This issue will be resolved in Release 5.0.

DDTS # CSCdx35561

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

- Enable OSPF on the LAN
- Enable Firewall

- Craft Access Only

When any of these features are enabled, the proxy ARP service on the node is also disabled. The ONS 15454 proxy ARP service assumes that all nodes are participating in the service.

This situation can also occur immediately after the aforementioned features are enabled. Other hosts on the Ethernet segment (for example, the subnet router) may retain incorrect ARP settings for the ONS 15454s.

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

You can avoid waiting for the ARP entries to expire on their own by removing the SDCC links from the affected ONS 15454 nodes. This will disconnect them for the purposes of the proxy ARP service and the nodes should become directly accessible over the Ethernet. Network settings on the nodes can then be provisioned as desired, after which the SDCC can be restored.

This issue will not be resolved.

DDTS # CSCdz84149

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

DDTS # CSCdz90753

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

DDTS # CSCdz35479

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

DDTS # CSCdy57891

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

DDTS # CSCdy56693

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

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

DDTS # CSCdy61275

Far end path FC-P is not counted on EC1 or OC3 cards. When a path defect is transmitted to the far end, it reports RDI-P. However, the condition is not examined and reported as a PM count. This issue will be resolved in a Release 5.0.

DDTS # CSCdy10030

CVs are not positively adjusted after exiting a UAS state. When a transition has been made from counting UAS, at least 10 seconds of non-SES must be counted to exit UAS. When this event occurs, Telcordia GR-253 specifies that CVs that occurred during this time be counted, but they are not. This issue will not be resolved.

DDTS # CSCdy55556

In a 1:N protection group, where a protect card is protecting a failed card and another working card, which is missing, has a lockon condition, upon removing the lockon condition from the missing working card, the protect card may switch from the card it had been protecting to carry the traffic of the missing working card that just had the lockon removed. To avoid this issue, replace the failed working card before removing the lockon. This issue will be resolved in Release 5.0.

DDTS # CSCdy11012

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

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

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

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

NE Defaults

The following caveats apply for NE defaults.

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

DDTS # CSCdy35514

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

Overhead Circuit Types

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

Overhead Channel Types

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

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

DDTS # CSCds88976

When a new circuit is created around a ring (path protection or BLSR), the SD BER or SF BER alarm can be raised depending on the order in which the spans are provisioned. The alarms will eventually clear by themselves. Traffic is not affected. This issue will not be resolved.

DDTS # CSCdx40462, CSCdx47176, CSCdw22170

While upgrading nodes from releases prior to 3.2, CTC might lose connection to the far end nodes. When this occurs, you will not be able to ping the grayed-out nodes; however, if you continue the upgrade, this problem resolves itself. This issue is resolved in Release 3.2, but can still occur when upgrading from nodes with earlier software releases.

DDTS # CSCdw66895

XCVTs (both active and standby) reboot continuously when the K3 byte is mapped to the E2 byte on one side of a WTR span. The rebooting occurs after the WTR timer expires. This has been seen on a two fiber BLSR with OC-48AS. To avoid this issue, if possible, change the K3 mapping on both ends of the span before creating the ring; or, alternatively, you can prevent the ring from reverting during the K3 mapping by setting the Ring Reversion time to "never." Once you have completed the mapping of the K3 byte to the E2 byte on both sides, return the Ring Reversion to its normal value. This issue will be resolved in Release 4.6.

ONS 15454 Conducted Emissions Kit

If you are deploying the Cisco ONS 15454 within a European Union country that requires compliance with the EN300-386-TC requirements for Conducted Emissions, you must obtain and install the Cisco ONS 15454 Conducted Emissions kit (15454-EMEA-KIT) in order to comply with this standard.

Upgrading to Use the G1000-4 Ethernet Card

Before installing or seating the G1000-4 Ethernet card on node running Release 3.1 or prior, you must upgrade the software on that node to Release 3.2 or later. This is as designed.

DDTS # CSCdv10824: Netscape Plugins Directory

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

DDTS # CSCdu82934

When you auto-route a VT circuit on an ONS 15454 node, a path is computed based on the availability of STSs on the nodes involved. This selection process, when combined with a lack of VT matrix (or STS-VT connections) on an auto-route selected node, can result in the VT circuit creation failing with the message "unable to create connection object at node." To correct this situation, manually route VT circuits in cases when auto-routing fails. The error message will indicate which node is at issue.

"Are you sure" Prompts

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

Interoperability

DDTS # CSCds13769: Fujitsu FLM-150 and Nortel OC-3 Express

You cannot provision the FLM-150 and OC-3 Express in 1+1 revertive switching mode. The problem occurs when the ONS 15454 issues a user request in revertive mode to the protect channel. When the user request is cleared, the ONS 15454 issues a No Request. However, the FLM-150 and OC-3 Express issues a Do Not Revert, which causes traffic to remain on the protection channel. Based on GR-253, section 5.3.5.5, the FLM-150 and the OC-3 Express should respond with a No Request.

BLSR Functionality

DDTS # CSCeb24331 and CSCeb40119

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

DDTS # CSCeb40296

IPPM counts for PCA (extra) traffic will not be displayed in CTC if the BLSR switches back to working after a failure recovery. To see this issue, perform the following steps in a two-fiber or four-fiber BLSR configuration.

Step 1 Create a PCA circuit.

Enable IPPM on all OCn cards for this PCA circuit.

Step 2 Issue a Forced Switch Ring (FS-R) in CTC on the add or drop node. The BLSR switches.

Step 3 View the PCA path level counts shown in CTC.

Step 4 Clear the Forced Switch Ring in CTC. The BLSR switches back to working; however, IPPM path level counts for PCA circuits are not shown.

To recover from this situation, lock out the ring by issuing the LockoutOfProtection (LK-S) command on both east and west for all nodes in the ring. Reboot the OCn card that is not showing PCA path level counts. This procedure needs to be performed whenever there is a switch in BLSR configuration. This issue will be resolved in Release 4.6.

DDTS # CSCeb09217

Circuit states are not updated after a span update. If you update a four node OC-12 two-fiber BLSR to a four node OC-192 two-fiber BLSR, the previous PCA circuits should be shown as two-fiber BLSR protected, but they are shown as “UNKNOWN” protected. If you relaunch CTC this situation is corrected. This issue will be resolved in Release 5.0.

DDTS # CSCea59342

DS3 PCA traffic may take up to 20 seconds to recover after a BLSR switch is cleared. This can occur with DS3 PCA traffic on two-Fiber or four-Fiber BLSR configuration with XCVT cards in the same nodes as the DS3 cards. This issue will be resolved in a future release.

DDTS # CSCea81000

In a two-fiber or four-fiber BLSR, MS-RFI is not reported for an LOS or LOF with a ring lockout in place on a different span. This issue will be resolved in Release 6.0.

DDTS # CSCdy68207

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

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

Step 1 Create a four-fiber BLSR.

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

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

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

If this issue occurs, clear the lockout span. All extra traffic is immediately restored. You may then reissue the lockout span. This issue will be resolved in Release 5.0.

DDTS # CSCdy56668

Ethernet circuits may appear in the CTC circuit table with an INCOMPLETE status after a BLSR/MSSP span is upgraded. The circuits, when this occurs, are not truly incomplete. They are unaffected and continue to carry traffic. To see the circuit status correctly, restart CTC. This issue will be resolved in Release 6.0.

DDTS # CSCdy48872

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

To see this issue, on a node participating in a two fiber BLSR with PCA circuits terminating at the node over the two fiber BLSR, cause an SF-R by failing the receive fiber in one direction (say, west). Then, issue an LK-S in the other direction (in our example, east). Since the LK-S has higher priority than the SF-R, the ring switch should clear and PCA traffic should be restored on spans without a fiber fault. The ring switch does clear, but PCA traffic does not restore. To correct this issue, clear the fiber fault. All traffic restores properly. This issue will be resolved in Release 5.0.

DDTS # CSCdy45902

Traffic that should be dropped remains unaffected when a BLSR Protection Channel Access (PCA) VT tunnel is placed OOS. You must place all circuits in the tunnel OOS before the traffic will be dropped. This issue will be resolved in Release 6.0.

DDTS # CSCdw32540

The two protect OC48AS cards at the ends of a four fiber BLSR span must both be configured as either K3 or Z2 (not a mixture). If both ends are not the same, the BLSR may fail to switch correctly. In Release 3.4 the BLSR wizard ensures that both ends are configured correctly; however, you must still avoid manually changing the value on one side only (and hence, causing a mismatch) at the card level. If you do mismatch bytes at the card level, you can discover this by going to the BLSR edit map tied in with the BLSR wizard. The mismatched span will be red, and right-clicking on the span will allow you to correct the problem.

DDTS # CSCdw58950

You must lock out protection BLSR, 1+1, and path protection traffic to avoid long, or double traffic hits before removing an active XC, XCVT, or XC10G card. You should also make the active cross connect card standby before removing it.

DDTS # CSCdv70175

When configuring a node with one 4 Fiber BLSR and one 2 Fiber BLSR, or with two 2 fiber BLSRs, an issue exists related to the version of XC deployed. Revision 004H and earlier revisions of the XC do not support these configurations. All later revisions of the XC and all versions of the XCVT and XC10G cross connects support all permutations of two BLSRs per node.

DDTS # CSCdv53427

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

DDTS # CSCct03919

VT1.5 and VC3/VC12 squelching is not supported in BLSR/MSSPR.

Database Restore on a BLSR

When restoring the database on a BLSR, follow these steps:

Step 1 To isolate the failed node, issue a force switch toward the failure node from the adjacent east and west nodes.

Step 2 If more than one node has failed, restore the database one node at a time.

Step 3 After the TCC+/TCC2 has reset and booted up, release the force switch from each node.

Path Protection Functionality

DDTS # CSCeb37707

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

DDTS # CSCdv42151

When a path protection circuit is created end-to-end, CTC might not create the cross-connection on all the nodes along the path at the same time. This might cause an SD-P condition along the path. When the circuit is fully provisioned on all nodes, the SD-P will clear automatically. Other conditions that can be expected while the circuit is being created are LOP-P and UNEQ-P. To reduce the risk of unexpected transient conditions, circuits should be created in the OOS_AINS state.

Active Cross Connect (XC/XC10G/XCVT) or TCC+/TCC2 Card Removal

As in BLSR and 1+1, you must perform a lockout on path protection before removing an active cross connect or TCC+/TCC2 card. The following rules apply to path protection.

Active cross connect (XC/XC10G/XCVT) cards should not generally be physically removed. If the active cross connect or TCC+/TCC2 card must be removed, you can first perform an XC/XCVT/XC10G side switch or TCC+/TCC2 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 or active TCC+/TCC2 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

DDTS # CSCeb41916

If you create a 1+1 protection group, create a circuit on the working line, and then try to retrieve the path PMs on the protect side using TL1, the request is denied. To work around this issue, use CTC to retrieve the Path PMs on the protect line. This issue will be resolved in Release 5.0.

DDTS # CSCeb40296

IPPM counts for PCA (extra) traffic will not be displayed in CTC if a BLSR switches back to working after a failure recovery. To avoid this issue, lock out the ring by issuing the LockoutOfProtection (LK-S) user command on both east and west on all nodes in the ring. Reboot the OCn card that is not showing PCA path level counts. This procedure needs to be done whenever there is a switch in BLSR configuration. This issue will be resolved in Release 4.6.

DDTS # CSCea38791

In the CTC Performance > Statistics tab of the G1000-4 or G1000-2, there are no entries for Rx/Tx Multicast and Broadcast packets. This issue will be resolved in Release 4.6.

Documentation

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

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

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

The replacement information is contained in CWDM and DWDM GBIC Compatibility with G1000-4 Cards and G1K-4 Cards, page 3.

Transponder (TXP_MR_10G) and Muxponder (MXP_2.5G_10G) Documentation

The documentation set for the Cisco ONS 15454 contains references to new transponder (TXP_MR_10G) and muxponder (MXP_2.5G_10G) cards. These portions of the documentation are meant to refer to cards that will become available with a future release. The nXP cards are not available with Release 4.1.x. Cisco apologizes for any confusion this may cause.

TL1

Note To be compatible with TL1 and DNS, all nodes must have valid names. Node names should contain alphanumeric characters or hyphens, but no special characters or spaces.

DDTS # CSCeb33033

An exception is raised when retrieving PM stats via TL1 for the protect card of a 1:1 protection group when the working card is active. To avoid this issue, retrieve stats from the working card instead of the protect card. This issue will be resolved in a future release.

DDTS # CSCdz86121

In one rare case, the ONS 15454/15327 times out a user session without communicating the timeout to TL1. If this happens, the TL1 user remains logged in, although the session is actually timed out. This can occur when you log into the node with a timeout of X minutes. If the user session sits idle for all but 5 seconds of the X minutes, then you have only 5 seconds to type in a command to notify the node that the session is active. If you try this, you will likely miss the five second window, in which case the node will respond as though the session is inactive and deny access. However, because you have typed a key, irrespective of the five second window, TL1 responds as though the session is active and does not log you out (time out). You will not have access to the node and will receive a "DENY" response to TL1 commands. The error message may vary depending on commands issued. To recover from this situation, log out and log back in to TL1. This issue will be resolved in Release 5.0.

DDTS # CSCdz26071

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

DDTS # CSCdz79471

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

Scripts that depend on the RMV-<MOD2_IO> command defaulting to OOS-MT without specifying the primary and secondary states should be updated to force the primary and secondary state inputs to be populated. This issue will be resolved in Release 5.0.

DDTS # CSCdu53509

When a TL1 session to a remote node (ENE) is established via a gateway node (GNE) and you have changed the node name of the ENE via either TL1, CTC or SNMP, then you must wait for about 30 seconds to issue a TL1 command via the GNE. This delay is to permit the updates to propagate to all nodes in the network. During this transition, neither the old node name nor the new node name can be used in the TL1 session to access the ENE. This 30 second window may be reduced in Release 6.0.

Resolved Software Caveats for Release 4.1.1

The following items are resolved in Release 4.1.1.

Hardware

DDTS # CSCdv05723 and DDTS # CSCdw37046

DS-3 traffic hits can occur during synchronization changes (frequency offsets applied) on the node's timing.

A specific scenario under which this has been seen involves configurations with multiple nodes line-timed off each other in series. If a network configuration has a DS-3 circuit routed over a chain of nodes that are line-timed off each other in sequence (more than 1 line-timed "hop"), the DS-3 traffic might exhibit errors on timing disturbances applied on the source node.

The other scenario involves an abrupt change in reference frequency between two nodes. This can result in test set errors.

This issue is resolved in Release 4.1.

ML-Series Cards

DDTS # CSCin25238

If you configure Fast EtherChannel and POS-channel in the same bridge group, during system boot, the Fast EtherChannel or POS-channel configuration may be lost and following error message displayed:

```
Interface FastEthernet1 is attempting to join Port-channel1. But Port-channel1
belongs to bridge-group 1 which has another FE(C) member in it. FEC + FE(C) is not
allowed in the same bridge group. Please change your configuration and retry.
```

This issue is resolved in Release 4.1.

DDTS # CSCea23629

During an upgrade, all ML-series cards are reset at the same time. This can result in a lengthy disruption to local traffic. This issue will be resolved in a future release, in which the upgrade will be altered to reset ML cards one at a time, so that L2/L3 protection can be used to minimize loss of local add/drop traffic during node upgrade. This issue is resolved in Release 4.1.

DDTS # CSCea18623

To avoid possible ML-series card resets when adding interfaces to a bridge group, always configure the Spanning-Tree Protocol for the bridge group (using the **bridge** *number* **protocol** command) before performing any other configuration on the bridge group.

If you want to use a bridge group that does not run the Spanning-Tree Protocol, you must first configure the bridge group with the Spanning-Tree Protocol, and then disable the Spanning-Tree Protocol for that bridge group on every interface where it is used (using the **bridge-group** *number* **spanning-disabled** interface configuration command). This issue is resolved in Release 4.1.

Maintenance and Administration

DDTS # CSCec17406

The Cisco ONS 15327, ONS 15454, and ONS 15454 SDH hardware is susceptible to an ACK Denial of Service (DoS) attack on TCP port 1080. TCP port 1080 is used by network management applications to communicate with the controller card. The controller card on the optical device will reset under such an attack. An ACK DoS attack is conducted by not sending the final ACK required for a 3-way TCP handshake to complete.

To work around this issue, use access control lists on routers and firewalls that are installed in the network to allow only valid network management workstations to gain TCP port 1080 access to the TCC+/TCC2 control cards.

A Cisco Security Advisory for Cisco ONS 15327, ONS 15454, ONS 15454 SDH, and ONS 15600 vulnerabilities was released on 2004 February 19 at 1700 UTC (GMT) and applies to this issue. That advisory is located at the following URL:

http://www.cisco.com/warp/public/707/cisco-sa-20040219-ONS.shtml

This issue is resolved in Release 4.6.1 and maintenance Releases 4.0.2 and 4.1.1.

DDTS # CSCeb33776

VT level alarms fail to clear after traffic has recovered from an error. This can happen when you configure a VT 1.5 circuit terminating on a DS1 card, then inject UNEQ-V to the terminating node, wait for the UNEQ-V alarm to be raised, then terminate the UNEQ-V signal and restore normal traffic. This issue does not occur on intermediate nodes of the circuit. The UNEQ-V alarm can be cleared using a TCC side switch. This issue is resolved in Release 4.1.1.

DDTS # CSCeb65588

When the Clear message for an alarm shows a different severity from that of the Raise message, ONS 15454 nodes may display an issue in which the LED for a critical alarm on the LCD front panel is lit, even though there are no critical alarms reported via CTC and TL1. This will also show up as an incorrect summary count (CR/MJ/MN) in the upper left corner of the CTC screen. The inconsistent message severities are also visible in the history pane. This issue is resolved in Releases 4.1.1, 4.1.2, and 4.6.

DDTS # CSCec16812

UNEQ-V alarms are incorrectly raised prior to connecting a TAP to a TACC, and also after disconnecting the TAP from the TACC. This issue is resolved in Releases 4.1.1, 4.1.2, and 4.6.

DDTS # CSCdy01598

Rarely, there is a delay in CTC before the correct card status is displayed after a protection switch. When a manual or forced switch is made to a protection type, the protection switch occurs immediately, but the card status might take a while approximately 2 minutes to show up under rare circumstances. If a switch is not reflected right away, wait for the status change to occur. This issue is resolved in Release 4.1.

DDTS # CSCdy38603

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

BLSR Functionality

DDTS # CSCdy65890

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

Path Protection Functionality

DDTS # CSCec84338

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

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

DDTS # CSCec36669

In a non-revertive path protection circuit, when both working and protect paths are injected with UNEQ-P, both paths will show UNEQ-P, CR, SA and UNEQ-P, MN, NSA alarms correctly. However, the following scenarios can occur when LOS exists:

- If, with the traffic on the protect path, you pull the working RX fiber to create LOS, the UNEQ-P alarm on the working path is not masked by the LOS alarm.
- If, with the traffic on the working path, you pull the working RX fiber to create LOS, UNEQ-P is masked correctly; however, when you replace the working RX fiber, the UNEQ-P is not reported again.

After either of the above scenarios occur, deleting the path protection circuit will fail to cause the UNEQ-P alarm to clear. The alarm can be cleared by clicking the Synchronize button in the CTC alarm pane.

This issue is resolved in Releases 4.1.1 and 4.6.

DDTS # CSCec14995

In a non-revertive path protection configuration, when a double failure is detected on both paths with UNEQ-P or AIS-P, upon clearing the protect path defect, the UNEQ-P or AIS-P alarm may remain stuck on the working path for the node. The most reliable way to remove the alarm is a TCC side switch. This issue is resolved in Release 4.1.1.

TL1

DDTS # CSCea03186

The TL1 command, INH-USER-SECU, does not disable the userid appropriately. The command should disable the userid until the corresponding ALW-USER-SECU command is issued; however, the userid is automatically re-enabled after the user lock-out period expires. The user lockout period is set from the CTC. This issue is resolved in Release 4.1.

New Features and Functionality

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

New Software Features and Functionality

ML-Series Resilient Packet Ring

RPR (Resilient Packet Ring) is a new protocol available on the ML-Series cards enabling you to use SONET bandwidth more efficiently, with 50 ms recovery times.

Basic Feature Description

RPR for the ML-Series line cards provides a set of enhancements to the performance of any such card running the Release 4.1.x. These improvements include:

RPR for the ML-Series line cards allows new deployment applications for all cards running Release 4.1.x. These improvements include:

- Better SONET bandwidth utilization compared to an STP controlled ring topology.
- Non-SONET fail-over mechanism with sub 50-millisecond convergence for fiber cuts, restores, node failures and inserting new nodes.
- Ability to perform ML-Series QOS (quality of service) features on all SONET traffic (pass-through, drop, and add).
- No hardware changes: Only requires ONS 15454 Release 4.1.x, which includes the new IOS configuration.
- Increased number of supportable VLANs and MAC addresses on the ring.
- A scalable, inter-ring protection mechanism for increased network resiliency.
- The addition of RPR does not remove any Release 4.0 functionality. RPR features are enabled via a new set of configuration commands.

For further details of RPR uses and features, consult the user documentation for Release 4.1.x.

Open Ended Path Protection

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

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

NE Defaults

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

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

User Privileges

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

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

Protect Threshold Crossing Alarms

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

C-bit framing

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

Gigabit Ethernet Transponder

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

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

Note In this section, unless otherwise mentioned, all items apply equally to both G1000-4 cards and G1K-4 cards. Some capabilities also apply to G1000-2 cards.

CWDM GBICs

Note This applies only to the ONS 15454-based G-series cards (G1000-4 and G1K-4).

CWDM GBICs correspond to the eight wavelengths supported by the Cisco CWDM GBIC solution on the ONS 15454: CWDM-GBIC-1470, CWDM-GBIC-1490, CWDM-GBIC-1510, CWDM-GBIC-1530, CWDM-GBIC-1550, CWDM-GBIC-1550, CWDM-GBIC-1570, CWDM-GBIC-1590.

DWDM GBICs

This applies only to the latest revision of the ONS 15454-based G-series cards (G1000-4 and G1K-4).

DWDM GBICs correspond to the 32 different ITU-100GHz wavelengths supported on the ONS 15454: 1530.33, 1531.12, 1531.90, 1532.68, 1534.25, 1535.04, 1535.82, 1536.61, 1538.19, 1538.98, 1539.77, 1540.56, 1542.14, 1542.94, 1543.73, 1544.53, 1546.12, 1546.92, 1547.72, 1548.51, 1550.12, 1550.92, 1551.72, 1552.52, 1554.13, 1554.94, 1555.75, 1556.55, 1558.17, 1558.98, 1559.79, and 1560.61. The ONS 15454 version DWDM GBICs are the only officially supported DWDM GBICs for the G-Series Ethernet cards. These GBICs have wideband reception capability and can receive with adequate sensitivity across the 1260-1620 nm range (refer to GBIC specs in the user documentation for details). This capability can be exploited in some of the transponder applications.

GBIC Notes

New GBICs are supported for only those vendors/brands that are officially certified for use on the ONS 15454.

GBIC inventorying functions are not currently supported. However, the type of GBIC plugged in and the wavelength used are displayed to CTC and TL1 users (as well as CTM users when CTM support is added).

Performance monitoring of optical parameters such as DWDM power levels per wavelength are not supported in Release 4.1.x.

The GBIC security feature is not supported in Release 4.1.x.

Three Transponder Modes of Operation

Release 4.1.x supports three transponder modes of operation:

Bidirectional 2-port transponder

Bidirectional 1-port transponder

Unidirectional 2-port transponder

This applies only to the ONS 15454-based G-series cards (G1000-4 and G1K-4). This feature also includes the ability of the cards to operate (when in transponder mode) independent of the cross connect cards and even operate without any cross connect cards in the shelf.

When at least one port is provisioned in a transponder mode, the entire card will be in transponder mode. When SONET/SDH circuits are provisioned on a card, the card is said to be in normal/SONET mode.

Hybrid mode of operation is not supported in Release 4.1.x. At any given time, a card can be either in transponder mode (with one or more ports being provisioned to provide transponder capabilities) or in normal SONET mode. A mixed or hybrid mode (in which only some ports are performing transponder functions while others are switching traffic into the SONET/SDH network) is not supported and you will be prevented from provisioning such a combination. In order to move a card from SONET mode to transponder mode you must first delete all SONET/SDH circuits terminating on the card, after which ports will become provisionable as transponders. Similarly you must first turn off transponder mode on all ports before a card can become eligible for SONET/SDH circuits again.

Facility Loopback

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

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

Provisionable Flow Control Watermarks

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

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

Changed Alarms

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

SONET CRITICAL Alarms

LOC is added in Release 4.1.x.

SONET MAJOR Alarms

OTUK-IAE is dropped in Release 4.1.x.

PLM-V is added in Release 4.1.x.

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

FEC-MISM is added in Release 4.1.x.

SONET MINOR Alarms

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

SONET NA/NR Conditions

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

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

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

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

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

INTRUSION-PSWD is added in Release 4.1.x.

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

New TL1 Features

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

Removed Commands

The following commands were dropped from Release 4.0.

REPT^ALM^SECU

ALW-USER-SECU

INH-USER-SECU

New Commands

The following command was added in Release 4.1.x.

CLR-COND-SECU

New Support

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

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

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

- BLSROSYNC, MN, NSA, “BLSR Out Of Sync”—Always reported against the East working OCn facility of the BLSR.
- APSCNMIS, MN, NSA, “Node Id Mismatch”—Always reported against the working OCn facility that detects the mismatch.

- RING-MISMATCH, MN, NSA, “Far End Of Fiber Is Provisioned With Different Ring ID”—Always reported against the East working OCn facility of the BLSR.

Command Request changes

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

ED-G1000 In Release 4.0:

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

ED-G1000 In Release 4.1.x:

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

ED-T1 in Release 4.0:

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

ED-T1 in Release 4.1.x:

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

ED-T3 in Release 4.0:

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

ED-T3 in Release 4.1.x:

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

ED-EC1 in Release 4.0:

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

ED-EC1 in Release 4.1.x:

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

Command Response changes

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

RTRV-USER-SECU response in Release 4.0:

```
“<uid>:,<uap>”
```

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

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

RTRV-G1000 response in Release 4.0:

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

RTRV-G1000 response in Release 4.1.x:

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

RTRV-T1 response in Release 4.0:

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

RTRV-T1 response in Release 4.1.x:

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

RTRV-T3 response in Release 4.0:

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

RTRV-T3 response in Release 4.1.x:

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

RTRV-OCH response in Release 4.0:

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

RTRV-OCH response in Release 4.1.x:

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

RTRV-CLNT response in Release 4.0:

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

RTRV-CLNT response in Release 4.1.x:

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

RTRV-OCN response in Release 4.0:

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

RTRV-OCN response in Release 4.1.x:

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

RTRV-EC1 response in Release 4.0:

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

RTRV-EC1 response in Release 4.1.x:

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

ENUM changes

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

ALS_RESTART enum items added to Release 4.1.x:

ALS_RESTART_AUTO => “AUTO-RESTART”

ALS_RESTART_MAN => “MAN-RESTART”

ALS_RESTART_MAN_TEST => “MAN-TEST-RESTART”

MOD2 enum items added to Release 4.1.x:

MOD2_M2_G1000 => “G1000”

OPTICS enum items dropped from Release 4.0:

OPTICS_OP_IR => “IR”

OPTICS_OP_LR => “LR”

OPTICS_OP_SR => “SR”

OPTICS_OP_VLR => “VLR”

OPTICS enum items added to Release 4.1.x:

OPTICS_OP_1000_BASE_CX => “1000_BASE_CX”

OPTICS_OP_CWDM_1470 => “CWDM_1470”

OPTICS_OP_CWDM_1490 => “CWDM_1490”

OPTICS_OP_CWDM_1510 => “CWDM_1510”

OPTICS_OP_CWDM_1530 => “CWDM_1530”

OPTICS_OP_CWDM_1550 => “CWDM_1550”

OPTICS_OP_CWDM_1570 => “CWDM_1570”

OPTICS_OP_CWDM_1590 => “CWDM_1590”

OPTICS_OP_CWDM_1610 => “CWDM_1610”

OPTICS_OP_ITU_100G_1530_33 => “ITU_100G_1530_33”

OPTICS_OP_ITU_100G_1531_12 => “ITU_100G_1531_12”

OPTICS_OP_ITU_100G_1531_90 => “ITU_100G_1531_90”

OPTICS_OP_ITU_100G_1532_68 => “ITU_100G_1532_68”

OPTICS_OP_ITU_100G_1534_25 => “ITU_100G_1534_25”

OPTICS_OP_ITU_100G_1535_04 => “ITU_100G_1535_04”

OPTICS_OP_ITU_100G_1535_82 => “ITU_100G_1535_82”

OPTICS_OP_ITU_100G_1536_61 => “ITU_100G_1536_61”

OPTICS_OP_ITU_100G_1538_19 => “ITU_100G_1538_19”

OPTICS_OP_ITU_100G_1538_98 => “ITU_100G_1538_98”

OPTICS_OP_ITU_100G_1539_77 => “ITU_100G_1539_77”

OPTICS_OP_ITU_100G_1540_56 => “ITU_100G_1540_56”

OPTICS_OP_ITU_100G_1542_14 => “ITU_100G_1542_14”

OPTICS_OP_ITU_100G_1542_94 => “ITU_100G_1542_94”

OPTICS_OP_ITU_100G_1543_73 => “ITU_100G_1543_73”

OPTICS_OP_ITU_100G_1544_53 => “ITU_100G_1544_53”

OPTICS_OP_ITU_100G_1546_12 => “ITU_100G_1546_12”

OPTICS_OP_ITU_100G_1546_92 => “ITU_100G_1546_92”

OPTICS_OP_ITU_100G_1547_72 => “ITU_100G_1547_72”

OPTICS_OP_ITU_100G_1548_51 => “ITU_100G_1548_51”

OPTICS_OP_ITU_100G_1550_12 => “ITU_100G_1550_12”

OPTICS_OP_ITU_100G_1550_92 => “ITU_100G_1550_92”

OPTICS_OP_ITU_100G_1551_72 => “ITU_100G_1551_72”

OPTICS_OP_ITU_100G_1552_52 => “ITU_100G_1552_52”

OPTICS_OP_ITU_100G_1554_13 => “ITU_100G_1554_13”

OPTICS_OP_ITU_100G_1554_94 => “ITU_100G_1554_94”

OPTICS_OP_ITU_100G_1555_75 => “ITU_100G_1555_75”

OPTICS_OP_ITU_100G_1556_55 => “ITU_100G_1556_55”

OPTICS_OP_ITU_100G_1558_17 => “ITU_100G_1558_17”

OPTICS_OP_ITU_100G_1558_98 => “ITU_100G_1558_98”

OPTICS_OP_ITU_100G_1559_79 => “ITU_100G_1559_79”

OPTICS_OP_ITU_100G_1560_61 => “ITU_100G_1560_61”

TRANS enum items added to Release 4.1.x:

TRANS_NONE => “NONE”

TRANS_ONE_PORT_BI => “ONE-PORT-BI”

TRANS_TWO_PORT_BI => “TWO-PORT-BI”

TRANS_TWO_PORT_RX_ONLY => “TWO-PORT-RX-ONLY”

TRANS_TWO_PORT_TX_ONLY => “TWO-PORT-TX-ONLY”

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

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

ERFI-P-CONN—Enhanced Remote Failure Indication, Path, Connectivity

ERFI-P-PAYLD—Enhanced Remote Failure Indication, Path, Payload

ERFI-P-SRVR—Enhanced Remote Failure Indication, Path, Server

The following error has changed for Release 4.1.x.

IDMS has changed from “Loopback Type Missing” to “Missing Internal Data.”

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15454, Release 4.1*
- *Cisco ONS 15454 Software Upgrade Guide, Release 4.1.x and 4.5*

Platform-Specific Documents

- *Cisco ONS 15454 Procedure Guide, Release 4.1.x and 4.5*
- *Cisco ONS 15454 Reference Guide, Release 4.1.x and 4.5*
- *Cisco ONS 15454 Troubleshooting Guide, Release 4.1.x and 4.5*
- *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide, Release 4.1.x and 4.5*
- *Cisco ONS 15454 Product Overview, Release 4.1.x and 4.5*

Obtaining Documentation

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

World Wide Web

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

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.