



# Release Notes for Cisco ONS 15454 SDH Release 4.0

---

## March, 2003

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 Release 4.0 of the *Cisco ONS 15454 SDH Installation and Operations Guide*, and *Cisco ONS 15454 SDH Troubleshooting and Reference Guide*. For the most current version of the Release Notes for Cisco ONS 15454 SDH Release 4.0, 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](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 4.0, page 16](#)
- [New Features and Functionality, page 21](#)
- [Related Documentation, page 32](#)
- [Obtaining Documentation, page 32](#)
- [Obtaining Technical Assistance, page 33](#)



---

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

Copyright © 2003. 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 4.0* since the production of the Cisco ONS 15454 SDH System Software CD for Release 4.0.

The following changes have been added to the release notes for Release 4.0.

## Changes to Caveats

The following caveat has been added to the release notes.

[STM1E-12 and Associated FMEC Cards, page 16](#)

[DDTS # CSCsh41324, page 2](#)

## Caveats

Review the notes listed below before deploying the ONS 15454 SDH. 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.

## TL1

### DDTS # CSCsh41324

When running release 4.1.4, if a circuit is created within CTC and if that circuit is retrieved via TL1, all looks as expected. However, after the software is upgraded to release 6 and latter, the circuit retrieve does not show the same value as was before. For example FAC-4-1 changes to FAC-4-0. Workaround is to delete and recreate the circuit within CTC.

## Hardware

### DDTS # 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.

## DDTS # CSCdy00622

Very rarely, an Equipment Failure Alarm can occur on an externally timed TCC+ or TCC-I card after a reset. If this occurs, BITS will be displayed as good for one TCC, but bad for the other. If the issue occurs on the standby TCC, a second reset could clear the problem. If the issue occurs on the active TCC, the card must be replaced. This issue is closed, as it does not occur with TCC2, and is otherwise very rare.

## DDTS # 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
- XC10G

The alarms could potentially occur on any of these boards, as well: OC48AS, GigE, OC192 or OC192LR. This issue will be resolved in a future release.

## DDTS # CSCdw50903

E1-14 boards with second source components can incur bit errors under extreme environmental conditions. When these boards operate under voltage and temperature stress conditions and a temperature ramp rate of 1 degree per minute, the boards could exhibit dribbling bit errors at high temperatures: BER = 5.5e-6. To avoid this, you must apply the temperature ramp rate at 0.5 degree per minute. This ramp rate complies with the NEBS standard; however, this issue will be revisited in a future release.

## Line Cards

### Ethernet Polarity Detection

The TCC2 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 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 “DLP-A 21 Install LAN Wires on the Backplane” procedure in the user documentation.

### Active Cross Connect or TCCi/2 Card Removal

Active cross connect or TCCi/2 cards should not be removed. If the active cross connect or TCCi/2 card must be removed, to minimize network interruption you can first perform an XC10G (or 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 TCCi/2 will be removed (performing a lockout on all spans will also accomplish the same goal). No lockout is necessary for switches initiated through CTC.



**Caution**

If you mistakenly remove an active cross connect or TCCi/2 card and you subsequently lose traffic on some interface cards, you may need to physically reset these cards if they fail to regain traffic.

## DDTS # CSCdz21738

A cross connect card switch can result in double traffic hits or a long hit for a E1-VC12 circuit. This issue is under investigation.

## DDTS # CSCdy65482

On the AIC-i card, a volume adjustment on the receive value of a four-wire orderwire circuit will be displayed as the negative of its actual value. To work around this issue, enter the negative of the value you actually want for the receive value. For example, adjust the receive value on CTC to -2 dbm for a gain of 2 dbm. This issue will be resolved in a future release.

## SONET and SDH Card Compatibility

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

**Table 1 SDH Data Cards that are SONET Compatible**

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

**Table 2 SONET Data Cards that are SDH Compatible**

Product Name	Description
15454-G1000-4	4 Port Gigabit Ethernet
15454-E100T-G	10/100BT, 12 Circuit, compatible w/ XC, XCVT and XC-10G
15454-E1000-2-G	Gigabit Ethernet, 2 circuit., GBIC - G

**Table 3** *Miscellaneous Compatible Cards and Components*

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

**DDTS # 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. It is not known at this time when or if this issue will 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).

**DDTS # 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.

**DDTS # CSCdw57215**

In a configuration with STM16 Any Slot cards and an VC4-8c circuit, provisioned between G1000-4 cards with traffic going over the STM16 span, extracting the G1000-4 card at one end of the VC4-8c circuit before deleting the circuit can result in a traffic hit on all existing SDH circuits defined over that same span. There are no issues if the circuit is deleted prior to the removing the G1000-4 card.

**XC10G Boot Process**

If you install a new XC10G card to the node and it fails to boot, remove the card and reinsert it. If the card still fails to boot, return it using the RMA procedure. This issue will be resolved in future hardware.

## Jitter Performance with XC10G

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

## E Series and G Series Cards

### 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.

## ML-Series

### 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 SDH ports, with oversubscription of available circuit bandwidth configured, leading to output queue congestion.
- Traffic from SDH to Ethernet, with oversubscription of the available Ethernet bandwidth.

This issue will be resolved in a future release.

## DDTS # 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.

## 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 # CSCea01675

Packets without an 802.1q VLAN tag are classified as COS 0. 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 # 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 will be resolved in Release 4.0.1.

**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 # 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-channell. But Port-channell
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 will be resolved in a future release.

**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 # 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.

## DDTS # 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.

## Maintenance and Administration



### Caution

---

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

---

## DDTS # CSCea13593

DRI configuration rules require limits on multiple drops. However, in an ONS 15454 SDH DRI topology, a unidirectional circuit can be created from one ring to another with two drops at the destination node. This issue will be resolved in Release 5.0.

## DDTS # CSCdz90733

PCA traffic can remain down after restoring the incorrect database and then restoring the correct database to the node. To avoid this issue, exercise care in database restoration. If you accidentally restore the wrong database, first restore the correct database and check to see if all traffic has returned. If PCA traffic is still down, you may need to remove and reinsert a fiber or perform a cross connect card reset. This issue will be resolved in a future release.

## DDTS # CSCea19297

For any STS or VT circuit that terminates on a node, an AIS (path level) that raises and clears on that circuit's path may result in an inability of other path alarms to be cleared. This can also occur when a line-level alarm occurs on the circuit path's line, causing the OC-N to send AIS-path downstream on each path within the line. This issue is under investigation.

## DDTS # CSCea21686

Retrieving a diagnostic file may cause a Standby or Active TCC2 reset. This is not traffic affecting. This issue is under investigation.

## DDTS # CSCdz84149

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

## DDTS # CSCdz90753

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

## DDTS # 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 is currently under investigation.

## 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. There are no plans to resolve this issue at this time.

## DDTS # 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 is under investigation.

## DDTS # CSCdy11012

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

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

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

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

## DDTS # CSCdy57891

An LOP-P alarm can be inadvertently cleared by an LOS that is raised and cleared. On 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 be resolved in a future release.

## DDTS # 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.

## DDTS # CSCdw23208

The following table 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 0-4 Error Count Reporting**

	<b>B1</b>	<b>B2</b>	<b>B3</b>
<b>ITU Specification</b>	block	bit	block
<b>STM1</b>	block	bit	block
<b>STM4</b>	bit	bit	bit
<b>STM16 trunk</b>	bit	bit	bit
<b>STM16 AS</b>	block	bit	bit
<b>STM64</b>	block	bit	bit
<b>STM1-8</b>	bit	bit	bit
<b>STM4-4</b>	bit	bit	bit

## DDTS # 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.

## 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.

## “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.

## MS-SPRing Functionality

### DDTS # CSCea02986

In MS-SPRing configurations multiple node deletions and additions on a ring in quick succession can cause PCA traffic to go down. If this occurs, apply a Force Ring switch on the effected nodes. This issue will be resolved in a future release.

### DDTS # 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 be resolved in a future release.

### 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 is under investigation.

### DDTS # CSCdy65890

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

### DDTS # CSCdy63060

In a 4 node, two-fiber MS-SPRing configuration, the E100 unstitched circuit state can become stuck at OOS-AINS-PARTIAL, even if there are no alarms and conditions raised.

This issue has been seen under the following conditions:

- 
- Step 1** Set up a 4 node, two-fiber MS-SPRing.
  - Step 2** Provision an E100 point to point circuit starting with the OOS-AINS state and the longer
  - Step 3** path as the working path. The working path should have at least one pass-through node.
  - Step 4** Ensure that Ethernet ports and STM-N ports are all in service, no alarms or conditions are raised, and traffic is running clear.
- 

If the state does not change automatically, use the Circuit Edit Window to explicitly set the circuit state to IS. This issue will be resolved in a future release.

## DDTS # CSCdy56668

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

## DDTS # CSCdy48872

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

## DDTS # CSCdw53481

Two MS-Rs 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.

## DDTS # 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.

## DDTS # 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 be resolved in a future release.

## DDTS # 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 (or BLSR)

When restoring the database on an MS-SPRing (or BLSR), follow these steps:

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | To isolate the failed node, issue a force switch toward the failure node from the adjacent east and west nodes. |
| <b>Step 2</b> | If more than one node has failed, restore the database one node at a time.                                      |
| <b>Step 3</b> | After the TCCi has reset and booted up, release the force switch from each node.                                |
- 

## SNCP Functionality

### DDTS # CSCea23862

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

### DDTS # CSCea23732

If you try to manually create a VC4 circuit over a three node, STM4 SNCP using automatic routing and a required node, but there is no protected path from the source to the destination excluding the required node, automatic routing will fail to find a path and will raise a "ComputeRouteInMixedDomains: No Route Found" exception. To avoid this issue, you can avoid selecting required nodes, or use manual routing. This issue will be resolved in Release 5.0.

## Active Cross Connect or TCCi/2 Card Removal

As in MS-SPRing (or BLSR) and 1+1, you must perform a lockout on SNCP (or UPSR) before removing an active cross connect or TCCi (or TCC2) card. The following rules apply to SNCP (or UPSR).

Active cross connect cards should not be removed. If the active cross connect or TCCi/2 card must be removed, to minimize network interruption you can first perform an XC10G (or 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 TCCi/2 will be removed (performing a lockout on all spans will also accomplish the same goal). No lockout is necessary for switches initiated through CTC.

## Documentation

### STM1E-12 and Associated FMEC Cards

Although functionality for the STM1E-12 card and its associated FMEC cards is accurately documented in the user manuals and release notes for Release 4.0, the cards will not be available for this release. Cisco regrets any confusion this may have caused. These cards will be available with Release 4.6.

## Resolved Caveats for Release 4.0

The following items are resolved in Release 4.0

## Hardware

### DDTS # CSCdw65251

Recovery times in excess of 60 ms are possible for an E3 or DS3 circuit when there is a disruption on the fiber span. This occurs when you either remove or soft-reset active span cards. This issue is resolved in Release 4.0.

## Line Cards

### DDTS # CSCdz25539

E3 1:1 traffic may be lost or incur multiple traffic hits after a WTR expires. This issue is resolved in Release 4.0.

### DDTS # CSCdy56366 and CSCdy12392

With a Linear Multiplex Section Protection (LMSP) setup with STM-16, STM-64, or STM4-4 cards, when a protection switch occurs, the MS PSC and PSD fields on the STM-16 performance pane do not increment. This issue is resolved in Release 4.0.

### DDTS # CSCdy65172

No high order path (HP) TCAs are reported for E3 ports. HP PMs are correctly reported for all E3 ports. However, Threshold Crossing Alarms are only generated for Port 1. To work around this issue, examine the PM to see if there are HP errors on an E3 card. This issue is resolved in Release 4.0.



## Maintenance and Administration

### DDTS # CSCdy38603

VC12 cross-connects downstream from a E1 can automatically transition from the OOS-AINS state to the IS state even though the E1 signal is not clean (for example, when there is an LOS present). This can occur when you have created a VC12 circuit across multiple nodes with E1s at each end, and you have not yet applied a signal to the E1 ports, and then you place the E1 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 4.0.

### DDTS # CSCdz36843

When a power supply is connected on one port only, the Power Failure alarm is reported in reverse. For example, if power is connected at the A side, the alarm is “PWR-A failure.” This issue is resolved in Release 4.0.

### DDTS # CSCdz35812

When using the Defaults Editor (in the Node view, Provisioning tab of CTC), an exception may be thrown after which the following values cannot be set using the Defaults Editor:

- STM64.pmthresholds.rs.nearend.15min.BBE
- STM64.pmthresholds.rs.nearend.15min.EB
- STM64.pmthresholds.rs.nearend.15min.ES
- STM64.pmthresholds.rs.nearend.15min.SES
- STM16.pmthresholds.rs.nearend.15min.BBE
- STM16.pmthresholds.rs.nearend.15min.EB
- STM16.pmthresholds.rs.nearend.15min.ES
- STM16.pmthresholds.rs.nearend.15min.SES
- STM4.pmthresholds.rs.nearend.15min.BBE
- STM4.pmthresholds.rs.nearend.15min.EB
- STM4.pmthresholds.rs.nearend.15min.ES
- STM4.pmthresholds.rs.nearend.15min.SES
- STM1.pmthresholds.rs.nearend.15min.BBE
- STM1.pmthresholds.rs.nearend.15min.EB
- STM1.pmthresholds.rs.nearend.15min.ES
- STM1.pmthresholds.rs.nearend.15min.SES

These thresholds may still be set from the card view of CTC. This issue is resolved in Release 4.0.

## DDTS # CSCdy63135

If a mixed protection situation arises within the network and CTC freezes while you are routing a circuit automatically, end the CTC session, then restart CTC and route manually. Note that this is only likely to occur if you route automatically from source to destination when there is no bandwidth available from the chosen source to the chosen destination, a loop exists within the network with mixed protection, and the destination exists outside of the loop. This issue is resolved in Release 4.0.

## DDTS # CSCdy12392

In a Linear Multiplex Section Protection (LMSP) setup with STM-16, STM64 or STM4-4 cards, PSC and PSD counts do not increment after a protection switch. This issue is resolved in Release 4.0.

## DDTS # CSCdy47232

If an F-UDC is setup on a 1+1 protection path or an F-UDC circuit is changed to 1+1, the path does not function. Note that MS-UDC functions correctly, but F-UDC will not work with 1+1. This issue is resolved in Release 4.0.

## DDTS # CSCdy53835

When you delete an overhead AIC-I circuit that crosses an SDCC enabled link, the OSPF area IDs of both SDCCs on the link are lost. If this issue occurs, in the SDCC provisioning tab, click Edit and uncheck the Enable OSPF checkbox on both sides of the link. Return to the SDCC provisioning tab, click Edit once more, and check the Enable OSPF checkbox on both sides of the link again. This will restore the default OSPF area ID for both SDCCs. This issue is resolved in Release 4.0.

## DDTS # CSCdy46980

If you attempt to reseal both working and protect trunk cards at the same time while there are orderwire circuits running through a trunk card that is being reseated, the AIC-I card will sound an alarm until the booting process completes. To avoid this, ensure that any trunk card being reseated is protected. This issue is resolved in Release 4.0.

## DDTS # CSCdw47506

A CTC communications failure on the network during circuit creation can cause a “Circuit Provisioning Error” exception. An attempt to continue with the errored circuit creation results in other exceptions that occur repeatedly on each attempt to continue. This issue has been seen infrequently, and only on large networks. To correct the problem, abandon the attempted circuit creation and start over. This issue is resolved in Release 4.0.

## MS-SPRing Functionality

### DDTS # CSCdy62992

The E3 circuit state does not transition correctly when the destination drop is in the OOS state.

For example:

- 
- Step 1** Create a 3 node, two-fiber, STM-16 MS-SPRing.
  - Step 2** Provision E3 cards as drop nodes. The destination drop card ports should be provisioned as OOS.
  - Step 3** Create a port group circuit selecting the OOS\_AINS circuit state. The circuit states will transition to IS for all three VC3 circuits and the VCT.
- 

This issue is resolved in Release 4.0.

## DDTS # CSCdy59242

Under some circumstances, if a fail-to-switch alarm is raised upon introducing SF-R with the existing Lockout Span command, the alarm becomes stuck after the SF-R and Lockout Span are cleared.

The following example illustrates how this can occur.

In a two fiber MS-SPRing, say the east side of Node 1 is connected to the west side of Node 2.

- 
- Step 1** Perform a Lockout Span on the east side on Node 1.
  - Step 2** Remove the transmit fiber on the east span of Node 1. (Node 2 detects signal failure on its west side.) Traffic is lost, as expected, due to the Lockout Span on the ring. A Fail-to-Switch alarm is raised.
  - Step 3** Re-insert the transmit fiber. Traffic comes back, but the fail-to-switch alarm is still reported.
  - Step 4** Clear the Lockout Span. The Fail-to-Switch alarm becomes stuck.
- 

The issue is that Node 2 ignores a long-path Lockout Span on its east side and initiates a ring switch with a local SF-R request, then fails.

To avoid this issue, make sure the ring is in the idle state and issue an Exercise Ring command on the span that reports Fail-to-Switch alarm to clear that alarm. This issue is resolved in Release 4.0.

## DDTS # CSCdy48463

Protected traffic loss can occur when a PCA monitor circuit is created on one ring to monitor a protected circuit on another ring and the two rings switch. This can also occur on a common node when a circuit is PCA on one ring side and protected on the other side.

You can see this issue in one of two ways:

1. With a two-ring configuration, create a PCA monitor circuit on one ring to monitor a protected circuit on another ring, then set the monitor point to a trunk access point anywhere on that circuit. A ring switch on both rings can trigger the traffic loss.
2. In a two-MS-SPRing configuration, with PCA circuits passing through the common node, if one of the rings is a two fiber MS-SPRing and you upgrade it, then the previous PCA connection is promoted to become protected. The result is that now a protected circuit is connected to a PCA circuit, just as in the case of the monitor circuit, and the issue occurs.

This can occur with any colliding VC4s; in other words, any situation where the VC4 from the working side is going to overlay the VC4 from the protection side when a ring or span switch occurs.

To avoid this issue, when you create PCA monitor circuits, create them to monitor the drop side of the connection and never monitor the trunk side. Also when you perform two fiber MS-SPRing ring upgrades, make sure that no PCA circuits cross through the common node before you start the upgrade. Any PCA circuits that are added and dropped on the same ring are safe, as they will be promoted to become fully protected. All PCA circuits that cross the common node to go to another ring must be deleted before the upgrade, then recreated once the upgrade is successfully completed. This issue is resolved in Release 4.0.

## DDTS # CSCdy37939 and CSCdy01642

In STM-4 MS-SPRing configurations, a WKSWPR alarm that occurs can take several seconds before it appears. The workaround is to simply wait for the alarm, which should appear after a brief delay. This issue is resolved in Release 4.0.

## DDTS # CSCdy30125

In a two by two MS-SPRing configuration, with PCA circuits passing through the common node, if one of the rings is a two fiber MS-SPRing and you upgrade it, a PCA connection will be promoted to become protected on the upgraded ring side. In this scenario, you can end up with a circuit that is PCA on one ring and protected on the other ring.

This can occur with any colliding VC4s; in other words, any situation where the VC4 from the working side is going to overlay the VC4 from the protection side when a ring or span switch occurs. On a span switch in a four fiber MS-SPRing this would be VC4 #1 on the working and VC4 #1 on the protect on the same side (i.e. east or west). For a ring switch on a four fiber MS-SPRing it would be VC4 #1 on the working and VC4 #1 on the protect on the opposite side of the ring. In a two fiber BSLR there is only a ring switch, so the colliding VC4s would be VC4 #1 on one side of the ring and VC4 #7 on the opposite side (for an STM-4 ring, for example). Symptoms of a failure will be protected traffic that is dropped or that has a stuck AIS-P.

When you perform a two fiber MS-SPRing upgrade in a two by two configuration, ensure that no PCA circuits cross through the common node before you start the upgrade. Note that the PCA circuits that are added and dropped on the same ring are safe, as they will be promoted to become fully protected. All PCA circuits that cross the common node to go to another ring must be deleted before the upgrade, then recreated once the upgrade is successfully finished. This issue is resolved in Release 4.0.

## DDTS # CSCdz25246

Four fiber PSC & PSD PM counts may disappear when a switch clears. This issue is resolved in Release 4.0.

## DDTS # CSCdy55349

Rarely, some DS3i cards may fail to carry traffic after a power cycle. This can be seen when power cycling an entire chassis, inserting an unprotected DS3i card, or protection switching to a DS3i card that has not carried traffic since it was powered up. Executing a cross connect protect switch will restore traffic. This issue is resolved in Release 4.0.

**DDTS # CSCdx76262**

In a two fiber MS-SPRing, an E3 traffic loss can exceed 60 ms upon an optical switch or XC10G side switch. This can occur whenever an optical switch or XC10G side switch occurs, even on a passthrough node; however, it does not occur consistently. This issue is resolved in Release 4.0.

**DDTS # CSCdv89939 and CSCdy46597**

After a MS-SPRing span or ring switch, traffic is switched to a different set of nodes and a protection VC4 is used. At this point, any ongoing J1 monitoring does not follow the switch. As a result, there is no J1 monitoring on the protection path. If there is a mismatch of the J1 string on the protection path, the TIM\_P alarm will not be raised. Also, you can retrieve the actual captured J1 string on the working path, but if MS-SPRing switched from working to protect, you cannot retrieve the J1 string on the protect path. This issue is resolved in Release 4.0.

**DDTS # CSCdy41904**

After a ring switch (where PCA traffic is preempted), putting a PCA circuit in the out of service (OOS) state will not stop traffic flow for that circuit once the ring switch is cleared. To avoid this issue, delete the circuit or place the circuit in the IS, then the OOS state. This issue is resolved in Release 4.0.

**DDTS # CSCdy10805**

If you upgrade one of the rings in a two by two MS-SPRing configuration, an EXTRA-TRAF-PREEMPT alarm may be raised and subsequently fail to clear on one of the rings. If the ring that has the stuck alarm already has some PCA circuits on it, you can issue and then clear a Force Ring. This should clear the stuck alarm. If no PCA circuits exist on the ring, then create one temporarily, and follow the above procedure to clear the alarm. After the alarm clears, you can remove the Force Ring, then delete the PCA circuit. This issue is resolved in Release 4.0.

**DDTS # CSCdy35901**

In a four-node, STM-64, four fiber MS-SPRing, traffic remains lost after a lockout is cleared on an adjacent node when the local node has an SF-R raised. To correct this problem if it occurs, issue a force ring on the side of the SF-R affected node that the SF-R is raised on. This issue is resolved in Release 4.0.

**SNCP Functionality****DDTS # CSCdw66071**

After a switch to protect is cleared for a revertive SNCP circuit, the WTR alarm is not raised, although the wait period is observed and the circuit reverts back to working. This issue is resolved in Release 4.0.

**New Features and Functionality**

This section highlights new features and functionality for Release 4.0. For detailed documentation of each of these features, consult the user documentation.

## New Hardware

### G1K-4 Card

The G1K-4 card provides four ports of IEEE-compliant, 1000-MBits/s (Mbps) interfaces. Each interface supports full-duplex operation for a maximum bandwidth of 1 GBits/s (Gbps) or 2 GBits/s (Gbps) bidirectional per port, and 2.5 GBits/s (Gbps) or 5 GBits/s (Gbps) bidirectional per card. Each port autonegotiates for full duplex and 802.3x flow control. The G1K-4 card uses GBIC modular receptacles for the optical interfaces.

Cisco offers three GBIC modules as separate orderable products for maximum flexibility:

- IEEE 1000Base-SX compliant, 850-nm, optical module
- IEEE 1000Base-LX compliant, 1300-nm, optical module
- IEEE 1000Base-ZX compliant, 1550-nm, optical module

The 850-nm SX optics are designed for multimode fiber and distances of up to 220 meters on 62.5 micron fiber and up to 550 meters on 50 micron fiber. The 1300-nm LX optics are designed for single-mode fiber and distances of up to ten kilometers. The 1550-nm ZX optics are designed for single-mode fiber and distances of up to eighty kilometers.

For more specific details, consult the “Cisco ONS 15454 SDH Reference Manual,” Release 4.0.

### OC3IR/STM1SH 1310-8 Card

The OC3IR/STM1SH 1310-8 card provides eight intermediate or short range, ITU-T G.707- and G.957-compliant, SDH, STM-1 ports. Each port operates at 155.52 MBits/s (Mbps) over a single-mode fiber span. The card supports concatenated or non-concatenated payloads at the STM-1 signal level on a per VC-4 basis.

You can install the OC3IR/STM1SH 1310-8 card in any multispeed card slot, slots 1 to 4 and 14 to 17. The card can be provisioned as part of an SNCP or in an add/drop multiplexer/terminal monitor (ADM/TM) configuration. Each interface features a 1310-nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The card uses LC connectors on the faceplate, angled downward 12.5 degrees.

The OC3IR/STM1SH 1310-8 card supports 1+1 unidirectional and bidirectional protection switching. You can provision protection on a per port basis.

The OC3IR/STM1SH 1310-8 card detects LOS, LOF, LOP, MS-AIS, and MS-FERF conditions. Refer to Cisco ONS 15454 SDH Troubleshooting Manual for a description of these conditions. The card also counts section and line BIP errors. To enable MSP, the OC3IR/STM1SH 1310-8 card extracts the K1 and K2 bytes from the SDH overhead to perform appropriate protection switches. The OC3IR/STM1SH 1310-8 card supports full DCC/GCC connectivity for remote network management.

For more specific details, consult the “Cisco ONS 15454 SDH Reference Manual,” Release 4.0.

### OC192 LR/STM64 LH ITU 15xx.xx Card

Eight distinct STM-64 ITU 100 GHz DWDM cards comprise the ONS 15454 SDH DWDM channel plan. The OC192 LR/STM64 LH ITU 15xx.xx card provides one long-range, ITU-T G.707- and G.957-compliant, SDH STM-64 port per card. The port operates at 9.95328 GBits/s (Gbps) over unamplified distances up to 60 km with different types of fiber such as C-SMF or dispersion compensated fiber limited by loss and/or dispersion. The card supports concatenated or non-concatenated payloads on a VC-4 basis, as well as VC-4, VC-3, and VC-12 payloads. Four of the

cards operate in the blue band with a spacing of 100 GHz in the ITU grid (1534.25 nm, 1535.04 nm, 1535.82 nm, and 1536.61 nm). The other four cards operate in the red band with a spacing of 100 GHz in the ITU grid (1550.12 nm, 1550.92 nm, 1551.72 nm, and 1552.52 nm).

You can install OC192 LR/STM64 LH ITU 15xx.xx cards in any high-speed slot, slot 5, 6, 12, or 13, on the ONS 15454 SDH. You can provision this card as part of an MS-SPR, SNCP, or linear configuration or also as a regenerator for longer span reaches.

The OC192 LR/STM64 LH ITU 15xx.xx port features a laser on a specific wavelength in the 1550-nm range and contains a transmit and receive connector (labeled) on the card faceplate. The card uses a dual SC connector for optical cable termination. The card supports 1+1 unidirectional and bidirectional facility protection. It also supports 1:1 protection in four-fiber bidirectional line switched ring applications where both span switching and ring switching might occur.

The OC192 LR/STM64 LH ITU 15xx.xx card detects SF, LOS, or LOF conditions on the optical facility. Refer to the *Cisco ONS 15454 SDH Troubleshooting Manual* for a description of these conditions. The card also counts section and line BIP errors from B1 and B2 byte registers in the section and line overhead.

For more specific details, consult the “*Cisco ONS 15454 SDH Reference Manual*,” Release 4.0.

## OC192 IR/STM64 SH 1550 Card

The OC192 IR/STM64 SH 1550 card provides one short-range, ITU-T G.707- and G.957-compliant, SDH STM-64 port per card. The port operates at 9.95328 GBits/s (Gbps) over unamplified distances up to 40 km with SMF-28 fiber limited by loss and/or dispersion. The card supports concatenated or non-concatenated payloads on a VC-4 basis, as well as VC-4, VC-3, and VC-12 payloads.

You can install OC192 IR/STM64 SH 1550 cards in any high-speed slot, slot 5, 6, 12, or 13, on the ONS 15454 SDH. You can provision this card as part of an MS-SPRing, SNCP, or linear configuration, or also as a regenerator for longer span reaches.

The OC192 IR/STM64 SH 1550 port features a 1550-nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The card uses a dual SC connector for optical cable termination. The card supports 1+1 unidirectional and bidirectional facility protection. It also supports 1:1 protection in four-fiber bidirectional line switched ring applications where both span switching and ring switching might occur.

The OC192 IR/STM64 SH 1550 card detects SF, LOS, or LOF conditions on the optical facility. Refer to the “*Cisco ONS 15454 SDH Troubleshooting Manual*” for a description of these conditions. The card also counts section and line BIP errors from B1 and B2 byte registers in the section and line overhead.

For more specific details, consult the “*Cisco ONS 15454 SDH Reference Manual*,” Release 4.0.

## ML-Series Cards

The ML-Series 10/100/Gigabit Ethernet cards provide high throughput, low latency packet transport of Ethernet traffic (L2, IP and other L3 protocols), and a port based STS-48 backend for your SDH/SONET network. With ML-Series cards, efficient Ethernet transport and TDM can coexist on same card, thus enabling low cost interconnectivity for hubs and routers. The ML-Series works with Cisco IOS and takes advantage of IOS’s IP rich features and reliability. The ML-Series functions as a Fast-Ethernet or Gigabit-Ethernet extension, or, in an aggregation application, such as high-capacity customer LAN traffic, Internet traffic, or VPN, with 1 MBits/s (Mbps) and above bandwidth guaranteed traffic grooming. The following summaries highlight ML-Series card features. For more specific details, consult the “*Cisco ONS 15454 SDH Reference Manual*,” Release 4.0.

## ML1000-2 Card

The ML1000-2 card provides two ports of IEEE-compliant, 1000-MBits/s (Mbps) interfaces. Each interface supports full-duplex operation for a maximum bandwidth of 2 GBits/s (Gbps) per port and 4 GBits/s (Gbps) per card. Each port autoconfigures for full duplex and IEEE 802.3x flow control.

The ML1000-2 card works in any of the slots from 1 to 6 or 12 to 17 if you use the XC10G or the XC-VXL-10G cross-connect card. It works in slot 5, 6, 12, or 13 if you use the XC-VXL-2.5G cross-connect card.

Two SFP modules are offered as separate orderable products for maximum customer flexibility: an IEEE 1000Base-SX compliant, 850-nm optical module and an IEEE 1000Base-LX-compliant, 1300-nm optical module. The 850-nm SX optics are designed for multimode fiber and distances of up to 220 meters on 62.5 micron fiber and up to 550 meters on 50 micron fiber. The 1300-nm LX optics are designed for single-mode fiber and distances of up to five kilometers. Other SFP modules for long-reach 1550-nm and twisted-pair copper will be offered for use with the E1000 card in a future release.

The ML1000-2 Gigabit Ethernet card provides high-throughput, low-latency packet switching of Ethernet encapsulated traffic (IP and other Layer 3 protocols) across an SDH/SONET network while providing a greater degree of reliability through SDH/SONET “self-healing” protection services. This enables network operators to provide multiple 1000 MBits/s (Mbps) access drops for high-capacity customer LAN interconnects, Internet traffic, and cable modem traffic aggregation. Efficient transport and co-existence of traditional TDM traffic with packet-switched data traffic is provided.

The ML1000-2 card eliminates the need for external aggregation equipment such as Ethernet or ATM switches at the customer site, remote headends, or distributed POPs.

Each ML1000-2 card supports standards-based, Layer 2 Ethernet switching between its Ethernet ports and any other Ethernet or SDH/SONET trunk interfaces on the ONS 15454 SDH. The IEEE 802.1Q tag and port-based VLANs logically isolate traffic (typically subscribers). Priority queuing is also supported to provide multiple classes of service. Two queues are provided on card. Queue level is settable from 0 to 7; 0 to 3 map, and 4 to 7 map.

You can install the ML1000-2 card into any multispeed slot for a total shelf capacity of 20 Gigabit Ethernet ports. Multiple Ethernet cards installed in an ONS 15454 SDH can act as either a single switching entity or as a single switch supporting a variety of SDH/SONET port configurations.

## ML100T-12 Card

The ML100T-12 card provides 12 ports of IEEE 802.3-compliant, 10/100 interfaces. Each interface supports full-duplex operation for a maximum bandwidth of 200 MBits/s (Mbps) per port and 2.488 GBits/s (Gbps) per card. Each port independently detects the speed of an attached device (autosenses) and automatically connects at the appropriate speed. The ports autoconfigure to operate at either half or full duplex and can determine whether to enable or disable flow control. The ML100T-12 card works in any slot from 1 to 6 or 12 to 17 if you use the XC10G or XC-VXL-10G cross-connect card. It works in slot 5, 6, 12, or 13 if you use the XC-VXL-2.5G cross-connect card.

The ML100T-12 Ethernet card provides high-throughput, low-latency packet switching of Ethernet traffic across an SDH/SONET network while providing a greater degree of reliability through SDH/SONET “self-healing” protection services. This Ethernet capability enables network operators to provide multiple 10/100-MBits/s (Mbps) access drops for high-capacity customer LAN interconnects, Internet traffic, and cable modem traffic aggregation. Efficient transport and co-existence of traditional TDM traffic with packet-switched data traffic are provided.

The ML100T-12 eliminates the need for external aggregation equipment such as Ethernet switches, remote headends, or distributed POPs.



Each ML100T-12 card supports standards-based, wire-speed, Layer 2 Ethernet switching between its Ethernet ports. The 802.1Q tag and port-based VLANs logically isolate traffic (typically subscribers). Priority queuing is also supported to provide multiple classes of service.

You can install the ML100T-12 card in any multispeed slot. Multiple Ethernet cards installed in an ONS 15454 SDH act as a single switch supporting a variety of SDH/SONET port configurations. You can create logical SDH/SONET ports by provisioning a number of VC-4 channels to the packet switch entity within the ADM. Logical ports can be created with a bandwidth granularity of VC-4. The ONS 15454 SDH supports VC-4-1c, VC-4-2c, or VC-4-4c signal levels.

## TCC2

The TCC2 performs system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection/resolution, SDH section overhead (SOH) data communication channel/generic communication channel (DCC/GCC) termination, and system fault detection for the ONS 15454 SDH. The TCC2 also ensures that the system maintains Stratum 3 (ITU-T G.813) timing requirements. It monitors the supply voltage of the system. Figure 2-4 shows the TCC2 faceplate and Figure 2-5 shows a block diagram of the card.



### Note

The TCC2 card can work with the XC10G, XC-VXL-10G, or XC-VXL-2.5G cross connect cards. It requires Software Release 4.0 or higher.



### Note

The LAN interfaces of the TCC2 card meet the standard Ethernet specifications by supporting a cable length of 100 meters at temperatures from 0 degrees C to 65 degrees C (32 degrees F to 149 degrees F). The interfaces can operate with a cable length of 10 meters maximum at temperatures from -40 degrees C to 0 degrees C (-40 degrees F to 32 degrees F).

For TCC2 card functionality and details, consult the “*Cisco ONS 15454 SDH Reference Manual*,” Release 4.0.

## Cross Connect XCVXL-10G Card

The XCVXL-10G card cross connects E-1, E-3, DS-3, STM-1, STM-4, and STM-16 signal rates. The XCVXL-10G provides a maximum of 384 x 384 VC-4 nonblocking cross connections, 384 x 384 VC-3 nonblocking cross connections, or 2016 x 2016 VC-12 nonblocking cross connections. It is designed for 10-GBits/s (Gbps) solutions.

The XCVXL-10G card manages up to 192 bidirectional STM-1 cross-connects, 192 bidirectional E-3 or DS-3 cross-connects, or 1008 bidirectional E-1 cross-connects. The TCC2 assigns bandwidth to each slot on a per STM-1 basis. The XCVXL-10G card works with the TCC2 card to maintain connections and set up cross-connects within the system. Depending on requirements of the node, one of the XC10G, XCVXL-10G, or XCVXL-2.5G card types is required to operate the ONS 15454 SDH. You can establish cross-connect and provisioning information through the Cisco Transport Controller (CTC). The TCC2 establishes the proper internal cross-connect information and sends the setup information to the XCVXL-10G cross-connect card.



### Note

Cisco does not recommend nor support operating the ONS 15454 SDH with only one XCVXL-10G card. To safeguard your system, always operate in a redundant configuration. An XCVXL-10G is to be placed in each of slots 8 and 10.

For more specific details, consult the “*Cisco ONS 15454 SDH Reference Manual*,” Release 4.0.

## Cross Connect XCVXL-2.5G Card

The XCVXL-2.5G card cross connects E-1, E-3, DS-3, STM-1, STM-4, STM-16, and STM-64 signal rates. The XCVXL-2.5G provides a maximum of 192 x 192 VC-4 nonblocking cross connections, 384 x 384 VC-3 nonblocking cross connections, or 2016 x 2016 VC-12 nonblocking cross connections. It is designed for 2.5-GBits/s (Gbps) solutions.

The XCVXL-2.5G card manages up to 192 bidirectional STM-1 cross-connects, 192 bidirectional E-3 or DS-3 cross-connects, or 1008 bidirectional E-1 cross-connects. The TCC2 assigns bandwidth to each slot on a per STM-1 basis. The XCVXL-2.5G card works with the TCC2 card to maintain connections and set up cross-connects within the system. Depending on requirement in the node, one of the XC10G, XCVXL-10G, or XCVXL-2.5G card types is required to operate the ONS 15454 SDH. You can establish cross-connect and provisioning information through the Cisco Transport Controller (CTC). The TCC2 establishes the proper internal cross-connect information and sends the setup information to the XCVXL-2.5G cross-connect card.

**Note**

---

The XCVXL 2.5G does not support STM-64.

---

For more specific details, consult the “*Cisco ONS 15454 SDH Reference Manual*,” Release 4.0.

## E1-42 Card

The 42-port ONS 15454 SDH E1-42 card provides 42 ITU-compliant, G.703 E-1 ports. Each port of the E1-42 card operates at 2.048 MBits/s (Mbps) over a 120-ohm, twisted-pair copper cable. Front mount electrical connection is done using the FMEC E1-120 NP card for unprotected operation, the FMEC E1-120PROA for 1:3 protection in the left side of the shelf, or the FMEC E1-120PROB for 1:3 protection in the right side of the shelf.

**Note**

---

If you need 75-ohm unbalanced interfaces, you must additionally use the E1-75BB conversion panel.

---

For more specific details, consult the “*Cisco ONS 15454 SDH Reference Manual*,” Release 4.0.

## FMEC E1-120NP Card

The ONS 15454 SDH FMEC E1-120NP card provides front mount electrical connection for 42 ITU-compliant, G.703 E-1 ports. With the FMEC E1-120NP card, each E1-42 port operates at 2.048 MBits/s (Mbps) over a 120-ohm balanced interface. Twenty-one interfaces are led through one common Molex 96-pin LFH connector. You can install the FMEC E1-120NP card in any Electrical Facility Connection Assembly (EFCA) slot from slot 18 to 21 or slot 26 to 29 on the ONS 15454 SDH. Each FMEC E1-120NP card port features E1-level inputs supporting cable losses of up to 6 dB at 1024 kHz.

For more specific details, consult the “*Cisco ONS 15454 SDH Reference Manual*,” Release 4.0.

## FMEC E1-120PROA Card

The ONS 15454 SDH FMEC E1-120PROA card provides front mount electrical connection for 42 ITU-compliant, G.703 E-1 ports. With the FMEC E1-120PROA card, each E1-42 port operates at 2.048 MBits/s (Mbps) over a 120-ohm balanced interface. Twenty-one interfaces are led through one common

Molex 96-pin LFH connector. You can install the FMEC E1-120PROA card in the EFCA in the four left-most slots (slots 18 to 21) on the ONS 15454 SDH. Each FMEC E1-120PROA card port features E1-level inputs supporting cable losses of up to 6 dB at 1024 kHz.

For more specific details, consult the “*Cisco ONS 15454 SDH Reference Manual*,” Release 4.0.

## FMEC E1-120PROB Card

The ONS 15454 SDH FMEC E1-120PROB card provides front mount electrical connection for 42 ITU-compliant, G.703 E-1 ports. With the FMEC E1-120PROB card, each E1-42 port operates at 2.048 Mbits/s (Mbps) over a 120-ohm balanced interface. Twenty-one interfaces are led through one common Molex 96-pin LFH connector. You can install the FMEC E1-120PROB card in any EFCA slot from slot 26 to 29 on the ONS 15454 SDH. Each FMEC E1-120PROB card port features E1-level inputs supporting cable losses of up to 6 dB at 1024 kHz.

For more specific details, consult the “*Cisco ONS 15454 SDH Reference Manual*,” Release 4.0.

## E1-75BB Conversion Panel

The ONS 15454 SDH E1-75BB (BB = Black Box) impedance conversion panel provides front mount electrical connection for 42 ITU-compliant, G.703 E-1 ports. With the E1-75BB conversion panel, each E1-42 port operates at 2.048 Mbits/s (Mbps) over a 75-ohm unbalanced coaxial 1.0/2.3 miniature coax connector. For installation instructions and specific details, consult the “*Cisco ONS 15454 SDH Reference Manual*,” Release 4.0.

## STM1E-12 Card

The twelve-port ONS 15454 SDH STM1E-12 card provides twelve ITU-compliant, G.703 STM-1 ports per card. Ports 9 to 12 can be switched to E-4 instead of STM-1. Each interface operates at 155.52 Mbits/s (Mbps) for STM-1 or 139.264 Mbits/s (Mbps) for E-4 over a 75-ohm coaxial cable (with the FMEC STM1E NP card, the FMEC STM1E 1:1 card, or the FMEC STM1E 1:3 card). In E-4 mode, framed or unframed signal operation is possible. The STM1E-12 card operates as a working or protect card in 1:1 and in 1:3 protection schemes. You can install the STM1E-12 card in any multispeed card slot, slots 1 to 4 and 14 to 17, on the ONS 15454 SDH. Each STM1E-12 port features ITU-T G.703 compliant inputs supporting cable losses of up to 12.7 dB at 78 MHz. The STM1E-12 card supports 1:1 protection and 1:3 protection.



### Note

When a protection switch moves traffic from the STM1E-12 working/active card to the STM1E-12 protect/standby card, ports on the now active/standby card cannot be taken out of service. Lost traffic can result if you take a port out of service, even if the STM1E-12 active/standby card no longer carries traffic.

For more specific details, consult the “*Cisco ONS 15454 SDH Reference Manual*,” Release 4.0.

## FMEC STM1E NP Card

The ONS 15454 SDH FMEC STM1E NP card provides front mount electrical connection for 12 ITU-compliant, G.703 STM1E ports. Ports 9 to 12 can be switched to E-4 instead of STM-1 (via CTC on the STM1E-12 card). With FMEC STM1E NP, each interface of an STM1E-12 card operates at 155.52 Mbits/s (Mbps) for STM-1 or 139.264 Mbits/s (Mbps) for E-4 over a 75-ohm unbalanced coaxial 1.0/2.3 miniature coax connector.

You can install the FMEC STM1E NP card in any EFCA slot from slot 18 to 21 or slot 26 to 29 on the ONS 15454 SDH. Each FMEC STM1E NP card interface features STM1-level inputs supporting cable losses of up to 12.7 dB at 78 MHz.

For more specific details, consult the “*Cisco ONS 15454 SDH Reference Manual*,” Release 4.0.

## FMEC STM1E 1:1 Card

The ONS 15454 SDH FMEC STM1E 1:1 card provides front mount electrical connection for 12 ITU-compliant, G.703 STM1E ports. Ports 9 to 12 can be switched to E-4 instead of STM-1 (via CTC on the STM1E-12 card). With the FMEC STM1E 1:1 card, each interface of an STM1E-12 card operates at 155.52 Mbits/s (Mbps) for STM-1 or 139.264 Mbits/s (Mbps) for E-4 over a 75-ohm unbalanced coaxial 1.0/2.3 miniature coax connector. The FMEC STM1E 1:1 card is required if you want to use the 1:1 protection feature of the STM1E-12 card. You can also use the FMEC STM1E 1:1 for connection to two unprotected STM1E-12 cards. In a future release the card will support secondary priority traffic.

You can install the FMEC STM1E 1:1 card in any EFCA slot pair (18/19, 20/21, 26/27, or 28/29) on the ONS 15454 SDH. Each FMEC STM1E 1:1 card interface features STM1-level inputs supporting cable losses of up to 12.7 dB at 78 MHz.

For more specific details, consult the “*Cisco ONS 15454 SDH Reference Manual*,” Release 4.0.

## FMEC STM1E 1:3 Card

The ONS 15454 SDH FMEC STM1E 1:3 card provides front mount electrical connection for 12 ITU-compliant, G.703 STM1E ports. Ports 9 to 12 can be switched to E-4 instead of STM-1 (via CTC on the STM1E-12 card). With the FMEC STM1E 1:3 card, each interface of an STM1E-12 card operates at 155.52 Mbits/s (Mbps) for STM-1 or 139.264 Mbits/s (Mbps) for E-4 over a 75-ohm unbalanced coaxial 1.0/2.3 miniature coax connector. The FMEC STM1E 1:3 card is required if you want to use the 1:3 protection feature of the STM1E-12 card. You can also use the FMEC STM1E 1:3 for connection to four unprotected STM1E-12 cards. In a future release the card will support secondary priority traffic. The FMEC STM1E 1:3 card must be installed in slots 18 to 21 for use with STM1E-12 cards in slots 1 to 4. The FMEC STM1E 1:3 card must be installed in slots 26 to 29 for use with STM1E-12 cards in slots 14 to 17.

You can install the FMEC STM1E 1:3 card in any EFCA slot from slot 18 to 21 or slot 26 to 29 on the ONS 15454 SDH. Each FMEC STM1E 1:3 card interface features STM1-level inputs supporting cable losses of up to 12.7 dB at 78 MHz.

For more specific details, consult the “*Cisco ONS 15454 SDH Reference Manual*,” Release 4.0.

# New Software Features and Functionality

## Cross Connect Loopback

Prior to Release 4.0, testing and verifying circuit integrity often involved use of an entire line. With Release 4.0, XC loopbacks enable a single VC4, VC4-4c, and VC4-16c, within a higher rate STM signal, to be looped back without interrupting the other STM-N circuits. Specifically, XC loopbacks provide the ability to loop back on any embedded channel at supported payloads including and above VC4 granularities. XC loopbacks are supported for optical cards.

An XC loopback is allowed only if the connection state of the circuit is OOS-AINS or OOS-MT. The XC loopback option is available on all optical paths in the system that are cross-connected.

When a an XC loopback is selected, an AIS (Alarm Indication Signal) is transmitted from the far end of the existing cross-connect if the near end is involved in an XC loopback.

If the line supporting the path involved with an XC loopback is involved in a 1+1 protection scheme, both the Active and Working paths are looped back in the cross connect matrix.

Paths that are in an XC loopback are not permitted to be used for Test Access. Only one type of loopback is allowed on a supporting line and path. If a facility loop back exists on an STM-16 line, you may not perform an XC loopback on any paths in that line, and vice-versa.

Addition and deletion of cross connects is permitted while the port is in an active loopback. However, if a cross-connect is deleted while the path is in an XC loopback, the loopback is automatically removed by the system.

## LCD Enhancements

As of Release 4.0, the information displayed on the LCD, located on the fan tray assembly, can be controlled via software.

Release 4.0 allows you to modify parameters to control the following displayed information:

- Suppression of LCD IP display
- Display of the NE defaults name
- Alarm output one-button toggle (alarm counts and alarm summary in the LCD are displayed alternately)

You can also modify display parameters to prohibit configuration changes via the LCD display touchpad.

## SNCP Dual Ring Interconnect

The SNCP dual ring interconnect topology (SNCP DRI) provides an extra level of path protection between interconnected SNCPs. In DRIs traffic is dropped and continued at the interconnecting nodes to eliminate single points of failure. Two DRI topologies can be implemented on the ONS 15454 SDH. The traditional DRI uses four ONS 15454 SDHs at the interconnect nodes, while the integrated DRI uses two nodes.

For more specific details, consult the “Cisco ONS 15454 SDH Reference Manual,” Release 4.0.

## Audit Trail Enhancements

In Release 4.0, the Audit Trail feature has been improved. To use the Audit Trail features, you must be logged on with either provisioning or superuser privileges.

You can now save audit trail records created since the last archive operation to a local file. Multiple archive files, when viewed in combination, provide insight into the node’s audit travel over time, with no omissions or overlap.

Two new alarms indicate when an audit trail archive should be performed:

- AUD-LOG-LOW is raised when the audit trail is 80% full.
- AUD-LOG-LOSS is raised when the audit trail begins to overwrite records that have not yet been archived.

Both of the new alarms clear automatically when you perform an archive via CTC.

The contents of the audit trail have also been enhanced. The hexadecimal numbers previously displayed in audit trail records have been replaced with meaningful text, or decimal numbers, where appropriate.

Circuit size is now shown in the audit trail records for creation and/or deletion of a circuit.

VC4, VC3, and VC12 numbers are now displayed as one-based instead of zero-based in audit records.

## CTC Logical Network View

The Network view graphic area displays a background image with colored ONS 15454 SDH icons. With Release 4.0, a superuser can set up the new logical network view feature to enable each user to see the same network view.

## Port Based Numbering of Alarms

With Release 4.0, all alarms and conditions are announced against the associated externally visible port (numbered to match the ingress port of the signal). No alarms or conditions are announced against internal ports.

## E-series Linear Mode

With Release 4.0, CTC allows a circuit to be created end-to-end between an E-series (in Single-Card EtherSwitch or linear mode) and an EC1 span crossing over two or more nodes (with optical links) when the selected circuit size is STS-1.

## Graphical Display of Lockout

Release 4.0 offers a new, detailed graphical display of lockout conditions on a span. Prior to Release 4.0, there is no clear indication when a span that is locked out has been manually switched. In previous releases, these events are reported in the Conditions tab or as a non-reporting event in the alarm tab.

Graphical indications of a Lockout, Force, or Manual switch condition are displayed for the following schemes:

- 1 + 1 configuration
- 2 Fiber MS-SPRing
- 4 Fiber MS-SPRing

The graphical display of a condition can be viewed from the Network, Circuit and Detailed Circuit maps when a protection switch is applied.

Possible displayed values are:

- E—Exercise
- M—Manual
- F—Force
- L—Lockout

## Database Downgrade Protection

With Release 4.0, CTC prevents restoration of a database written by a software version newer than what the TCC, TSC, or TCC+ is running. CTC issues a warning, but allows you to proceed, when reverting to an older software version.

## Proxy Server Port Reduction

In previous releases, CTC was able to manage nodes behind routers that performed network address translation (NAT) but required that intermediate routers allow connections on many ports. Additionally, these intermediate routers needed to be configured to allow connections to be initiated from both CTC and the GNE. With Release 4.00, CTC can now manage nodes behind routers that perform NAT or port address translation (PAT). Intermediate routers need only be configured to allow connections from CTC to the GNE on ports 80 (HTTP) and 1080 (SOCKS) and packets for established connections from the GNE to CTC. The superuser can enable this functionality on the node level Provisioning > Network tab.

## Ethernet Transmit and Receive Utilization

Release 4.0 provides separate utilization categories for Ethernet Transmit (Tx) and Receive (Rx) utilization, instead of the single value provided by previous releases.

## DCC Expansion

An important benefit of the TCC2 card offered with Release 4.0 is that each node in which TCC2s are installed can terminate up to 32 section DCCs. Routing abilities of the system are also enhanced to ensure that the TCC2 can effectively manage the increased amount of DCC traffic resulting from the change in the number of possible DCC terminations. This increase in potential DCC terminations gives your network greater capacity for creating and administering SNCs.

## MS-SPRing J1 CTC

In Release 4.0, several enhancements have been made to improve support for C2 and unmatched J1 path trace with MS-SPRing protection switching. In summary, the following have been addressed.

CTC displays all unmatched J1 Path Trace detected and C2 byte, including:

- STS Number
- Slot
- Port
- Expected J1 Byte
- Received J1 Byte
- Received C2 Byte

This allows you to locate Path Trace Mismatch even for a switched MS-SPRing circuit.

## CTC Path Trace Alarm Support

In Release 4.0, after traffic has switched to a protection span, standard TIM-P alarms will be raised when there is a J1 mismatch detected on the switched STSs.

## CTC NCP Display Enhancement

In Release 4.0, NCP is enhanced to support the display of a switched MS-SPRing path, in addition to the working path. NCP is also enhanced to display alarms on STSs where a switched MS-SPRing path is located, and allows you to monitor path trace on the switched MS-SPRing path such that:

- CTC provides visibility of the ASCII contents of the monitored J1 byte for each STS path even when active traffic has switched to the protection span of an MS-SPRing.

- CTC provides visibility to the expected J1 value for each STS path even when active traffic has switched to the protection span of an MS-SPRing.

### CTC PM Support

In Release 4.0, when traffic is switched from the working to the protection span, standard SONET and SDH Near End Path PM values are available over the protection span in the 2-fiber or 4-fiber MS-SPRing.

## Related Documentation

### Release-Specific Documents

- *Release Notes for Cisco ONS 15454 SDH Release 3.4.1*
- *Release Notes for Cisco ONS 15454 Release 4.0*
- *Release Notes for Cisco ONS 15327 Release 4.0*

### Platform-Specific Documents

- *Cisco ONS 15454 SDH Installation and Operations Guide, Release 4.0*
- *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide, Release 4.0*
- *Cisco ONS 15454 SDH Product Overview, Release 4.0*

## 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](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](mailto: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.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0301R)

Copyright © 2003, Cisco Systems, Inc.  
All rights reserved.

