Release Notes for Cisco ONS 15600 SDH Release 8.0

January 04, 2008

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 15600 SDH. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to Release 8.0 of the *Cisco ONS 15600 SDH Procedure Guide, Cisco ONS 15600 SDH Reference Guide, Cisco ONS 15600 SDH TL1 Command Guide, and Cisco ONS 15600 SDH Troubleshooting Guide.* For the most current version of the *Release Notes for Cisco ONS 15600 SDH Release 8.0*, visit the following URL:

http://www.cisco.com/en/US/docs/optical/15000r8_0/release/notes/655RN80.html

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

http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

Contents

CISCO SYSTEMS

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 15600 SDH Release 8.0* since the production of the Cisco ONS 15600 SDH System Software CD for Release 8.0.

No changes have been added to the release notes for Release 8.0.

Caveats

Review the notes listed below before deploying the ONS 15600 SDH. Caveats with tracking numbers are known system limitations that are scheduled to be addressed in a subsequent release. Caveats without tracking numbers are provided to point out procedural or situational considerations when deploying the product.

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 When the Cisco ONS 15600 SDH is used in the Data Communications Network (DCN) as a Gateway Network Element (GNE), Cisco Systems, Inc. recommends that:

a. Each Cisco ONS 15600 SDH GNE should cater to no more than 64 Data Communications Channels (DCC)-connected External Network Elements (ENE).
b. No ENE should be more than 8 DCC hops away from its GNE.
c. With large networks, the Cisco Transport Controller (CTC) Java Virtual Machine (JVM) Heap Size should be set to 512 MB (default is 128 MB).
d. When running R7.2.1 and above, the ONS 15600 SDH GNE should be declared a SOCKS proxy in CTC preferences.
e. The number of simultaneous CTC sessions on the network should be limited to five.

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.

Line Cards

CSCuk47837

On an STM 64 card the far-end MS-SES and far-end MS-UAS counters are not incremented. As a consequence the related threshold crossing alerts are never raised. The far-end MS-SES and far-end MS-UAS counters work correctly on MS-RDI defects. This is a hardware limitation.

MS-SPRing

CSCed20559

Rarely, if, using TL1, you issue an EXERCISE-RING on the east span of a two-fiber multiplex-section shared protection ring (MS-SPRing) and then immediately issue an EXERCISE-RING on the west span of the same two-fiber MS-SPRing, one of the requests might become stuck. If this occurs, wait 10 seconds and then issue another EXERCISE-RING on the east span. This issue will be resolved in a future release.

SNCP

CSCed39435

A manual switch request remains in place even after the path switches due to failure. The switch state should become APS_CLEAR, but remains MANUAL. This issue will be resolved in a future release.

Resolved Caveats for Release 8.0

The following caveats are resolved in Release 8.0.

Maintenance and Administration

CSCuk47105

A HELLO alarm is raised when a port is put out of service, because the DCC link is taken down (hence OSPF hello failure, when the port is out of service). The HELLO alarm will be present on a port even though the port is out of service and most alarms are masked for out of service ports. This issue is resolved in Release 8.0.

CSCed29830

Circuit creation via CTC using auto-range incorrectly puts up circuits from the source node to the source node if bandwidth runs and is unavailable on the connecting DCC spans during the auto-ranged circuit creation. To avoid this issue, create the circuits individually instead of ranging the circuits if you have insufficient bandwidth on the links between the nodes. This issue is resolved in Release 8.0.

CSCec82095

A DCC in CTC grays out and does not come back if the DCC between two interconnected rings goes down (or is deleted) on one end. For this to occur, the login node and topology node must not be the same node. Also, the login node must lose visibility to the topology node when the DCC goes down. If the issue does occur, restart the active CTC session, or ensure that both sides of the DCC termination have been deleted. Either action will update the CTC session OSPF information, allowing CTC to choose another topology host that is accessible. This issue is resolved in Release 8.0.

SNCP

CSCed47156

When you manually create an open-ended SNCP circuit (two sources and one drop), only spans originating from the primary source are selectable. CTC does not allow you to select spans originating from the secondary source. Since the route is incomplete, manual creation of an open-ended SNCP circuit always fails. To work around this, when creating an open-ended SNCP circuit, select both Route Automatically and Review Routes before creation options in the “Circuit Routing Preferences” pane, then edit the spans in the “Route Review and Edit” pane. This issue is resolved in Release 8.0.

Interoperability

CSCed42362

When the ONS 15600 SDH interoperates with an NE that does not transmit bidirectional mode information in bits 6-8 of the K2 byte, for 1+1 APS bidirectional mode operation, the following APS defect alarms are not declared in SDH mode:

- FEPRLF
- APSM
- APSCM
- APSB

This issue is resolved in Release 8.0.

New Features and Functionality

This section highlights new features and functionality for Release 8.0. For an overview of all features of the 15600 SDH, consult the user documentation.

New Hardware

Customer Access Panel

The Customer Access Panel (CAP or CAP2) is located in the middle on the rear of the shelf. The CAP and CAP2 provide an alarm pin field, timing, and LAN connections. The CAP or CAP2 plugs into the backplane using 2mm Hard Metric connectors with 752 pins and is held in place with one large captive bolt and multiple screws.

The CAP2 has the additional capability of providing provisionable power monitoring.

Note The ONS 15600 SDH supports only T1 (100 ohm) building integrated timing supply (BITS).

The ONS 15600 CAP and CAP2 provide the following features:

- BITS T1 (100 ohm) interfaces via wire-wrap pins.
- Two Ethernet interfaces via RJ-45 connectors with internal transformer isolation.
- An EIA/TIA-232 craft interface via DB-9 connectors. This interface is surge-protected and provides
- EMI filtering. Two interfaces are provided for redundancy.
- Four audio alarm interfaces via a DB-15 connector that is surge-protected and EMI-filtered. The audio alarm indication is provided by the Timing and Shelf Controller (TSC) card and this interface can receive a signal to disable the audio alarm.
- Four visual alarm interfaces via a DB-15 connector that is surge-protected and EMI-filtered. The visual alarm indication is provided by the TSC card and the signal is connected to the PDU where LEDs indicate the alarm status and severity.
- Environmental (external) alarms and controls (16 inputs and 16 outputs) via wire-wrap pins. The interface is surge-protected and provides isolation by using an opto-isolator for alarm inputs and relays for alarm outputs. By connecting to different wire-wrap pins on the CAP/CAP2, the alarm outputs can be configured for either normally open (NO) or normally closed (NC) operation. Alarms are initiated by shorting these contacts. The alarm input interface provides a pair of positive and negative wire-wrap pins.

The isolation and termination meet the intra-building lightning surge specification in Telcordia GR-1089. The CAP and CAP2 have –48 VDC monitoring with an I2C interface and nonvolatile memory to store the CAP/CAP2 revision information.

If the CAP/CAP2 fails, the node raises an EQPT alarm. You can replace the CAP/CAP2 on an in-service node without affecting traffic. To replace a CAP, refer to the *Cisco ONS 15600 Procedure Guide*. Always replace the CAP during a maintenance window.

SSXC Card

The SSXC is the central element for ONS 15600 SDH switching. The SSXC card establishes connections and performs time division switching (TDS) at VC3 and VC4-Nc levels between ONS 15600 SDH traffic cards.

The SSXC card works with the TSC card to maintain connections and set up cross-connects within the ONS 15600 SDH. You establish cross-connect and provisioning information using CTC or TL1. The TSC card stores the proper internal cross-connect information and relays the setup information to the SSXC card.

SSXC Switch Matrix

The switch matrix on each SSXC card consists of 6,144 bidirectional VC3 ports, with a maximum of 6,144 bidirectional VC3 cross-connections. When creating bidirectional VC3 cross-connects, each bidirectional cross-connect uses two VC3 ports, with the result that the SSXC card supports 3,072 bidirectional VC3 cross-connects. Any VC3 on any port can be connected to any other port, meaning that the STS cross-connections are nonblocking. Nonblocking connections allow network operators to connect any VC3, VC4, VC4-4c, VC4-8c, VC4-16c, or VC4-64c payload that is received on an STM-16 or STM-64 interface (or additionally any VC4-2c and/or VC4-3c payload that is received on an ASAP interface) to any other interface capable of supporting the bandwidth.

The SSXC card has 128 input ports and 128 output ports capable of VC4-16c. A VC3 on any of the input ports can be mapped to an VC3 output port, thus providing full VC3 time slot assignments (TSAs).

SSXC Slots and Connectors

Install an SSXC card in Slot 6 and a second SSXC card in Slot 8 for redundancy. (Slots 7 and 9 are also occupied by the SSXC faceplates.) The SSXC card has no external interfaces. All SSXC card interfaces are provided on the ONS 15600 SDH backplane.

OC48 ELR/STM16 EH 100 GHz Cards

Thirty-seven distinct OC48 ELR/STM16 EH 100 GHz cards provide the ONS 15454 DWDM channel plan. Each OC48 ELR/STM16 EH 100 GHz card has one SONET OC-48/SDH STM-16 port that complies with Telcordia GR-253-CORE, ITU-T G.692, and ITU-T G.958.

The port operates at 2.49 Gbps over a single-mode fiber span. The card carries VT, concatenated (STS-1), and nonconcatenated (STS-1, STS-3c, STS-6c, STS-12c, or STS-48c) payloads.

Any Service Any Port Card

The ASAP card provides up to 16 Telcordia GR-253-CORE compliant, SDH STM-1, STM-4, STM-16, or Gigabit Ethernet ports, or up to 4 Telcordia GR-253-CORE compliant, SDH STM-64 ports, in any combination of line rates. The ASAP card, when used with the 4-Port I/O (4PIO) module, has up to 16 physical connector adapters (known as Small Form-factor Pluggables [SFPs]). The SFP ports operate at up to 2488.320 Mbps over a single-mode fiber. The ASAP card, when used with the 1-Port I/O (1PIO) module, has up to 4 physical connector adapters (known as 10Gigabit Small Form Factor Pluggables [XFPs]). The XFP ports operate at up to 9953.280 Mbps over a single-mode fiber. Both XFP and SFP physical connector adapters have two fibers per connector adapter (transmit [Tx] and receive [Rx]). The ASAP card supports VC3 payloads and concatenated payloads at VC4, VC4-2c, VC4-3c, VC4-4c, VC4-8c, VC4-16c and VC4-64c signal levels. The ASAP card is interoperable with ONS 15454 SDH E-Series, G-Series, and ML-Series Ethernet cards.

There are three major components to the ASAP card:

- Carrier card, which can be installed in Slots 1 through 4 and 11 through 14
- 4PIO and 1PIO modules, also called Pluggable Input/Output Module (PIMs), which plug into the ASAP carrier card
- SFPs/XFPs, called Pluggable Port Modules (PPMs) in CTC, which plug into the 4PIO or 1PIO (PIM) module and provide the fiber interface using a female LC connector

For card level indicators, port level indicators, and port numbering consult the *Cisco ONS 15600 SDH Reference Manual.*

ASAP Card Application

The ASAP Carrier Card plugs into any of the eight available I/O slots for the ONS 15600 SDH. Each ASAP carrier card has four slots available for up to and including four ASAP Pluggable Input/output Modules (PIMs). There are four slots available on each PIM for Pluggable Port Modules (PPMs), which are Small Form-factor Pluggable (SFP) optics. Four PPMs per ASAP PIM are allowed, which means that there can be as many as 16 PPM optical network interfaces for each ASAP carrier card. Each PPM port can support any of the following SFP optics modules:

- ONS-SI-155-L2 single rate optics module, supporting the STM-1 LR-2 rate
- ONS-SI-622-L2 single rate optics module, supporting the STM-4 LR-2 rate
- ONS-SE-2G-L2 single rate optics module, supporting the STM-16 LR-2 rate
- ONS-SE-Z1 multi-rate optics module, supporting the following rates:
  - STM-1 SR-1
  - STM-4 SR-1
  - STM-16 IR-1
  - GE LX

Each ASAP 4port I/O (ASAP_4PIO) PIM is hot-pluggable while other ports on other PIMs are functional. Each SFP is also hot-pluggable.

Layer 1 Ethernet transport is implemented for Gigabit Ethernet (GE) interfaces. GE traffic is generic framing procedure (GFP), ITU X.86, or Cisco high-level data link control/LAN extension (HDLC/LEX) encapsulated and mapped into an SDH payload.

The data path processing consists of:

- Optical-to-electrical conversion (O/E) and electrical to optical (E/O) on the ASAP_4PIO PIM
- Gigabit Ethernet to Ethernet over SDH (EoS) mapping (for the GE ports only)

Note For a single flow of Gigabit Ethernet, traffic can be mapped to a VC4-16c. This choice limits maximum usable Ethernet ports to eight when all are mapped to VC4-16c. Any time a VC4-16c is used for an Ethernet connection, one-eighth of the total card bandwidth is consumed on the EoS mapper. If you want to use all 16 ports for Gigabit Ethernet, each port should be mapped to VC4-8c or less bandwidth.

Ethernet facilities on the ASAP card include:

- Ethernet ports can be provisioned on a multirate PPM.
- Encapsulation methods allowed for the Ethernet ports are:
  - Cisco HDLC/LEX
  - GFP
  - ITU X.86

For specifics on Ethernet operation, framing, mapping, etc. using the ASAP card refer to the *Cisco ONS 15600 SDH Reference Manual*.

One-Port I/O Module for STM-64 Support on ASAP Cards

Release 8.0 supports a new 1-Port I/O (1PIO) module, also called a Pluggable Input/Output Module (PIM), which plugs into the ASAP carrier card. With the Release 8.0 1PIO module the ASAP card provides up to four STM-64 ports per card. The ports operate at up to 2488.320 Mbps over a single-mode fiber. The ASAP card, when used with the new 1PIO module, supports up to four physical connector adapters (known as Small Form-factor Pluggables [SFPs or XFPs]), with two fibers per connector adapter (transmit [Tx] and receive [Rx]), for use with STM-64 line rates.

New ASAP Connectors

The following XFPs are new for Release 8.0, and work with the 1PIO only:

- ONS-XC-10G-S1
- ONS-XC-10G-L2

An ASAP carrier card supports up to four 1PIO/PIMs for STM-64 LR-2 line rates. Each 1PIO supports one SFP/XFP. The maximum configuration for an ASAP card using 1PIOs is 4 SFP/XFP ports. These ports can each be provisioned as STM-64 LR-2 line rate.

STM16 DWDM SFPs for the ASAP 4PIO

With Release 8.0 the OC-48/STM16 supports 32 DWDM channel SFPs that can be plugged into the four port ASAP 4PIO. The following parameters are common across all 32 SFPs.

- Receiver Wavelength: 1260 to 1620 nm
- Minimum Overload: -9 dBm
- Maximum Reflectance of Receiver, measured at Rs: -27 dB
- Maximum Receiver Power, Damage Threshold: +5 dBm
- Transmitter Output Power Min/Max (dBm): 0 to +4 dBm

For further details, including a list of the SFPs by their name and associated operating wavelengths consult the user documentation.

New Software Features

Network Circuit Automatic Routing Overridable NE Default

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

The new NE default supporting this feature is:

CTC.circuits.RouteAutomaticallyDefaultOverridable

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

CTC.circuits.RouteAutomatically

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

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

- Using Required Nodes/Spans
- Review Route Before Creation

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

Daylight Savings Time Support

With Release 8.0 CTC and TL1 display daylight savings time (DST) in keeping with the new DST rules applicable from 2007 forward. As described in the change in energy policy for the United States of America (USA), the DST start date will be the 2nd Sunday of March and the DST end date will be 1st Sunday of November.

Server Trails

Release 8.0 adds support for server trails. A server trail is a non-DCC link across a third-party network that connects two CTC network domains. A server trail allows circuit provisioning when no DCC is available. You can create server trails between any two STM-N ports. Server trails are not allowed on DCC-enabled ports.

The server trail link is bidirectional and can be VC4-2c, VC4-3c, VC4-4c, VC4-6c, VC4-8c, VC4-12c, VC4-16c, VC4-64c, VC4, VC3, VC12, or VC11; you cannot upgrade an existing server trail to another size. A server trail link can be one of the following protection types: Preemptible, Unprotected, and Fully Protected. The server trail protection type determines the protection type for any circuits that traverse it. PCA circuits will use server trails with the Preemptible attribute.

When creating circuits or VCATs, you can choose a server trail link during manual circuit routing. CTC may also route circuits over server trail links during automatic routing. VCAT common-fiber automatic routing is not supported.

Link Consolidation

CTC provides the ability to consolidate the DCC, general communications channel (GCC), optical transport section (OTS), server trail, and provisionable patchcord (PPC) links shown in the network view into a more streamlined view. Link consolidation allows you to condense multiple internodal links into a singular link. The link consolidation sorts links by class, meaning that all DCC links are consolidated together, for example. You can access individual links within consolidated links using the right-click shortcut menu. Each link has an associated icon.

Link consolidation is only available on non-detailed maps. Non-detailed maps display nodes in icon form instead of detailed form, meaning the nodes appear as rectangles with ports on the sides. Refer to the *Cisco ONS 15600 SDH Procedure Guide* for more information about consolidated links.

Data Communications Network Tool

Release 8.0 CTC includes a data communications network (DCN) tool that assists with network troubleshooting for Open Shortest Path First (OSPF) networks. This tool, located in network view, executes an internal dump command to retrieve information about all nodes accessible from the entry point. The retrieved information is the same as you would get if you were to execute a dump using special networking commands. The contents of the dump file can be saved or printed and furnished to Cisco Technical Support for use in OSPF network support.

Advanced Circuit Filtering and Export

Release 8.0 adds an Advanced tab to the Circuit Filter dialog. With advanced circuit filtering you can filter on selected rings, nodes, links, or source/drop combinations.

Also, you can export the active Circuit window data in HTML, comma-separated values (CSV), or tab-separated values (TSV) format using the Export command from the File menu.

Local Domain Creation and Viewing

With Release 8.0 a Superuser can control whether domains that any future users create and view persist globally (for all CTC sessions), or only locally (within the current CTC session in which they are created), as well as who can create domains (all users, or just Superusers). This control is given to Superusers by means of the NE default, CTC.network.LocalDomainCreationAndViewing. The factory pre-set default value is FALSE, meaning domain information is applied to all CTC sessions and only Superusers can create a domain or add a node to a domain. Setting the default to TRUE enables the option for local domain creation by any user.

MS-SPRing VC4/VC3 Squelching

Release 8.0 supports MS-SPRing VC4 and VC3 squelching for the ONS 15600 SDH. MS-SPRing squelching is performed on VC4s that carry VC4 circuits only, or on VC3s that carry VC3 circuits only. MS-SPRing VC4 and VC3 squelch tables show VC4s/VC3s that will be squelched for every isolated node, providing MS-SPRing VC4/VC3 numbers, and East and West source and destination information.

The ONS 15600 SDH platform does not support low-order path squelching; however, when an ONS 15454 SDH and an ONS 15600 SDH are in the same network, the ONS 15600 SDH node allows the ONS 15454 SDH node to carry low-order path circuits in a VC_LO_PATH_TUNNEL. The ONS 15600 SDH performs 100-ms VC4-level squelching for each low-order-access VC at the switching node in case of a node failure.

"Ring is Squelching VC Traffic" Condition

The ONS 15600 SDH Release 8.0 supports an informational Ring is Squelching VC Traffic (MS-SQUELCH-HP) condition that can be raised on an STM-N facility. The MS-SQUELCH-HP condition indicates that traffic is squelched due to node failure (traffic outage). If the node failure scenario includes the source or destination node, switching the nodes will squelch all the VCs that originate from or terminate to the failed node. The condition resolves when the node is no longer failing.

Enhanced Security Features

Security Policy Enhancements

With Release 8.0 the range of days over which you can enforce disabling of inactive users has increased. The previous range was 45 to 90 days. The new range is 1 to 99 days.

With Release 8.0 enforced single concurrent user session applies to EMS, TL1, telnet, SSH, sftp, and ftp. This support applied only to EMS and TL1 in previous releases.

In Release 8.0 you can set how many characters difference must exist between a user's old password and the next new password in a range of one to five characters.

Superuser Privileges for Provisioning Users

With Release 8.0 Superusers can grant permission to Provisioning users to perform a set of tasks, including retrieving the audit log, restoring a database, clearing performance monitoring (PM) parameters, activating a software load, and reverting a software load. These privileges can only be set using the node-level network element (NE) defaults, with the exception of the PM clearing privilege, which can be granted to a Provisioning user from the CTC Provisioning > Security > Access tabs. For more information about setting up Superuser privileges, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Secure Shell Encryption and Node Access Security

In previous releases the ONS platforms supported SSH version 2 (SSHv2) as an alternative to the ability to telnet into a node (shell access). In Release 8.0 SSH encrypts all traffic (including passwords) to effectively eliminate unwanted monitoring of node activity. SSHv2 also supports access to the line card shell via shelf controller (that is, via relay).

In Release 8.0 all HTTP access to a node (for example, database backup, bulk PM retrieval, or software download) allows the use of HTTPS.

In previous releases any service type supported by ONS software could access ONS nodes. In Release 8.0 node access can be controlled by service type. Each service type from which you can access a node in Release 8.0 is configurable to support a choice of access states. The available states are non-secure (the default), secure (via SSHv2), and disabled (deny access from this service type). The SSHv2 secure state is supported for shell and ftp (using sftp), TL1, and EMS access types. Only nonsecure and disabled modes are supported for SNMP access.

RADIUS Security

As of Release 8.0 users with Superuser security privileges can configure nodes to use Remote Authentication Dial In User Service (RADIUS) authentication. Cisco Systems uses a strategy known as authentication, authorization, and accounting (AAA) for verifying the identity of, granting access to, and tracking the actions of remote users.

RADIUS Authentication

RADIUS is a system of distributed security that secures remote access to networks and network services against unauthorized access. RADIUS comprises three components:

- A protocol with a frame format that makes use of User Datagram Protocol (UDP)/IP
- A server
- Clients

The server runs on a central computer, while clients reside in the dial-up access servers and can be distributed throughout the network.

An ONS node operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and returning all configuration information necessary for the client to deliver service to the user. RADIUS servers can act as proxy clients to other kinds of authentication servers. Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. User passwords are sent encrypted between the client and RADIUS server. This eliminates the possibility that someone illicitly monitoring an unsecured network might detect a user's password.

An ONS node acting as a RADIUS client can request authentication from up to ten hierarchically arranged RADIUS servers. RADIUS security provisioning features are located in the Provisioning > Security > RADIUS tabs. For further details and operation of RADIUS security features consult the user documentation.

RADIUS Session Time Limits

Release 8.0 RADIUS supports RADIUS session time limits. This feature applies only when a RADIUS server is used for authentication. When RADIUS indicates that a session is to have a time limit, that session is terminated immediately after the time expires. There is no local database support for session time limits. Rather, when EMS users are forcibly logged out by the RADIUS server, they are presented with a notification dialog box indicating that they have been forcibly logged out due to session time expiration. Similarly, when a TL1 user is logged out, an autonomous REPT_EVT_SESSION is sent. After a TL1 user is logged out, the next command the user enters receives a DENY response with a reason code of PLNA (Login Not Active).

AAA Server Enable/Disable

In Release 8.0 RADIUS a Superuser can turn AAA server authentication on or off. When AAA server authentication is turned off, the local security policy and settings are employed for user authentication. When AAA server authentication is enabled, it applies to all NE management services, overriding local settings where the two conflict.

Note The following security policy features are not available when AAA server authentication is used:

- Idle user timeout (RADIUS user session timeouts are employed instead)
- Single session per user
- Forced password change at first login (global policy)
- Forced password change at next login (individual user)
- Password change prevention
- Excess failed login attempt lockout
- Password reuse prevention
- Inactive account disable
- Password expiration

AAA server authentication can be set in the node view > Provisioning > Defaults tabs. The default for AAA server authentication is OFF.

Audit Trail Enhancements

The following features enhance your ability to monitor node and network activity through use of the audit trail in Release 8.0.

- Archival of the audit trail in TL1, with a supporting archival failure transient alarm, AUD-ARCHIVE-FAIL
- Tracking of all Release 8.0 supported failed login types (incorrect password, disabled account, locked account, single login per user per node denial)
- Shell session login, logout, and activity trail
- Tracking of FTP/sftp logins and logouts
- Sustained audit trail for all logins and logouts whether or not an AAA server is used for user authentication
- Tracking of all user attempts to log in to the node
- When a login is denied, the audit trail records the reason (type of login failure)

CTC Enhanced Security Support

Note All of the security options and settings described in this section are available to Superuser level users. For specific security levels for any given feature, consult the user documentation.

CTC provides several user-configurable security features in the following subtabs under the The CTC node view Security tab.

- Users
- Active Logins
- Policy
- Access
- RADIUS

The Active Logins, Policy, Access, and RADIUS tabs support new features for Release 8.0, as described below.

Active Logins

The Active logins tab supports session management for Release 8.0. The Active Logins tab displays current login status information for the network. In previous releases the Active Logins tab displayed only which users were logged in, and the IP address from which each user was logged in. As of Release 8.0, in addition to user names and IP addresses, the Active Logins tab displays the specific node to which the user is logged in, the type of session used to log in, the date and time each user logged in, and the last date/time each user was active during the login. You can refresh the Last Activity Time by clicking the Retrieve Last Activity Time button. You also have the option to log out selected sessions. This feature logs out any selected sessions immediately, and interrupts any activities associated with those sessions. When you log out an active user session you have the option to lock the user out (from future sessions) prior to the logout.

In Release 8.0 the following services are monitored in the Active Logins tab.

- TL1

- EMS
- FTP
- sftp
- telnet shell sessions (via serial port only; not the debug port)
- SSH shell sessions

Policy

The Policy tab supports user security policy options. The Policy tab provides security policy settings and options. In previous releases the Policy tab provided the following functionality, in five display areas, in which settings could be applied:

- Idle User Timeout—Sets the hours and minutes a user can remain idly logged in before a timeout will occur; settings are provided for each user level.
- User Lockout—Sets the number of times a user can fail an attempt to log in before a lockout will occur, with an option to enforce manual unlocking of the user name by a Superuser, or alternatively, to set the lockout duration in minutes and seconds. Login failure types include:
  - Incorrect password
  - Disabled account
  - Locked account
  - Single login per user per node denial
- Password Change—Sets the number of unique passwords that must be used before a single password can be reused. Sets the option to disable changing of passwords for a fixed, user-configurable number of days. Sets the option to require a password change on first login to a new account.
- Password Aging—Enables you to optionally set a fixed number of days for each user security level (after which time a warning will be issued to create a new password), and to set a fixed number of days after which the password will actually expire and the user will no longer be able to log in.
- Other—Sets the option to enforce a single concurrent session per user (EMS and TL1 only). Also sets the option to enforce disabling of inactive users for users inactive a specified number of days; for example, if this feature is checked, with 90 days selected, a user ID that has not logged in for 90 days or more will be unable to log in again.

With Release 8.0, in the “Other” area, enforced single concurrent user session applies to EMS, TL1, telnet, SSH, HTTP, sftp, and ftp, and also, the range of days over which you can enforce disabling of inactive users has increased. The new range is 1 to 99 days.

Release 8.0 also adds a new Password Change configuration that sets how many characters difference must exist between the old password and the new password in a range of one to five characters.

Node Access

The Access tab supports node access options, including enhanced SSH secure connection support for Release 8.0. The Access tab provides settings and options for each type of access that can be used to reach the node. In previous releases, the Access tab included the following three areas for applying node access settings and options.

- LAN Access—Sets the option of None, Front only, Backplane only, or Front and Backplane. Also includes a “Restore Timeout” setting, configurable in minutes.
- Shell Access—Sets a choice between Telnet, with a configurable port number, and SSH, with a fixed port number.

- Other—Sets the PM clearing privilege as Provisioning or Superuser.

With Release 8.0 the Access tab provides four new areas, plus functional changes to the Shell Access area, for a total of seven areas in which settings can be applied as follows.

- LAN Access—(Same as in previous releases.) Sets the option of None, Front only, Backplane only, or Front and Backplane. Also includes a “Restore Timeout” setting, configurable in minutes.
- Serial Craft Access—Sets the option to enable or disable the shelf controller serial craft port.
- Shell Access—Sets the Access security state for shell logins as Disable, Nonsecure, or Secure. Sets the configurable Telnet Port. Sets the option to Enable Shell Password.
- EMS Access—Sets the Access security state for EMS logins as Nonsecure or Secure. Sets the Corba IIOP Listener Port.
- TL1 Access—Sets the Access security state for TL1 logins as Disable, Nonsecure, or Secure.
- SNMP Access—Sets the Access security state for SNMP logins as Disable or Nonsecure.
- Other—(Same as in previous releases.) Sets the PM clearing privilege as Provisioning or Superuser.

RADIUS

The RADIUS tab is new for Release 8.0, and supports the new RADIUS security features, including RADIUS server management, authentication, accounting, and management of shared secrets. The RADIUS tab provides an area for setting the options to:

- Enable RADIUS Authentication
- Enable RADIUS Accounting
- Enable the given node as the final Authentication when no RADIUS server is reachable

The RADIUS tab also provides a display area for RADIUS servers, in order of authentication preference. This area displays the IP Address, Shared Secret, Authentication Port, and Accounting Port for each RADIUS server.

In the RADIUS tab you can create a RADIUS server by clicking the Create button. The RADIUS tab also provides the following additional actions, which can be performed upon selected server(s).

- Edit
- Delete
- Move up (in order of Authentication)
- Move down (in order of Authentication)

For information on using and configuring RADIUS features in Release 8.0 consult the user documentation.

IP and OSI on DCC

As of Release 8.0, IP and OSI can coexist on DCC on a Cisco ONS network, addressing legacy OSI via NSIF Mediation, and allowing migration into IP via G.7712. IP on DCC provides security through strong encryption, SSH, SSL, and HTTPS; centralized control and strong authentication (AAA); RADIUS; communication to Layer 2 and Layer 3 devices (IP + Optical); and pseudo wire, in support of the interworking function between IP and OSI. The ability to address IP/OSI issues gives you flexibility for the future, while working within existing DCN/DCC/OSS infrastructure.

Release 8.0 uses PPP, a Layer 2 encapsulation protocol, with high-level data link control (HDLC) datagram encapsulation to transport IP and OSI data, and link control protocol (LCP) to establish, configure, and test the point-to-point connections. CTC automatically enables IP over PPP whenever you create an RS-DCC or MS-DCC. The RS-DCC or MS-DCC can also be provisioned to support OSI over PPP. Link access protocol on the D channel (LAP-D), a data link protocol used in the OSI protocol stack, provides provisionable parameters when you elect to provision an ONS RS-DCC as OSI only.

Release 8.0 TCP/IP and OSI networking employs the following additional features, described in detail in the user documentation.

OSI Connectionless Network Service

OSI connectionless network service is implemented by using the Connectionless Network Protocol (CLNP) and Connectionless Network Service (CLNS). CLNP and CLNS are described in the ISO 8473 standard.

OSI Routing

OSI routing uses a set of routing protocols that allow end system and intermediate system information collection and distribution; a routing information base; and a routing algorithm (shortest path first).

TARP

TID Address Resolution Protocol (TARP) is used when TL1 target identifiers (TIDs) must be translated to network service access point (NSAP) addresses.

TCP/IP and OSI Mediation

Two mediation processes, T-TD and FT-TD, facilitate TL1 networking and file transfers between NEs and ONS client computers running TCP/IP and OSI protocol suites.

OSI Virtual Routers

Release 8.0 supports three OSI virtual routers, provisionable on the Provisioning > OSI > Routers tab.

IP-over-CLNS Tunnels

IP-over-CLNS tunnels are used to encapsulate IP for transport across OSI NEs. Release 8.0 supports two tunnel types, Generic Routing Encapsulation (GRE) and Cisco IP.

OSI Provisioning in CTC

The following OSI features are provisionable in the CTC node view, Provisioning tab. For full explanations of CTC provisioning for OSI, consult the user documentation.

- OSI setup
- TARP configuration, static TDC, and MAT
- Router setup and subnets
- Tunnels
- Communication channels

CTC Launcher

Release 8.0 introduces the CTC Launcher utility, CtcLauncher.jar. The CTC Launcher utility can be used to launch CTC and manage an ONS node running Release 8.0 or higher.

CTC Launcher provides two connection options. First, it can be used to access ONS NEs that have IP connectivity to the CTC computer (supported for the ONS 15600 and ONS 15600 SDH). Second, CTC Launcher can establish connectivity to ONS NEs that reside behind a third party, OSI-based GNE (supported for other ONS platforms). To create a connection through the OSI-based GNE, CTC Launcher creates a TL1 tunnel. This tunnel is similar to the static IP-over-CLNS tunnels that are available in CTC Release 6.0.x. (For information about IP-over-CLNS tunnels, refer to the Release 6.0 ONS product documentation.) However, unlike the static IP-over-CLNS tunnels, the TL1 tunnel does not require provisioning on the third party GNE, the DCN routers, or the ONS NEs. The tunnel connection is created using the CTC Launcher. It can then be managed using CTC.

Note To establish a TL1 tunnel, the ONS node behind the GNE must be running Release 8.0 or higher.

Prior to using the CTC Launcher utility, the CTC jar files must be precached, either from the installation CD, using the LDCACHE utility, or from the node, by launching CTC from a web browser. For installation instructions for the CTC Launcher utility, consult the readme file. The CtcLauncher.jar utility and the CtcLauncher-README.txt file are located in the CtcLauncher directory on the R8.0 software CD. For additional information about CTC Launcher, refer to the CTC Launcher Application Guide. To access the application guide:

Step 1 Go to http://www.cisco.com.

Step 2 Choose Technical Support & Documentation.

Step 3 Choose Optical Networking.

Step 4 Choose the ONS 15300, ONS 15400, or ONS 15600 product category.

Step 5 Choose the Configuration Guides category.

Step 6 Click the CTC Launcher Application Guide link under the appropriate product.

GFP-F Framing

Generic Framing Procedure (GFP) defines a standard-based mapping for different types of services onto SONET/SDH. With Release 8.0 the ASAP card supports frame-mapped GFP (GFP-F), the PDU-oriented client signal adaptation mode for GFP. GFP-F maps one variable length data packet onto one GFP packet. GFP defines common functions and payload specific functions. Common functions are those shared by all payloads. Payload-specific functions differ depending on the payload type. The GFP standard is detailed in ITU recommendation G.7041.

Provisionable Framing Mode

Release 8.0 provides a method to provision framing mode in the card view, Provisioning > Card tab, which displays the framing mode selections for the card in a drop-down list, and allows you to change the framing mechanism to either HDLC or GFP-F. You can also preprovision the framing mode prior to installing the card, and the card will boot up in the pre-provisioned mode. For details on framing mode provisioning consult to user documentation.

Pluggable Port Module Support

Release 8.0 supports small form-factor pluggables (SFPs), also known as Pluggable Port Modules (PPMs), for the ONS 15600 SDH ASAP card.

The following table lists the available SFPs for the Cisco ONS 15600 SDH.

Table 1 SFP Compatibility

Card	Compatible SFP (Cisco Product ID)	Cisco Top Assembly Number (TAN)
ASAP 4PIO only (ONS 15600 SDH SONET/SDH)	ONS-SE-2G-L2 ONS-SE-Z1 ONS-SI-622-L2 ONS-SI-155-L2 ONS-SC-2G-46.1 through 60.6 ONS-SC-2G-30.3 through 44.5 ONS-SI-2G-S1	10-2013-01 10-1971-01 10-1936-01 10-1937-01 10-2170-01 through 10-2184-01, and 10-2186-01 10-2155-01 through 10-2169-01, and 10-2185-01 10-1992-01

For SFP applications with the ASAP card refer to the *Cisco ONS 15600 SDH Reference Manual*.

Enhanced State Model

Release 8.0 introduces new administrative and service states for Cisco ONS 15600 SDH cards, ports, and cross-connects. Administrative and service states are based on the generic state model defined in Telcordia GR-1093 Core, Issue 2 and ITU-T X.731 and are available for all support management interfaces. The following state types and state transition types are defined for Release 8.0. Consult the *Cisco ONS 15600 SDH Reference Manual* for specific states and their applications.

Service States

Service states include a Primary State (PST), a Primary State Qualifier (PSTQ), and one or more Secondary States (SST).

Administrative States

Administrative states are used to manage service states. Administrative states consist of a PST and an SST. A change in the administrative state of an entity does not change the service state of supporting or supported entities.

Service State Transitions

The possible transitions from one service state to the next state for cards, ports, and cross-connects. A service state transition is based on the action performed on the entity and any autonomous activity.

Card Service State Transitions

The service state transitions for cards.

Port and Cross-Connect Service State Transitions

Port states do not impact cross-connect states with one exception. A cross-connect in the Unlocked-disabled,automaticInService service state cannot transition autonomously into the Unlocked-enabled service state until the parent port is Unlocked-enabled.

Circuit State Model

Release 8.0 adds support for circuit service and administrative states in CTC. For more information consult the user documentation.

New Secondary State: failed

Release 8.0 introduces a new secondary service state (SST), failed. The failed secondary state is defined as follows:

- failed—The entity has a raised alarm or condition.

The failed SST is an extension to the existing ONS State Model. It identifies that the affected entity is disabled because it is faulty. The failed secondary state affects the service state only. The administrative state (the state you manage the entity into) is not affected. The failed SST is the result of autonomous action; you cannot manage an entity into the failed SST. The failed SST is for retrieval purposes only. An entity's service state will transition into an autonomously disabled service state if alarms or conditions are present. The failed SST is appended to the existing secondary state for the entity when an alarm or condition exists.

Some equipment alarms will not generate a failed SST transition. If a state already exists to represent the equipment condition, failed will not be added to the secondary state list. For further information about the failed SST consult the user documentation.

Enhanced Fault Management

Release 8.0 adds increased flexibility for fault management. When an entity is put in the Locked,maintenance administrative state, the ONS 15454 SDH suppresses all standing alarms on that entity. All alarms and events appear on the Conditions tab. You can change this behavior for the LPBKFACILITY and LPBKTERMINAL alarms. To display these alarms on the Alarms tab, you can set the default, NODE.general.ReportLoopbackConditionsOnPortsInLocked,MaintenancePorts to TRUE in the NE Defaults editor.

32 Ring Two-fiber MS-SPRing

With Release 8.0 the ONS 15600 SDH can support 32 concurrent two-fiber MS-SPRings. Each MS-SPRing can support up to 24 ONS 15600 SDHs. Because the working and protect bandwidths must be equal, you can create only STM-16 or STM-64 MS-SPRings.

In-Service Topology Upgrades

In Release 8.0 in-service topology upgrades are supported for unprotected to SNCP, and terminal to linear (add a node to a 1+1). Release 8.0 provides both manual methods and CTC wizards for completing these upgrades.

Note Traffic hits resulting from an in service topology upgrade are less than 50 ms; however, traffic might not be protected during certain upgrades: in the case where you are upgrading from unprotected to SNCP, with unidirectional routing, traffic hits might be greater than 50 ms. Cisco recommends waiting for a maintenance window to perform the topology upgrade in this case.

CTC Topology Upgrade Wizards

The following CTC topology upgrade wizard has been added for Release 8.0 to support in service topology upgrades.

Terminal to Linear—Add a Node to 1+1

The wizard for this feature is invoked by right-clicking on a 1+1 link and then selecting the "terminal to linear" option. The option adds a node between a two nodes connected by a 1+1.

Additional Support for In-Service Topology Upgrades

Circuit Routing

With Release 8.0 you can choose between manually or automatically routing SNCP circuits for a topology upgrade.

The following circuit types are supported for topology upgrades.

- Virtual container (VC)
- Unidirectional and bidirectional
- Automatically routed and manually routed
- CTC-created and TL1-created
- Ethernet (unstitched)
- Multiple source and destination (both sources should be on one node and both drops on one node)

Circuit Merge and Reconfigure

The circuit merge and reconfigure features enable you to merge selected CTC or TL1 circuits into one or more discovered CTC circuits based on the alignment of the circuit cross-connects, rather than the circuit ID.

Circuit Merge merges m circuits into one circuit. This feature takes one master circuit and merges aligned circuits with the master.

Circuit Reconfigure merges m circuits into n circuits. This feature takes m circuits and reconfigures them based on cross-connect alignment. To merge circuits choose the Merge subtab of the Edit Circuits tab in CTC. To merge circuits choose the Merge subtab of the Edit Circuits tab in CTC. To reconfigure circuits, choose the CTC Tools > Circuits tab, and select "Reconfigure Circuits..."

Dual-ring Interconnect

Dual-ring interconnect (DRI) topology provides an extra level of path protection for circuits on interconnected rings. DRI allows users to interconnect MS-SPRings, SNCPs, or an SNCP with an MS-SPRing, with additional protection provided at the transition nodes. In a DRI topology, ring interconnections occur at two or four nodes.

DRI Features

The following list provides supported MS-SPRing DRI features at a glance.

- MS-SPRing two fiber configurations
- MS-SPRing with SNCP supported at the VC high order path level (VC low order path level not supported)
- Traditional DRI and integrated (IDRI)

- Traditional four node interconnect
- Integrated two node interconnect
- MS-SPRing path level protection
- Drop and continue included
- Circuit routing, both manual and automatic
- Same side, or opposite side interconnect
- Ring interconnect on protect (RIP)
- Interconnection with mixed STMn
- Open ended DRI (supported for multi-vendor)

Note Interconnection links do not support 1+1, 1:1, or 1:n.

MS-SPRing DRI

Unlike MS-SPRing automatic protection switching (APS) protocol, MS-SPRing DRI is a path-level protection protocol at the circuit level. Drop-and-continue MS-SPRing-DRI requires a service selector in the primary node for each circuit routing to the other ring. Service selectors monitor signal conditions from dual feed sources and select the one that has the best signal quality. Same-side routing drops the traffic at primary nodes set up on the same side of the connected rings, and opposite-side routing drops the traffic at primary nodes set up on the opposite sides of the connected rings. For MS-SPRing DRI, primary and secondary nodes cannot be the circuit source or destination.

A DRI circuit cannot be created if an intermediate node exists on the interconnecting link. However, an intermediate node can be added on the interconnecting link after the DRI circuit is created.

DRI protection circuits act as protection channel access (PCA) circuits. In CTC, you set up DRI protection circuits by selecting the PCA option when setting up primary and secondary nodes during DRI circuit creation.

SNCP to MS-SPRing DRI Handoff Configurations

SNCPs and MS-SPRings can also be interconnected. In SNCP to MS-SPRing DRI handoff configurations, primary and secondary nodes can be the circuit source or destination, which is useful when non-DCC optical interconnecting links are present.

Open GNE

Release 8.0 supports open GNE configurations, through which the ONS 15600 SDH can communicate with non-ONS nodes that do not support point-to-point protocol (PPP) vendor extensions or OSPF type 10 opaque link-state advertisements (LSA), both of which are necessary for automatic node and link discovery. An open GNE configuration allows the DCC-based network to function as an IP network for non-ONS nodes. To support open GNE Release 8.0 provides provisionable foreign DCC terminations, provisionable proxy server tunnels, and provisionable firewall tunnels.

Foreign DCC termination

To configure an open GNE network, you can provision RS-DCC, MS-DCC, and GCC terminations to include a far-end, non-ONS node using either the default IP address of 0.0.0.0 or a specified IP address. You provision a far-end, non-ONS node by checking the “Far End is Foreign” check box during

RS-DCC, MS-DCC, and GCC creation. The default 0.0.0.0 IP address allows the far-end, non-ONS node to provide the IP address; if you set an IP address other than 0.0.0.0, a link is established only if the far-end node identifies itself with that IP address, providing an extra level of security.

Proxy Server Tunnels and Firewall Tunnels

By default, the SOCKS proxy server only allows connections to discovered ONS peers, and the firewall blocks all IP traffic between the DCC network and LAN. You can, however, provision proxy tunnels to allow up to 12 additional destinations for SOCKS version 5 connections to non-ONS nodes. You can also provision firewall tunnels to allow up to 12 additional destinations for direct IP connectivity between the DCC network and LAN. Proxy and firewall tunnels include both a source and destination subnet. The connection must originate within the source subnet and terminate within the destination subnet before either the SOCKS connection or IP packet flow is allowed.

To set up proxy and firewall subnets in CTC, use the Provisioning > Network > Proxy and Firewalls subtabs. The availability of proxy and/or firewall tunnels depends on the network access settings of the node. See the user documentation for further details.

State Verification Scan Before Activation

Before allowing a software activation or reversion to proceed, Release 8.0 nodes verify that their current state meets required activation criteria. Activation criteria must be met in order to avoid traffic hits. For ONS 15454, ONS 15454 SDH, and ONS 15310 nodes, all MS-SPRing spans on the node must be locked-out, and no 1:1, 1:N, 1+1 or Y-Cable protection switches can be in progress. For ONS 15600 and ONS 15600 SDH nodes, all MS-SPRing spans on the node must be locked-out.

Admin SSM

Synchronization status messaging (SSM) is a protocol that communicates information about the quality of the timing source. SSM messages enable nodes to automatically select the highest quality timing reference and to avoid timing loops. With Release 8.0 you can configure an SSM value for a timing source (either BITS-IN or Optical Line) by selecting from the “ADMIN. SSM” selection box in the BITS Facilities subtab of the node view, Provisioning > Timing tabs. This feature is useful when the selected external timing source has no SSM information. When you select the Admin SSM value, all switching decisions are subsequently made based on your selection. The same SSM value is transmitted out of the interface configured for BITS Out, and in transmit Optical S1. The DS1 BITS type with framing type SF(D4) only supports Admin SSM. The 64KHz+8KHz clock (ONS 15454 SONET) also only supports Admin SSM. ESF Framing must have Sync Messaging turned off (uncheck the check box) in order to enable Admin SSM selection. SONET nodes use the SSM Generation II message set, as defined in Table 4 of ANSI T1.101-1999. SDH nodes support SDH generation 1 SSM and STU. SONET nodes support only SONET SSM (GR-253).

STS Around Ring

Release 8.0 supports manual provisioning of contiguous concatenation (CCAT) STS circuits around the ring (traffic travels around the ring, starting and ending at the same node). In previous releases, if you selected the circuit source and destination as starting and ending on different I/O ports of the same node, the result would be an intra-node circuit only. With Release 8.0, you can manually route this type of circuit all the way around the ring. STS around the ring is supported for an unprotected path, in an unprotected ring, unless the underlying topology is line protected, in which case the around the ring circuit will also be line protected. STS around the ring is supported for all circuit sizes, starting with STS1 (SONET), or STM1 (SDH), and for all supported management interfaces.

Provisionable Patchcords

A provisionable patchcord is a user-provisioned link that is advertised by OSPF throughout the network. Provisionable patchcords, also called virtual links, are needed if an ONS 15600 SDH optical port is connected to an ONS 15454 SDH transponder or muxponder client port provisioned in transparent mode. Provisionable patchcords are required on both ends of a physical link. The provisioning at each end includes a local patchcord ID, slot and port information, remote IP address, and remote patchcord ID. Patchcords appear as dashed lines in CTC network view.

For supported combinations for ONS 15600 SDH optical cards and the ONS 15454 SDH transponder/muxponder cards used in a provisionable patchcord, refer to the *Cisco ONS 15600 SDH Reference Manual*. For more information about the ONS 15454 transponder and muxponder cards, refer to the *Cisco ONS 15454 Reference Manual*.

Optical ports have the following requirements when used in a provisionable patchcord:

- An optical port connected to an ONS 15454 SDH transponder or muxponder port requires an RS-DCC or MS-DCC termination.
- If the optical port is the protection port in a 1+1 group, the working port must have an RS-DCC or MS-DCC termination provisioned.
- If a remote end (ONS 15454 SDH) of a provisionable patchcord is Y-cable protected, an optical port requires two patchcords.

SDH J1 Path Trace Automatic Mode

With Release 8.0 the ONS 15600 SDH supports J1 path trace automatic mode through both CTC and TL1.

You can enable the SDH J1 Path Trace byte to monitor interruptions or changes to circuit traffic provisioned on the following ONS 15600 SDH cards.

- OC48/STM16 SR/SH 16 Port 1310—Receive only
- OC48/STM16 LR/LH 16 Port 1550—Receive only
- OC192/STM64 SR/SH 4 Port 1310—Receive only
- OC192/STM64 LR/LH 4 Port 1550—Receive only
- ASAP STM-N PPMs—Receive only
- ASAP Ethernet PPMs—Receive and transmit

The J1 byte transmits a repeated, 64-byte, fixed-length string. If the string received at a circuit drop port does not match the string the port expects to receive, an alarm is raised. In automatic mode, the receiving port assumes the first J1 string it receives is the baseline J1 string.

Note The ONS 15600 SDH does not support J1/IPPM for MS-SPRing.

Timing Synchronization Enhancements

Support for additional timing synchronization enhancements is added for the Release 8.0 ONS 15600 SDH. The following additional timing enhancements are supported by both CTC and TL1.

- Mixed mode timing references (external BITS, Line and Internal)
- BITS Out

- Forced switching of reference sources

For full details of timing synchronization support, refer to the *Cisco ONS 15600 SDH Reference Manual*.

CTC Enhancements

CTC Download Highest Level NET JAR File

As of Release 8.0 CTC, during network topology discovery, polls each node in the network to determine which one contains the most recent version of the CTC software. If CTC discovers a node in the network that has a more recent version of the CTC software than the version you are currently running, CTC generates a message stating that a later version of CTC has been found in the network, and offers to install the CTC software upgrade JAR files. If you have network discovery disabled, CTC will not seek more recent versions of the software. Unreachable nodes are not included in the upgrade discovery.

SSH Shell Access Option

With Release 8.0 an ONS 15600 SDH Superuser can select secure shell (SSH) as an alternative to Telnet at the CTC Provisioning > Security > Access tabs. SSH is a terminal-remote host Internet protocol that uses encrypted links. It provides authentication and secure communication over unsecure channels. Port 22 is the default port and cannot be changed.

CTC Circuits State Default

The Release 8.0 circuit creation wizard uses the new node default value, Node.circuits.State, as the default circuit state when creating a circuit. This default can be set in the NE Defaults window, and will not be overridden by the "user preferences" command feature, which caused the default value to be abandoned when using the wizard in previous releases.

Shell Login Challenge

Release 8.0 supports the requirement of a specific shell password, set initially by the first shell user and then required of subsequent shell users at login. When this feature is enabled, the password is required of all shell users (rather than each user having a separate account) from the time it is set or changed. In the CTC node view, Provisioning > Security> Access tabs, check the "Enable Shell Password" check box to enable the shell password feature. The password can then be set or changed in a telnet or SSH shell session using the "passwd" command.

Note The password should be 8 characters or less to avoid possible conflicts with certain FTP clients.

Date Format Selection

Release 8.0 adds a date format option to CTC, enabling you to choose between U.S. (MM/DD/YY) and European (DD/MM/YY) date formats. To choose the date format, click the Edit menu and choose Preferences. Select the desired date format (the default is MM/DD/YY) and click OK. The name/value pair ("ctc.dateFormat=DD/MM/YY" or "ctc.dateFormat=MM/DD/YY") will be updated in the ctc.ini (Windows), or .ctcrc (UNIX) file, where preferences are stored. Subsequently, the date format used in all tables, dialogs, and tabs will be changed to the format you selected in the Preferences dialog.

Provisionable Patchcord Tab

Provisionable patchcords, also called virtual links, are needed if an ONS 15600 SDH optical port is connected to an ONS 15454 SDH transponder or muxponder client port provisioned in transparent mode. Release 8.0 features a Provisionable Patchcord subtab in CTC that displays physical links and their associated protection types, so that, when a control channel cannot be terminated on either end of a physical link, and as a result, the physical link cannot be automatically discovered by OSPF, you can still view the physical link and its protection type in the management software interface. You can view the physical links and their terminations from the CTC network view > Provisioning > Provisionable Patchcords tabs; or from the CTC node view > Provisioning > Comm Channels > Provisionable Patchcords tabs. To provision the patchcord, you select the Node Name, Slot, Port, and ID for both ends of the physical link. The ID is a unique 16-bit number used to identify a virtual link on a node. IDs are only unique for the particular node.

TL1-CTC Circuit Unification

In Release 8.0 CTC fully supports TL1-created circuits and TL1 fully supports CTC-created circuits. Release 8.0 circuit behavior and appearance is unified across both management interfaces, and you can easily alternate between the two. It is also no longer necessary to upgrade a TL1 circuit for CTC, or to downgrade a CTC circuit for TL1. The following circuit unification enhancements are supported with Release 8.0.

- Release 8.0 cross-connects can be given names via TL1 using ENT-CRS and ED-CRS (use the “CKTID” parameter).
- CTC-created circuits can now be fully deleted if all cross-connects are deleted via TL1. (Deleting a source node cross-connect automatically deletes the CTC “circuitInfo” database object.)
- TL1 circuits now have names (like CTC circuits).
- You can use TL1 to change the name of any circuit, TL1-created or CTC-created.
- Low order (LO) tunnels and LO aggregation point circuits created via TL1 are now recognized and displayed in CTC.
- You can use TL1 to add cross-connects to a CTC-created circuit.
- You can edit TL1 circuits using CTC. (No need for upgrading the circuit first.)
- Circuit “upgrade” and “downgrade” functions have been removed.
- You can merge two or more CTC circuits into a single CTC circuit. (Circuit Merge and Circuit Reconfigure.)
- “ACTIVE” circuits are now called “DISCOVERED.”
- “INCOMPLETE” circuits are now called “PARTIAL.”
- “UPGRADABLE” circuits are now called “DISCOVERED_TL1.”
- “INCOMPLETE_UPGRADABLE circuits are now called “PARTIAL_TL1.”

SFP Management Completion

Supported services (rates, wavelengths, formats, reach, and so on) are encoded in the EEPROMs of SFPs and XFPs following industry standards. PPMs (SFPs or XFPs) that do not follow this standard cannot be read by the platform and are referred to as Unrecognized PPMs.

PPMs that are inserted into a card may be checked for the validity of an MD5 security code. PPMs failing this test are referred to as non-Cisco PPMs. PPMs passing this test as referred to in this document as Cisco PPMs.

Different cards are tested with a limited subset of Cisco PPMs. Customers are encouraged to use these PPMs, referred to as Qualified Cisco PPMs (for the particular card). Since each card supports different services (rates and formats), a PPM qualified for one card is not necessarily qualified for another. For example, a PPM qualified to work on a DWDM card may not be qualified to work on a SONET card. Cisco PPMs that are not recommended for use with a particular card are termed Unqualified Cisco PPMs (for the particular card).

Note This feature may not be described in the Release 8.0 documentation

DISA Password Complexity, Max Password Length, Min Password Length.

The password length, by default, must be set to a minimum of six and a maximum of 20 characters. You can configure the default values in node view through Provisioning > NE Defaults > Node > security > passwordComplexity. The minimum length can be set to eight, ten or twelve characters, and the maximum length to 80 characters. The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters, where at least two characters are nonalphabetic and at least one character is a special character. For TL1 compatibility, the password must be 6 to 10 characters. The password must not contain the user name.

Required JRE Version is 5.0

JRE version 5.0 was optional in Release 7.0. It is required for release 8.0 that JRE be version 5.0.

Solaris 10 Supported.

Solaris 10 is supported in release 8.0

Mozilla 1.7 Supported on Solaris 9 with Java plug-in 5.0.

Mozilla 1.7 on Solaris 9 with Java plug-in 5.0 is supported in release 8.0.

IPv6

Cisco ONS 15xxx products can function in an IPv6 network when an internet router that supports Network Address Translation - Protocol Translation (NAT-PT) is positioned between the GNE, such as an ONS 15454, and the client workstation. NAT-PT is defined in RFC-2766. IPv4 and IPv6 nodes communicate with each other using NAT-PT by allowing both IPv6 and IPv4 stacks to interface between the IPv6 DCN and the IPv4 DCC networks.

NAT-PT binds addresses in IPv6 networks with addresses in IPv4 networks and vice versa to provide transparent routing for the packets traveling between address types. This requires no changes to end nodes and IP packet routing is completely transparent to end nodes. It does, however, require NAT-PT to track the sessions it supports and mandates that inbound and outbound datagrams pertaining to a session traverse the same NAT-PT router. Protocol translation is used to extend address translation with protocol syntax/semantics translation.

Note Only Mozilla 1.7 is supported on clients interfacing with IPv6 networks.

ASAP Card Ethernet Performance Monitoring Parameters

CTC provides Ethernet performance information, including line-level parameters, port bandwidth consumption, and historical Ethernet statistics. The ASAP card Ethernet performance information is divided into Ether Ports and POS Ports windows within the card view Performance tab window.

TL1

In Release 1.4 only TL1 test access was available for the ONS 15600 SDH platform. As of Release 8.0 the full range of TL1 commands and support is available. For specific commands, syntax, and their uses, consult the *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 Command Guide*.

TL1 Command Changes

New Commands

The following new TL1 commands are added for Release 8.0.

- LIST
- DLT-NNI-ETH
- DLT-QNQ-ETH
- DLT-RMONTH-MOD2-DATA
- DLT-VLAN
- DLT-WDMSIDE
- ED-COS-ETH
- ED-ETH
- ED-L2-ETH
- ED-LMP
- ED-OTU2
- ED-QNQ-ETH
- ED-VLAN
- ED-WDMSIDE
- ENT-NNI-ETH
- ENT-QNQ-ETH
- ENT-VLAN
- ENT-WDMSIDE
- LMP-CTRL
- LMP-DLINK
- LMP-TLINK
- RTRV-COS-ETH
- RTRV-ETH

- RTRV-L2-ETH
- RTRV-NNI-ETH
- RTRV-PATH-OCH-TYPE
- RTRV-PM-ALL
- RTRV-QNQ-ETH
- RTRV-VLAN
- RTRV-WDMSIDE
- RTRV-WLEN

Removed Commands

The following commands were removed in Release 8.0.

- DLT-OSC
- ED-OSC
- ENT-OSC
- RTRV-OSC

Command Syntax Changes

The syntax of the following commands is changed in Release 8.0.

CHG-EQPT syntax changed:

CHG-EQPT[:<TID>]:<aid>:<CTAG>::<new_eqpt_type>;

CHG-EQPT[:<TID>]:<aid>:<CTAG>::<new_eqpt_type>[:PPMTYPE=<ppmtype>,][PPMNUM=<ppmnum>,][PORTNUM=<portnum>,][PORTRATE=<portrate>];

ED-APC syntax changed:

ED-APC[:<TID>]::<CTAG>[:::APCENABLE=<apcenable>][:];

ED-APC[:<TID>]:<aid>:<CTAG>[:::APCENABLE=<apcenable>][:];

The syntax of the following commands was changed from the last release:

(ALW-SWTOPROTN-EQPT enum changes:
DIRECTION)

(ALW-SWTOWKG-EQPT enum changes:
DIRECTION)

(DLT-RMONTH-MOD2-DATA enum changes
MOD2_DATA)

ED-APC syntax changed:

```
ED-APC[:<TID>]::<CTAG>[:::APCENABLE=<apcenable>][:];
ED-APC[:<TID>]:<aid>:<CTAG>[:::APCENABLE=<apcenable>][:];
```

(ED-BITS enum changes:

SYNC_CLOCK_REF_QUALITY_LEVEL)

(ED-E1 enum changes:

SYNC_CLOCK_REF_QUALITY_LEVEL)

ED-EQPT syntax changed:

```
ED-EQPT[:<TID>]:<aid>:<CTAG>[:::PROTID=<protid>,][PRTYPE=<prtype>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][CARDMODE=<cardmode>,][PEERID=<peerid>,][REGENNAME=<regenname>,][CMDMDE=<cmdmde>,][RETIME=<retime>,][SHELFROLE=<shelfrole>,][NEWSHELFID=<newshelfid>][:<pst>[,<sst>]];
```

```
ED-EQPT[:<TID>]:<aid>:<CTAG>[:::PROTID=<protid>,][PRTYPE=<prtype>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][CARDMODE=<cardmode>,][PEERID=<peerid>,][REGENNAME=<regenname>,][PEERNAME=<peername>,][CMDMDE=<cmdmde>,][RETIME=<retime>,][SHELFROLE=<shelfrole>,][NEWSHELFID=<newshelfid>,][FRPROLE=<frprole>,][FRPSTATE=<frpstate>][:<pst>[,<sst>]];
```

(ED-FAC enum changes:

PAYLOAD)

ED-FSTE syntax changed:

```
ED-FSTE[:<TID>]:<src>:<CTAG>[:::FLOW=<flow>,][EXPDUPLEX=<expduplex>,][EXPSPEED=<expspeed>,][VLANCOS=<vlancosthreshold>,][IPTOS=<iptosthreshold>,][NAME=<name>,][CMDMDE=<cmdmde>,][SOAK=<soak>][:<pst>[,<sst>]];
```

```
ED-FSTE[:<TID>]:<src>:<CTAG>[:::FLOW=<flow>,][EXPDUPLEX=<expduplex>,][EXPSPEED=<expspeed>,][VLANCOS=<vlancosthreshold>,][IPTOS=<iptosthreshold>,][NAME=<name>,][CMDMDE=<cmdmde>,][SUPPRESS=<suppress>,][SOAK=<soak>][:<pst>[,<sst>]];
```

ED-GIGE syntax changed:

```
ED-GIGE:[<TID>]:<aid>:<CTAG>:::[ADMINSTATE=<adminstate>],[LINKSTATE=<linkstate>],[MTU=<mtu>],[FLOWCTRL=<flowctrl>],[AUTONEG=<autoneg>],[HIWMRK=<hiwmrk>],[LOWMRK=<lowmrk>],[OPTICS=<optics>],[DUPLEX=<duplex>],[SPEED=<speed>],[NAME=<name>],[CMDMDE=<cmdmde>],[MACADDR=<macaddr>],[FREQ=<freq>],[LOSSB=<lossb>],[SOAK=<soak>]:[<pst>[,<sst>]];
```

ED-GIGE:[<TID>]:<aid>:<CTAG>:::[ADMINSTATE=<adminstate>],[LINKSTATE=<linkstate>],[MTU=<mtu>],[FLOW=<flow>],[FLOWCTRL=<flowctrl>],[AUTONEG=<autoneg>],[HIWMRK=<hiwmrk>],[LOWMRK=<lowmrk>],[OPTICS=<optics>],[DUPLEX=<duplex>],[SPEED=<speed>],[NAME=<name>],[CMDMDE=<cmdmde>],[MACADDR=<macaddr>],[FREQ=<freq>],[LOSSB=<lossb>],[SUPPRESS=<suppress>],[SOAK=<soak>],[SQUELCH=<squelch>],[CIR=<cir>],[CBS=<cbs>],[EBS=<ebs>]:[<pst>[,<sst>]];

(ED-G1000 enum changes:

ENCAP)

(ED-L2-ETH enum changes:

ETH_BRIDGESTATE

ETH_NIMODE

ETH_QNQMODE)

(ED-LMP enum changes:

OPSTATE

WDM_ROLE)

ED-NE-GEN syntax changed:

ED-NE-GEN[:<TID>]::<CTAG>[:::NAME=<name>,][IPADDR=<ipaddr>,][IPMASK=<ipmask>,][DEFRTR=<defrtr>,][IIOPPORT=<iiopport>,][NTP=<ntp>,][PROXYSRV=<isProxyServer>,][FIREWALL=<isFireWall>,][SUPPRESSIP=<mode>,][MODE=<mode>];

ED-NE-GEN[:<TID>]::<CTAG>[:::NAME=<name>,][IPADDR=<ipaddr>,][IPMASK=<ipmask>,][DEFRTR=<defrtr>,][IIOPPORT=<iiopport>,][NTP=<ntp>,][SUPPRESSIP=<mode>,][MODE=<mode>,][SERIALPORTECHO=<serialportecho>];

ED-NE-PATH syntax changed:

ED-NE-PATH[:<TID>]::<CTAG>[:::PDIP=<pdip>];

ED-NE-PATH[:<TID>]::<CTAG>[:::PDIP=<pdip>,][XCMODE=<xcmode>];

ED-OMS syntax changed:

ED-OMS[:<TID>]:<aid>:<CTAG>[:::RDIRN=<rdirn>,][EXPBAND=<expband>,][VOAATTN=<voaattn>,][VOAPWR=<voapwr>,][CALOPWR=<calopwr>,][CHPOWER=<chpower>,][NAME=<name>,][SOAK=<soak>,][CMDMDE=<cmdmde>][:<pst>[,<sst>]];

ED-OMS[:<TID>]:<aid>:<CTAG>[:::EXPBAND=<expband>,][VOAATTN=<voaattn>,][VOAPWR=<voapwr>,][CALOPWR=<calopwr>,][CHPOWER=<chpower>,][NAME=<name>,][SOAK=<soak>,][CMDMDE=<cmdmde>][:<pst>[,<sst>]];

(ED-OMS enum changes:

RDIRN_MODE)

ED-OTS syntax changed: (MultiShelf 454, 54 SDH)

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

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

(ED-OTS enum changes:

RDIRN_MODE)

(ED-OTU2 enum changes:

PMMODE

REACH)

(ED-POS enum changes:

ENCAP)

(ED-QNQ-ETH enum changes:

ETH_RULE)

(ED-T1 enum changes:

SYNC_CLOCK_REF_QUALITY_LEVEL)

ED-WDMANS syntax changed:

ED-WDMANS[:<TID>]:<aid>:<CTAG>[:::POWERIN=<powerIn>,][POWEROUT=<powerOut>,][POWEREXP=<powerExp>,][NTWTYPE=<ringType>];

ED-WDMANS[:<TID>]:<aid>:<CTAG>[:::POWERIN=<powerIn>,][POWEROUT=<powerOut>,][POWEREXP=<powerExp>,][NTWTYPE=<ringType>,][PPMESH=<ppmesh>,][DITHER=<dither>];

(ED-WDMANS enum changes:

PPMESH)

(ENT-CKT-ORIG enum changes:

MOD_PATH)

(ENT-CKT-TERM enum changes:

MOD_PATH)

ENT-EQPT syntax changed:

ENT-EQPT[:<TID>]:<aid>:<CTAG>::<aidtype>[:PROTID=<protid>,][PRTYPE=<prtype>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][CARDMODE=<cardmode>,][PEERID=<protid>,][REGENNAME=<regename>,][CMDMDE=<cmdmde>,][TRANSMODE=<transmode>,][RETIME=<retime>,][SHELFROLE=<shelfrole>][:];

ENT-EQPT[:<TID>]:<aid>:<CTAG>::<aidtype>[:PROTID=<protid>,][PRTYPE=<prtype>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][CARDMODE=<cardmode>,][PEERID=<protid>,][REGENNAME=<regename>,][CMDMDE=<cmdmde>,][TRANSMODE=<transmode>,][RETIME=<retime>,][SHELFROLE=<shelfrole>,][FRPROLE=<frprole>,][FRPSTATE=<frpstate>][:];

(ENT-EQPT enum changes:

CARDMODE (454, 310MA, 310CL : Lotus20GCE2, Gt3CE2)

EQUIPMENT_TYPE (454, 454 SDH,310MA, 310CL : Lotus20GCE2, Gt3CE2)

FRPROLE

FRPSTATE)

(ENT-QNQ-ETH enum changes:

ETH_RULE)

(INH-SWTOPROTN-EQPT enum changes:

DIRECTION)

(INH-SWTOWKG-EQPT enum changes:

DIRECTION)

(LMP-CTRL enum changes:

OPSTATE)

(LMP-DLINK enum changes:

DATALINK

OPSTATE)

(LMP-TLINK enum changes:

MUXCAP

OPSTATE)

OPR-APC syntax changed:

OPR-APC[:<TID>]::<CTAG>;

OPR-APC[:<TID>]:<aid>:<CTAG>;

RTRV-ALM-ALL syntax changed: (All platforms)

RTRV-ALM-ALL[:<TID>][:<aid>]:<CTAG>[::<ntfcncde>,][<condtype>,][<srveff>][,,,];

RTRV-ALM-ALL[:<TID>][:<aid>]:<CTAG>[::<ntfcncde>,][<condtype>,][<srveff>,][<locn>,][<dirn>][,];

RTRV-ALM-ALL response changes:

[<aid>],[<aidtype>]:<ntfcncde>,<condtype>,<srveff>,<ocrdat>,<ocrtm>,,:[<desc>],[<aiddet>]

[<aid>],[<aidtype>]:<ntfcncde>,<condtype>,<srveff>,<ocrdat>,<ocrtm>,[<location>],[<direction>]:[<desc>],[<aiddet>]

(RTRV-ALM-ALL enum changes:

DIRECTION

MOD2B)

RTRV-ALM-BITS syntax changed: (All platforms)

RTRV-ALM-BITS[:<TID>]:<aid>:<CTAG>[::<ntfcncde>,][<condtype>,][<srveff>][,,,];

RTRV-ALM-BITS[:<TID>]:<aid>:<CTAG>[::<ntfcncde>,][<condtype>,][<srveff>,][<locn>,][<dirn>][,];

RTRV-ALM-BITS response changes:

<aid>,[<aidtype>]:<ntfcncde>,<condtype>,<srveff>,[<ocrdat>],[<ocrtm>],,:[<desc>],

<aid>,[<aidtype>]:<ntfcncde>,<condtype>,<srveff>,[<ocrdat>],[<ocrtm>],[<location>],[<direction>]:[<desc>],

(RTRV-ALM-BITS enum changes:

DIRECTION

MOD2B)

RTRV-ALM-EQPT syntax changed: (All platforms)

RTRV-ALM-EQPT[:<TID>]:<aid>:<CTAG>[::<ntfcncde>,][<condtype>,][<srveff>][,,,];

RTRV-ALM-EQPT[:<TID>]:<aid>:<CTAG>[::<ntfcncde>,][<condtype>,][<srveff>,][<locn>,][<dirn>][,];

RTRV-ALM-EQPT response changes:

[<aid>],[<aidtype>]:<ntfcncde>,<condtype>,<srveff>,[<ocrdat>],[<ocrtm>],[<stringValue>],:[<desc>],

[<aid>],[<aidtype>]:<ntfcncde>,<condtype>,<srveff>,[<ocrdat>],[<ocrtm>],[<location>],[<direction>]:[<desc>],

(RTRV-ALM-EQPT enum changes:

DIRECTION

MOD2B)

RTRV-ALM-SYNCN syntax changed: (All platforms)

RTRV-ALM-SYNCN[:<TID>]:<aid>:<CTAG>[::<ntfcncde>,][<condtype>,][<srveff>][,,,];

RTRV-ALM-SYNCN[:<TID>]:<aid>:<CTAG>[::<ntfcncde>,][<condtype>,][<srveff>,][<locn>,][<dirn>][,];

RTRV-ALM-SYNCN response changes:

<aid>,[<aidtype>]:<ntfcncde>,<condtype>,<srveff>,[<ocrdat>],[<ocrtm>],,:[<desc>],

<aid>,[<aidtype>]:<ntfcncde>,<condtype>,<srveff>,[<ocrdat>],[<ocrtm>],[<location>],[<direction>]:[<desc>],

(RTRV-ALM-SYNCN enum changes:

DIRECTION

MOD2B)

REPT^ALM^<MOD2ALM> response changes : (All platforms)

"<aid>:< ntfcncde>,<condtype>,<srveff>,[<ocrdat>],[<ocrtm>]>],,:[<desc>],[<aiddet>]";

"<aid>:< ntfcncde>,<condtype>,<srveff>,[<ocrdat>],[<ocrtm>]>],<locn>,<dirn>,,:[<desc>],[<aiddet>]";

REPT^ALM^BITS response changes: (All platforms)

```
   "<aid>:<ntfcncde>,<condtype>,<srveff>,[<ocrdat>],[<ocrtm>]:[<desc>]";
   "<aid>:<ntfcncde>,<condtype>,<srveff>,[<ocrdat>],[<ocrtm>],<locn>,<dirn>:[<desc>]";
```

REPT^ALM^COM response changes: (All platforms)

```
   "[<aid>]:<ntfcncde>,<condtype>,<srveff>,[<ocrdat>],[<ocrtm>]:[<desc>]";
   "[<aid>]:<ntfcncde>,<condtype>,<srveff>,[<ocrdat>],[<ocrtm>],[<locn>],[<dirn>]:[<desc>]";
```

REPT^ALM^EQPT response changes: (All platforms)

```
   "<aid>:<ntfcncde>,<condtype>,<srveff>,[<ocrdat>],[<ocrtm>]:[<desc>],[<aiddet>]";
   "<aid>:<ntfcncde>,<condtype>,<srveff>,[<ocrdat>],[<ocrtm>],<locn>,<dirn>:[<desc>],[<aiddet>]";
```

Same response change applies to REPT^ALM^SYNCN

REPT^EVT^<MOD2ALM> response changes : (All platforms)

```
   "<aid>:<condtype>,[<condeff>],,,[<monval>],[<thlev>],[<tmper>]:[<desc>],[<aiddet>]";

"<aid>:<condtype>,[<condeff>],,,[<locn>],[<dirn>],[<monval>],[<thlev>],[<tmper>]:[<desc>],[<aiddet>]";
```

REPT^EVT^BITS response changes: (All platforms)

```
   "<aid>:<condtype>,[<condeff>],,,,,:[<desc>]";
   "<aid>:<condtype>,[<condeff>],,,,,[<locn>],[<dirn>],:[<desc>]";
```

REPT^EVT^COM response changes: (All platforms)

```
   "[<aid>]:<condtype>,[<condeff>],,,,,:[<desc>]";
   "[<aid>]:<condtype>,[<condeff>],,,[<locn>],[<dirn>],,,:[<desc>]";
```

REPT^EVT^SECU response changes: (All platforms)

```
   "<aid>:<condtype>,<condeff>,,,,,:<security>:<msg>";
   "<aid>:<condtype>,<condeff>,,,<locn>,<dirn>,,,:<security>:<msg>";
```

REPT^EVT^EQPT response changes: (All platforms)

```
   "<aid>:<condtype>,[<condeff>],,,,,,:[<desc>],[<aiddet>]";
   "<aid>:<condtype>,[<condeff>],,,,,,[<locn>],[<dirn>]:[<desc>],[<aiddet>]";
```

Same response change applies to REPT^EVT^SYNCN

RTRV-APC syntax changed:

```
  RTRV-APC[:<TID>]::<CTAG>[::::];
  RTRV-APC[:<TID>]:<aid>:<CTAG>[::::];
```

RTRV-APC response changes:

::[<apcenable>],[<apcstate>]:

[<aid>]::[<apcenable>],[<apcstate>]:

RTRV-BITS response changes:

<aid>::[<linecde>],[<fmt>],[<lbo>],[<syncmsg>],[<aisthrshld>],<saBit>,[<bitsfac>],[<admssm>]:[<pst>]

<aid>::[<linecde>],[<fmt>],[<lbo>],[<syncmsg>],[<aisthrshld>] [<saBit>],[<impedance>],[<bitsfac>],[<admssm>] [<pst>]

(RTRV-BITS enum changes:

SYNC_CLOCK_REF_QUALITY_LEVEL)

(RTRV-CKT-ORIG enum changes:

MOD_PATH)

(RTRV-CKT-TERM enum changes:

MOD_PATH)

RTRV-COND-ALL syntax changed:

RTRV-COND-ALL[:<TID>][:<aid>]:<CTAG>[::<typereq>][,,,];

RTRV-COND-ALL[:<TID>][:<aid>]:<CTAG>[::<typereq>,][<locn>,][<dirn>][,];

RTRV-COND-ALL response changes:

<aid>,[<aidtype>]:[<ntfcncde>],<typerep>,[<srveff>],[<ocrdat>],[<ocrtm>],,,[<desc>]

<aid>,[<aidtype>]:[<ntfcncde>],<typerep>,[<srveff>],[<ocrdat>],[<ocrtm>],[<location>],[<direction>],[<desc>]

(RTRV-COND-ALL enum changes:

DIRECTION

MOD2B)

RTRV-COND-BITS syntax changed:

RTRV-COND-BITS[:<TID>]:<aid>:<CTAG>[::<typereq>][,,,];

RTRV-COND-BITS[:<TID>]:<aid>:<CTAG>[::<typereq>,][<locn>,][<dirn>][,];

RTRV-COND-BITS response changes:

<aid>,[<aidtype>]:[<ntfcncde>],<typerep>,[<srveff>],[<ocrdat>],[<ocrtm>],,,[<desc>]

<aid>,[<aidtype>]:[<ntfcncde>],<typerep>,[<srveff>],[<ocrdat>],[<ocrtm>],[<location>],[<direction>],[<desc>]

(RTRV-COND-BITS enum changes:

DIRECTION

MOD2B)

RTRV-COND-EQPT syntax changed:

RTRV-COND-EQPT[:<TID>]:<aid>:<CTAG>[::<typereq>][,,,];

RTRV-COND-EQPT[:<TID>]:<aid>:<CTAG>[::<typereq>,][<locn>,][<dirn>][,];

RTRV-COND-EQPT response changes:

<aid>,[<aidtype>]:[<ntfcncde>],<typerep>,[<srveff>],[<ocrdat>],[<ocrtm>],,,[<desc>]

<aid>,[<aidtype>]:[<ntfcncde>],<typerep>,[<srveff>],[<ocrdat>],[<ocrtm>],[<location>],[<direction>],[<desc>]

(RTRV-COND-EQPT enum changes:

DIRECTION

MOD2B)

RTRV-COND-SYNCN syntax changed:

RTRV-COND-SYNCN[:<TID>]:<aid>:<CTAG>[::<typereq>][,,,];

RTRV-COND-SYNCN[:<TID>]:<aid>:<CTAG>[::<typereq>,][<locn>,][<dirn>][,];

RTRV-COND-SYNCN response changes:

<aid>,[<aidtype>]:[<ntfcncde>],<typerep>,[<srveff>],[<ocrdat>],[<ocrtm>],,,[<desc>]

<aid>,[<aidtype>]:[<ntfcncde>],<typerep>,[<srveff>],[<ocrdat>],[<ocrtm>],[<location>],[<direction>],[<desc>]

(RTRV-COND-SYNCN enum changes:

DIRECTION

MOD2B)

(RTRV-CRS enum changes:

CRS_TYPE (454, 454 SDH : Lotus20gML2Lite)

MOD_PATH)

RTRV-DGN-EQPT response changes:

<aid>:

<slot>:

(RTRV-E1 enum changes:

DIRECTION

SYNC_CLOCK_REF_QUALITY_LEVEL)

(RTRV-E4 enum changes:

PAYLOAD)

RTRV-EQPT response changes:

<aid>:<aidtype>,<equip>,[<role>],[<status>]:[<protid>],[<prtype>],[<rvrtv>],[<rvtm>],[<cardname>],[<ioscfg>],[<cardmode>],[<peerid>],[<regenname>],[<transmode>],[<retime>],[<shelfrole>]:<pst>,[<sst>]

<aid>:<aidtype>,<equip>,[<role>],[<status>]:[<protid>],[<prtype>],[<rvrtv>],[<rvtm>],[<cardname>],[<ioscfg>],[<cardmode>],[<peerid>],[<regenname>],[<peername>],[<transmode>],[<retime>],[<shelfrole>],[<frprole>],[<frpstate>]:<pst>,[<sst>]

RTRV-FSTE response changes:

<aid>::[<adminstate>],[<linkstate>],[<mtu>],[<flowctrl>],[<optics>],[<duplex>],[<speed>],[<flow>],[<expduplex>],[<expspeed>],[<vlancosthreshold>],[<iptosthreshold>],[<name>],[<soak>],[<soakleft>]:<pst>,[<sst>]

<aid>::[<adminstate>],[<linkstate>],[<mtu>],[<flowctrl>],[<optics>],[<duplex>],[<speed>],[<flow>],[<expduplex>],[<expspeed>],[<vlancosthreshold>],[<iptosthreshold>],[<name>],[<suppress>],[<soak>],[<soakleft>]:<pst>,[<sst>]

RTRV-GIGE response changes:

<aid>:,,<role>,<status>:[adminstate>],[linkstate>],[mtu>],[encap>],[flowctrl>],[<autoneg>],[hiwmrk>],[<lowmrk>],[<optics>],[<duplex>],[<speed>], [<name>],[<freq>],[<lossb>],[<soak>],[<soakleft>],[<squelch>]:<pst>,<sst>;

<aid>:,,<role>,<status>:[adminstate>],[linkstate>],[mtu>],[encap>],[<flow>],[flowctrl>],[<autoneg>],[hiwmrk>],[<lowmrk>],[<optics>],[<duplex>],[<speed>],[<name>],[<freq>],[<lossb>],[<suppress>],[<soak>],[<soakleft>],[<squelch>], [<cir>],[<cbs>],[<ebs>]:<pst>,<sst>;

(RTRV-G1000 enum changes:

ENCAP)

RTRV-INV response changes:

<aid>,<aidtype>::[<pn>],[<hwrev>],[<fwrev>],[<sn>],[<clei>],[<twl1=nwl in code>],[<pluginvendorid>],[<pluginpn>],[<pluginhwrev>],[<pluginfwrev>],[<pluginsn>],[<ilossref>],[<productId>],[<versionId>],[<fpgaVersion>],[<vendorId>]

<aid>,<aidtype>::[<pn>],[<hwrev>],[<fwrev>],[<sn>],[<clei>],[<twl>],[<pluginvendorid>],[<pluginpn>],[<pluginhwrev>],[<pluginfwrev>],[<pluginsn>],[<ilossref>],[<productId>],[<versionId>],[<fpgaVersion>],[<vendorId>],[<moduletype>]

(RTRV-L2-ETH enum changes:

ETH_BRIDGESTATE

ETH_NIMODE

ETH_QNQMODE)

(RTRV-NE-APC enum changes:

MOD2)

RTRV-NE-GEN response changes :

[IPADDR=<ipaddr>],[IPMASK=<ipmask>],[DEFRTR=<defrtr>],[IIOPPORT=<iiopport>],[NTP=<ntp>],[ETHIPADDR=<ethipaddr>],[ETHIPMASK=<ethipmask>],[NAME=<name>],[SWVER=<swver>],[LOAD=<load>],[PROTSWVER=<protswver>],[PROTLOAD=<protload>],[DEFDESC=<defdesc>],[PLATFORM=<platform>],[SECUMODE=<secumode>],[SUPPRESSIP=<suppressip>],[MODE=<mode>]

[IPADDR=<IPADDR>],[IPMASK=<IPMASK>],[DEFRTR=<DEFRTR>],

[IIOPPORT=<IIOPPORT>],[NTP=<NTP>],[ETHIPADDR=<ETHIPADDR>],

[ETHIPMASK=<ETHIPMASK>],[NAME=<NAME>],[SWVER=<SWVER>],[LOAD=<LOAD>],

[PROTSWVER=<PROTSWVER>],[PROTLOAD=<PROTLOAD>],[DEFDESC=<DEFDESC>],

[PLATFORM=<PLATFORM>],[SECUMODE=<SECUMODE>],[SUPPRESSIP=<SUPPRESSIP>],

[PROXYSRV=<PROXYSRV>],[FIREWALL=<FIREWALL>],[AUTOPM=<AUTOPM>], [SERIALPORTECHO=<SERIALPORTECHO>

RTRV-NE-PATH response changes:

<rvtm>

<pdip>,<loxcmode>

RTRV-NE-SYNCN response changes:

[<aid>]::[<tmmd>],[<ssmgen>],[<qres>],[<rvrtv>],[<rvtm>]

[<aid>]::[<tmmd>],[<ssmgen>],[<qres>],[<rvrtv>],[<rvtm>],[<systmn>]

(RTRV-NE-SYNCN enum changes:

SYSTEM_TIMING)

<aid>:,,[<role>],[<status>]:[<opticalPortType>],[<power>],[<expWlen>],[<actWlen>],[<iloss>],[<voamode>],[<voaattn>],[<voapwr>],[<voarefattn>],[<voarefpwr>],[<refopwr>],[<calopwr>],[<chpower>],[<chpowerFlg>],[<portname>],[<gcc>],[<gccrate>],[<dwrap>],[<fec>],[<payloadmap>],[<lbclcurr>],[<optcurr>],[<oprcurr>],[<osfber>],[<osdber>],[<soak>],[<soakleft>],[<lossb>]:<pst>,[<sst>]

RTRV-OMS response changes:

<aid>::<rdirn>,<opticalPortType>,[<power>],<expBand>,[<actBand>],[<iloss>],[<voamode>],[<voaattn>],[<voapwr>],[<voarefattn>],[<voarefpwr>],[<refopwr>],[<calopwr>],[<chpower>],[<name>],[<soak>],[<soakleft>]:<pst>,[<sst>]

<aid>::<opticalPortType>,[<power>],<expBand>,[<actBand>],[<iloss>],[<voamode>],[<voaattn>],[<voapwr>],[<voarefattn>],[<voarefpwr>],[<refopwr>],[<calopwr>],[<chpower>],[<chpowerFlg>],[<name>],[<soak>],[<soakleft>]:<pst>,[<sst>]

(RTRV-OMS enum changes:

RDIRN_MODE

WDMANS_FLAG)

RTRV-OPM response changes:

<aid>::[<powerout>],[<poweradd>],[<powerpt>]:

RTRV-OTS response changes:

<aid>::<rdirn>,<opticalPortType>,[<power>],[<iloss>],[<voamode>],[<voaattn>],[<voapwr>],[<voarefattn>],[<voarefpwr>],[<osri>],[<amplmode>],[<chpower>],[<gain>],[<expgain>],[<refopwr>],[<offset>],[<reftilt>],[<caltilt>],[<aseopwr>],[<dculoss>],[<awgst>],[<heatst>],[<name>],[<soak>],[<soakleft>]:<pst>,[<sst>]

<aid>::<opticalPortType>,[<power>],[<iloss>],[<voamode>],[<voaattn>],[<voapwr>],[<voarefattn>],[<voarefpwr>],[<osri>],[<amplmode>],[<amplmodeFlg>],[<chpower>],[<chpowerFlg>],[<gain>],[<expgain>],[<expgainFlg>],[<refopwr>],[<offset>],[<reftilt>],[<reftiltFlg>],[<caltilt>],[<aseopwr>],[<dculoss>],[<awgst>],[<heatst>],[<name>],[<soak>],[<soakleft>]:<pst>,[<sst>]

(RTRV-OTS enum changes:

RDIRN_MODE

WDMANS_FLAG)

(RTRV-PM-ALL enum changes:

DIRECTION)

(RTRV-QNQ-ETH enum changes:

ETH_RULE)

(RTRV-STM1E enum changes:

PAYLOAD)

(RTRV-TH-ALL enum changes:

MOD2B)

(RTRV-TRC-OC48 enum changes:

MOD_PATH)

(RTRV-TRC-OCH enum changes:

MOD2)

RTRV-VC syntax changed:

RTRV-VC[:<TID>]:<aid>:<CTAG>[:::BLSRPTHTYPE=<blsrpthtype>][:];

RTRV-VC[:<TID>]::<CTAG>;

(RTRV-VC enum changes:

PRODUCT_TYPE)

(RTRV-WLEN enum changes:

WCT)

(SW-TOPROTN-EQPT enum changes:

DIRECTION)

(SW-TOWKG-EQPT enum changes:
DIRECTION)

TL1 ENUM Changes

TL1 ENUM Items Added or Removed

The following section highlights ENUM items changed (added or removed) for Release 8.0, by ENUM type.

AUTOPM_TMPER

AUTOPM_TMPER enum added with the following items in it (all platforms):

AUTOPM_TMPER_NONE
AUTOPM_TMPER_15MIN
AUTOPM_TMPER_1DAY
AUTOPM_TMPER_BOTH

DIRECTION

DIRECTION enum items added (454, 454 SDH, 310 MA, 310 CL, 600, 600 SDH):

DIRECTION_TD_NA => "NA"

DIRECTION is used in the following commands:

ALW-SWTOPROTN-EQPT
ALW-SWTOWKG-EQPT
EX-SW-OCN-BLSR
INH-SWTOPROTN-EQPT
INH-SWTOWKG-EQPT
INIT-REG-MOD2
OPR-PROTNSW-OCN-TYPE
RLS-PROTNSW-OCN-TYPE
RTRV-ALM-ALL
RTRV-ALM-BITS
RTRV-ALM-EQPT
RTRV-ALM-MOD2ALM
RTRV-ALM-SYNCN
RTRV-COND-ALL
RTRV-COND-BITS

RTRV-COND-EQPT

RTRV-COND-MOD2ALM

RTRV-COND-SYNCN

RTRV-E1

RTRV-PM-ALL

RTRV-PM-MOD2

SW-TOPROTN-EQPT

SW-TOWKG-EQPT

ENCAP

ENCAP enum items added to (454, 454 SDH, 310 MA, 310 CL, 600 SDH):

ENCAP_RPR_GFP_F => "RPR-GFP-F"

ENCAP is used in the following commands:

ED-G1000

ED-POS

RTRV-FC

RTRV-G1000

RTRV-POS

EQPT_TYPE

EQPT_TYPE enum items dropped:

EQPT_TYPE_EQPT_ID_ML2_EXIGE_MAPPER_CARD => "CE-100T-8"

EQPT_TYPE enum items added:

EQPT_TYPE_EQPT_ID_OC192_4_DWDM => "OC192-4-DWDM" (600, 600 SDH)

EQPT_TYPE_EQPT_ID_PIM_1_PPM => "PIM-1" (600 SDH)

EQUIPMENT_TYPE

EQUIPMENT_TYPE enum items dropped:

EQUIPMENT_TYPE_ET_ML2_EXIGE_MAPPER_CARD => "CE-100T-8"

EQUIPMENT_TYPE enum items added:

EQUIPMENT_TYPE_ET_OC192_4_DWDM => "OC192-4-DWDM" (600,600 SDH)

EQUIPMENT_TYPE_ET_PIM_1 => "PIM-1" (600 SDH)

EQUIPMENT_TYPE_ET_STM16_16 => "STM16_16" (600 SDH)

EQUIPMENT_TYPE_ET_STM64_4 => "STM64_4" (600 SDH)

EQUIPMENT_TYPE_ET_STM64_4_DWDM => "STM64-4-DWDM" (600, 600 SDH)

EQUIPMENT_TYPE

EQUIPMENT_TYPE is used in the following commands:

CHG-EQPT
ENT-EQPT

MOD2B

MOD2B enum items added:

MOD2O

MOD2O enum items added:

MOD2O_M2_ILK => "ILK" (454)
MOD2O_M2_OTU2 => "OTU2" (454, 454 SDH)

MOD2O is used in the following commands:

RTRV-ALMTH-MOD2O

OPTICAL_NODE_TYPE

OPTICAL_NODE_TYPE enum items added:

OPTICAL_NODE_TERMINAL => "TERMINAL"

OPTICAL_NODE_TYPE is used in the following commands:

RTRV-WDMANS

PMMODE

PMMODE enum items added:

PMMODE_PROPRIETARY => "PROPRIETARY"
PMMODE_STD => "STD"

PMMODE is used in the following commands:

ED/RTRV-OTU2

PRODUCT_TYPE

PRODUCT_TYPE enum items added: (600 SDH):

PRODUCT_TYPE_NE_15600SDH => "ONS15600SDH"

PRODUCT_TYPE is used in the following commands:

RTRV-MAP-NETWORK
RTRV-VC

REACH

REACH enum items added:

REACH_CWDM => "CWDM"
REACH_DWDM => "DWDM"
REACH_ZR => "ZR"

REACH is used in the following commands:

ED-DWDM-CLNT
ED-FC
ED-GIGE
ED-OCH
ED-OCN-TYPE
ED-OTU2
RTRV-DWDM-CLNT
RTRV-FC
RTRV-GIGE
RTRV-OCH
RTRV-OCN-TYPE
RTRV-OTU2

REGULATED_PORT_TYPE

REGULATED_PORT_TYPE enum items added:

REGULATED_PORT_MISSING_PARAM => "MISSING-PARAM"

REGULATED_PORT_TYPE is used in the following commands:

RTRV-NE-WDMANS

REPTPM_TYPE

REPTPM_TYPE enum added with the following items in it (all platforms)

REPTPM_TYPE_NONE
REPTPM_TYPE_AUTO
REPTPM_TYPE_SCHED
REPTPM_TYPE_BOTH

REPTPM_TYPE

REPTPM_TYPE is used in the following commands:

SCHED-PMREPT-<MOD2>

RFILE

RFILE enum items added (454, 454 SDH, 310 MA, complete Db backup):

  RFILE_COMPDB => "RFILE-COMPDB"

RFILE is used in the following commands:

    COPY-IOSCFG
    COPY-RFILE

SYNC_CLOCK_REF_QUALITY_LEVEL

SYNC_CLOCK_REF_QUALITY_LEVEL enum items added:

  SYNC_CLOCK_REF_QUALITY_LEVEL_QREF_SSM_FAILED => "SSM-FAILED"

SYNC_CLOCK_REF_QUALITY_LEVEL is used in the following commands:

    ED-BITS
    ED-E1
    ED-OCN-TYPE
    ED-T1
    RTRV-BITS
    RTRV-E1
    RTRV-OCN-TYPE
    RTRV-SYNCN
    RTRV-T1

SYSTEM_TIMING

SYSTEM_TIMING enum items added:

  SYSTEM_TIMING_SDH => "SDH"
  SYSTEM_TIMING_SONET => "SONET"

SYSTEM_TIMING is used in the following commands:

    ED-NE-SYNCN
    RTRV-NE-SYNCN

VALIDITY

VALIDITY enum items dropped:

  VALIDITY_CV_OFF => "OFF"

VALIDITY enum items added:

  VALIDITY_CV_OFF => "NA"

VALIDITY is used in the following commands:

RTRV-PM-MOD2

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15600 SDH, Release 1.4*
- *Release Notes for the Cisco ONS 15454 SDH, Release 8.0*
- *Release Notes for the Cisco ONS 15600, Release 8.0*
- *Release Notes for the Cisco ONS 15454, Release 8.0*
- *Release Notes for the Cisco ONS 15310-CL, Release 8.0*
- *Release Notes for the Cisco ONS 15310-MA, Release 8.0*
- *Cisco ONS 15600 SDH Software Upgrade Guide, Release 8.0*

Platform-Specific Documents

- *Cisco ONS 15600 SDH Procedure Guide*
  Provides installation, turn up, test, and maintenance procedures
- *Cisco ONS 15600 SDH Reference Manual*
  Provides technical reference information for SONET/SDH cards, nodes, and networks
- *Cisco ONS 15600 SDH Troubleshooting Guide*
  Provides a list of SONET alarms and troubleshooting procedures, general troubleshooting information, and hardware replacement procedures
- *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 Command Guide*
  Provides a comprehensive list of TL1 commands

Note From Release 8.0 onwards, the platform-specific documents listed above are not available through the CTC Help menu. You can access PDF and HTML versions of these documents on Cisco.com.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation,* which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.