Release Notes for Cisco ONS 15327 Release 6.0.3

August 2007

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15327 SONET. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to Release 6.0 of the *Cisco ONS 15327 Procedure Guide, Cisco ONS 15327 Reference Manual, Cisco ONS SONET TL1 Command Guide, and Cisco ONS 15327 Troubleshooting Guide.* For the most current version of the Release Notes for Cisco ONS 15327 Release 6.0.3, visit the following URL:

http://www.cisco.com/en/US/products/hw/optical/ps2006/prod_release_notes_list.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

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.

Contents

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

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15327 Release 6.0.3* since the production of the Cisco ONS 15327 System Software CD for Release 6.0.3.

No changes have been added to the release notes for Release 6.0.3.

Caveats

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

Maintenance and Administration

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

Note In releases prior to 4.6 you could independently set proxy server gateway settings; however, with Release 4.6.x and forward, this is no longer the case. To retain the integrity of existing network configurations, settings made in a pre-4.6 release are not changed on an upgrade to Release 6.0.x. Current settings are displayed in CTC (whether they were inherited from an upgrade, or they were set using the current GUI).

CSCeh84908

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

CSCed24448

After a static route is provisioned to 0.0.0.0 and then deleted, the default route disappears. If this occurs, reprovision the default gateway. This issue will not be resolved.

CSCee65731

An ONS 15327 that does not have an SNTP server reference resets the time to Jan. 1, 1970 during a software activation. A routine common control switchover does not cause the node to lose the time setting. To avoid this issue provision a SNTP server reference. This issue cannot be resolved.

CSCdy10030

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

CSCdy49608

A node connection might fail during bulk circuit creation, causing the circuit creation to also fail. For example, this has been seen while creating 224 VT 1.5 protected circuits, on a path protection consisting of eight ONS 15327 nodes. If you experience a bulk circuit creation failure of this type, cancel the circuit creation batch, then delete any incomplete circuits. Restart the batch from the last successful circuit. This issue will not be resolved.

CSCdx35561

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

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

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

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

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

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

This issue will not be resolved.

CSCdy11012

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

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

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

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

CSCdy37198

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

CSCds23552

You cannot delete the standby XTC once it is removed. If you have two XTC cards and then decide to operate with only one, you will get a standing minor alarm. The alarm cannot be removed by CTC. The XTC is a combo card, combining the functionality of the ONS 15454 TCC2, cross connect, DS1 and DS3 cards, with a protection group automatically provisioned. On the ONS 15454, similar behavior occurs for the TCC2 card. The cross connect card for the ONS 15454 can only be deleted if there are no circuits provisioned. DS1 and DS3 cards can only be deleted if they are not in a protection group. User-defined alarm profiles from Release 5.0.x allow you to mask the improper removal alarm from the standby XTC slot without masking any other items if desired, thus avoiding this issue. This issue will not be resolved.

Data IO Cards

CSCdy41135

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

CSCdy13035

Excessive Ethernet traffic loss (greater than 60 ms) might occur when the active XTC is removed from the chassis while using the G1000-2 card. On rare occasions, permanent loss of traffic can occur. Do not remove the active XTC from the chassis to force a protection switch. Instead, perform a soft reset of the active XTC through the network management interface. Once the XTC is in standby mode, it can be removed from the chassis without inducing excessive traffic loss.

This issue impacts only cards with Version number 800-18490-01 and is resolved by a newer version of the G1000-2 cards. Cards with Version number 800-18490-02, rev A0 or later incorporate improved hardware PLL circuitry on the G1000-2 line card to allow an active XTC removal without causing excessive traffic loss. The caveat herein is for the previous hardware version.

Path Protection Functionality

CSCee53579

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

CSCeb37707

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

Performance Monitoring

CSCdt10886

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

Bridge and Roll

CSCei37364

When a rollTo leg is not receiving a good signal, and because of this the rollPending alarm is not cleared, there is no alarm indicating the reason that the RollPending alarm fails to clear. This issue is resolved in Release 7.0.

TL1

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

Resolved Caveats for Release 6.0.x

The following items are resolved in Release 6.0.x

Path Protection Functionality

CSCsh77496

If Path Protection/SNCP circuits are created while path defects are present on Path Protection/SNCP trunks, then sometimes Path Protection/SNCP circuits may not switch and traffic outage is observed

Workaround: Avoid creating path protection circuits while faults are present on either of the path protection trunks ports. This issue is resolved in 6.03, 7.05 and 7.2.3

CSCec15064

A Path Protection/SNCP circuit with a defect signal present (for example, AIS-P or AIS-V) on the protect path will produce RDI-P or RDI-V upstream of the detection point, but these signals will not be detected or indicated. This issue will be resolved in a future release.

New Features and Functionality

This section highlights new features and functionality for Release 6.0.x. For detailed documentation of each of these features, consult the user documentation.

New Software Features

Bridge and Roll

Release 6.0.x introduces bridge and roll for the ONS 15327. You can use the bridge and roll feature for maintenance functions such as card or facility replacement, or for load balancing. As of Release 6.0 you can perform bridge and roll operations using CTC or TL1 on all of the following ONS platforms: ONS 15454, ONS 15454 SDH, ONS 15600, ONS 15327, and ONS 15310-CL.

The CTC Bridge and Roll wizard reroutes live traffic without interrupting service. The bridge process takes traffic from a designated “roll from” facility and establishes a cross-connect to the designated “roll to” facility. When the bridged signal at the receiving end point is verified, the roll process creates a new cross-connect to receive the new signal. When the roll completes, the original cross-connects are released.

CTC Rolls Window

The CTC Rolls window provides access to information about a rolled circuit before the roll process is complete. To view the Rolls window, click the Circuits > Rolls tabs in either network or node view.

The Rolls window provides information on the following roll states and options. For descriptions of each state or option, consult the user documentation.

- Roll From Circuit
- Roll To Circuit
- Roll State
- Roll Valid Signal
- Roll Mode (automatic or manual)
- Roll Path
- Roll From Circuit
- Roll From Path
- Roll To Path
- Complete
- Force Valid Signal
- Finish
- Cancel
- Types of Rolls

TL1 Bulk Roll

Release 6.0.x TL1 bridge and roll features support for bulk rolling. Bulk rolling enables you to roll a subset of cross-connections from one port/facility to another port/facility.

The following TL1 commands specifically support bulk rolls. These commands support line-level rolling/bulk rolling and cannot be used for path-level rolling. For a complete list of TL1 commands supporting bridge and roll, as well as examples for each of the supported features, including bulk roll, consult the user documentation.

DLT-BULKROLL-<OCN_TYPE>

This command deletes an attempted rolling operation or completes an attempted rolling operation. The rolls that are created using the ENT-BULKROLL-<OCN_TYPE> command can be deleted using the DLT-BULKROLL-<OCN_TYPE> command.

ED-BULKROLL-<OCN_TYPE>

This command edits information about rolling traffic from one end point to another without interrupting service. This command can use the CMDMDE option to force a valid signal. The only parameter that can be edited is CMDMDE. The time slots cannot be edited.

ENT-BULKROLL-<OCN_TYPE>

This command enters information about rolling traffic from one end-point to another without interrupting service.

RTRV-BULKROLL-<OCN_TYPE>

This command retrieves roll data parameters.

Single and Dual Rolls

CTC supports two roll types. In a single roll operation you select only one roll point. This allows you to move either the source or destination of a circuit to a new end-point on the same node (similar to a TL1 single roll), or on a different node (rolling the original circuit onto another circuit).

In a dual roll, you select two roll points. This allows you to reroute a segment between the two roll points of a circuit. The new route for a dual roll can be a new link (no circuit is required), or it can be another circuit (created before or during the bridge and roll process).

For dual roll constraints, consult the user documentation.

Enhanced Security Features

Security Policy Enhancements

With Release 6.0.x 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 6.0.x 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 6.0.x 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.

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 6.0.x 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 6.0.x 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 6.0.x node access can be controlled by service type. Each service type from which you can access a node in Release 6.0.x 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 6.0 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 6.0.x 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 6.0.x 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 6.0.x.

- Archival of the audit trail in TL1, with a supporting archival failure transient alarm, AUD-ARCHIVE-FAIL
- Tracking of all Release 6.0.x 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 6.0.x, as described below.

Active Logins

The Active logins tab supports session management for Release 6.0.x. 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 6.0.x, 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 6.0.x 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 6.0.x, 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 6.0.x 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 6.0.x. 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. 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 6.0.x 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. 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 6.0.x, 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 6.0.x consult the user documentation.

IP and OSI on DCC

As of Release 6.0, 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 6.0.x 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 SDCC or LDCC. The SDCC or LDCC 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 SDCC as OSI only.

Release 6.0.x 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 6.0.x 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 6.0.x 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

FLT Secondary State

Release 6.0.x introduces a new secondary service state (SST), Fault (FLT). The FLT secondary state is defined as follows:

- FLT (Fault) The entity has a raised alarm or condition.

The FLT SST is an extension to the existing ONS state model. As such, the FLT state is a Telcordia GR-1093 secondary state. It identifies that the affected entity is OOS because it is faulty. The FLT secondary state affects the service state only. The AdminState (the state you manage the entity into) is not affected. The FLT SST is the result of autonomous action; you cannot manage an entity into the FLT SST. The FLT SST is for retrieval purposes only. An entity's service state will transition into the OOS-AU or OOS-AUMA (AU for autonomous) service state if alarms or conditions are present. The FLT SST is appended to the existing secondary state for the entity when an alarm or condition exists.

Equipment FLT Service State

Some Equipment alarms will not generate an FLT SST transition. If a state already exists to represent the equipment condition, FLT will not be added to the secondary state list:

- MEA–Mismatch of equipment is represented as MEA SST
- IMPROPRMVL–Improper Removal is represented as UEQ SST
- No FLT will be added, and there will be no alarms, when equipment is in AINS

FLT SST with Ports

In pre-6.0 releases, an IS-NR port with an LOS alarm remains as IS-NR service state. There is no service state change to reflect the port is down. A new PST-PSTQ service state is introduced in Release 6.0.x to reflect a port in MT state that is alarmed, OOS-AUMA (Autonomous, Management).

Any port alarm that results in the AINS countdown being inhibited will result in an FLT SST transition for the port. Loopback alarms will not result in an FLT SST transition, as there is a LPBK state to represent this information. There is NO FLT SST in the DSBLD state, as all alarms are cleared in the DSBLD state.

Connection FLT Service State

FLT SST connection changes are the same as for port changes. As with the port, the connection with an alarm in pre-6.0 releases has a service state of IS-NR. A new PST-PSTQ pair is introduced in Release 6.0.x to reflect a cross connect in maintenance with an alarm, OOS-AUMA (Autonomous, Management). Any connection alarm that results in the AINS countdown being inhibited will result in the FLT SST transition for the connection. There is no FLT SST in the DSBLD state, as all alarms are cleared in the DSBLD state.

CTC Launcher

Release 6.0.x introduces the CTC Launcher utility, CtcLauncher.jar. The CTC Launcher utility can be used to launch CTC and manage an ONS node running Release 6.0.x 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. Second, CTC Launcher can establish connectivity to ONS NEs that reside behind a third party, OSI-based GNE. 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 6.0 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 R6.0.x 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.

TL1

TL1 Open GNE

TL1 supports the ability to act as a GNE or ENE to an OEM IP DCN (foreign) connected node that also uses TL1. To accomplish TL1 GNE-ENE interoperability, the DCN communication path between the GNE and ENE employs PPP and OSPF in a non-proprietary manner, while ensuring that these connections remain secure. Open GNE TL1 functionality enables you to configure DCC terminations to interoperate with a system on the far end that does not support proprietary PPP vendor extensions or OSPF types.

Open GNE Commands

The following commands support TL1 open GNE. For input and output formats and parameters, plus examples of how to use each command, consult the user documentation.

RTRV-TADRMAP

- RETRIEVE-TID_ADDRESS_MAP

  This command is used to instruct a Gateway NE to return the entries of the TADRMAP. One row is used for each displayed TID name.

DLT-TADRMAP

- DELETE-TID_ADDRESS_MAP

  This command is used to instruct a Gateway NE to delete an entry in the table which maps the TIDs of the subtending NEs to their addresses. The OSs will address the subtending NEs using the TID in TL1 messages and a Gateway NE will address these NEs using IP Addresses or NSAPs. This table, which resides in a Gateway NE, correlates a TID and an address.

ENT-TADRMAP

- ENTER-TID_ADDRESS_MAP

  This command is used to instruct a Gateway NE to create an entry in the table which maps the TIDs of the subtending NEs to their addresses. The OSs will address the subtending NEs using the TID in TL1 messages and a Gateway NE will address these NEs using IP Addresses or NSAPs. This table, which resides in a Gateway NE, correlates a TID and an address. This command requires that at least one of (IPADDR or NSAP) be specified.

ENT-TUNNEL-PROXY

- ENTER-TUNNEL_PROXY

  This command is used to create a proxy tunnel.

DLT-TUNNEL-PROXY

- DELETE-TUNNEL_PROXY

  This command is used to delete a proxy tunnel.

RTRV-TUNNEL-PROXY

- RETRIEVE-TUNNEL_PROXY

  This command is used to a view the proxy tunnels contained in the NE proxy table.

ENT-TUNNEL-FIREWALL

- ENTER-TUNNEL_FIREWALL

  This command is used to create a firewall tunnel.

DLT-TUNNEL-FIREWALL

- DELETE-TUNNEL_FIREWALL

  This command is used to a delete a firewall tunnel.

RTRV-TUNNEL-FIREWALL

- RETRIEVE-TUNNEL_FIREWALL

  This command is used to a view the firewall tunnels contained in the NE proxy table.

Changed Commands for Open GNE

The following previously-existing TL1 commands support new parameters for open GNE.

ED-<OCN_TYPE>

- foreignFarEnd—Input parameter used to indicate that the far end NE on the DCC is a foreign NE.
- foreignIPAddress—Input parameter specifying the IP Address of the far end Node on the DCC. Used only if foreignFarEnd is ‘Y’.

RTRV-<OCN_TYPE>

- foreignFarEnd—Output parameter used to indicate that the far end NE on the DCC is a foreign NE.
- foreignIPAddress—Output parameter specifying the IP Address of the far end Node on the DCC. Used only if foreignFarEnd is ‘Y’.

The following command has been modified to support open GNE as described.

REPT^DBCHG

Generate an update after an addition to or deletion from the TADRMAP or an addition or deletion of a firewall or proxy tunnel. The ENT-TADRMAP, DLT-TADRMAP, ENT-TUNNEL-PROXY, DLT-TUNNEL-PROXY, ENT-TUNNEL-FIREWALL, and DLT-TUNNEL-FIREWALL commands each generate an appropriate REPT^DBCHG message.

TL1 Command Changes

New Commands

The following new TL1 commands are added for Release 6.0.x.

- ALW-CONSOLE-PORT
- DLT-BULKROLL
- DLT-ROLL
- DLT-ROUTE-GRE
- DLT-TADRMAP
- DLT-TUNNEL-FIREWALL
- DLT-TUNNEL-PROXY
- ED-BULKROLL
- ED-PROTOCOL
- ED-ROLL
- ENT-BULKROLL
- ENT-ROUTE-GRE
- ENT-TADRMAP
- ENT-TUNNEL-FIREWALL
- ENT-TUNNEL-PROXY
- INH-CONSOLE-PORT
- RTRV-AUDIT-LOG
- RTRV-BULKROLL
- RTRV-TUNNEL-FIREWALL
- RTRV-TUNNEL-PROXY
- RTRV-FFP
- RTRV-ROLL
- RTRV-ROUTE-GRE
- RTRV-TADRMAP

Command Syntax Changes

The syntax of the following commands is changed in Release 6.0.x.

Note These changes apply to all ONS platforms.

COPY-IOSCFG syntax:

COPY-IOSCFG[:<TID>]:<aid>:<CTAG>::SRC=<src>,DEST=<dest>;

Is changed to:

COPY-IOSCFG[:<TID>]:<aid>:<CTAG>::SRC=<src>,DEST=<dest>[,FTTD=<fttd>];

COPY-RFILE syntax:

COPY-RFILE[:<TID>]:<src>:<CTAG>::TYPE=<xfertype>,[SRC=<srcurl>,][DEST=<desturl>,][OVWRT=<ovwrt>,][FTTD=<fttd>];

Is changed to:

COPY-RFILE[:<TID>][:<src>]:<CTAG>::TYPE=<xfertype>,[SRC=<srcurl>,][DEST=<desturl>,][OVWRT=<ovwrt>,][FTTD=<fttd>];

DLT-ROUTE syntax:

DLT-ROUTE[:<TID>]::<CTAG>::<DESTIP>,<IPMASK>;

Is changed to:

DLT-ROUTE[:<TID>]::<CTAG>::<DESTIP>;

ED-10GIGE syntax:

ED-10GIGE[:<TID>]:<aid>:<CTAG>[:::NAME=<portname>,][MACADDR=<macaddr>,][MFS=<mfs>,][CMDMDE=<cmdmde>][:<pst>[,<sst>]];

Is changed to:

ED-10GIGE[:<TID>]:<aid>:<CTAG>[:::NAME=<portname>,][MACADDR=<macaddr>,][MFS=<mfs>,][CMDMDE=<cmdmde>,][FREQ=<freq>,][LOSSB=<lossb>][:<pst>[,<sst>]];

ED-BITS syntax:

ED-BITS[:<TID>]:<aid>:<CTAG>[:::LINECDE=<linecde>,][FMT=<fmt>,][SABIT=<sabit>,][IMPEDANCE=<impedance>,][LBO=<lbo>,][SYNCMSG=<syncmsg>,][AISTHRSHLD=<aisthrshld>,][BITSFAC=<bitsfac>,][ADMSSM=<admssm>][:<pst>];

Is changed to:

ED-BITS[:<TID>]:<aid>:<CTAG>[:::LINECDE=<linecde>,][FMT=<fmt>,][SABIT=<sabit>,][LBO=<lbo>,][SYNCMSG=<syncmsg>,][AISTHRSHLD=<aisthrshld>,][BITSFAC=<bitsfac>,][ADMSSM=<admssm>][:<pst>];

ED-CRS-STS-PATH syntax:

ED-CRS-STS-PATH:<src>,<dst>:<CTAG>[:::ADD=<add>,][REMOVE=<remove>,][CKTID=<cktid>,][CMDMDE=<cmdmde>][:<pst>[,<sst>]]

Is changed to:

ED-CRS-STS-PATH:<src>,<dst>:<CTAG>[::<cct>][:ADD=<add>,][REMOVE=<remove>,][CKTID=<cktid>,][CMDMDE=<cmdmde>][:<pst>[,<sst>]]

ED-E1 syntax:

ED-E1[:<TID>]:<aid>:<CTAG>[:::LINECDE=<linecde>,][FMT=<fmt>,][TACC=<tacc>,][TAPTYPE=<taptype>,][SFBER=<sfber>,][SDBER=<sdber>,][SOAK=<soak>,][NAME=<name>,][CMDMDE=<cmdmde>][:<pst>[,<sst>]];

Is changed to:

ED-E1[:<TID>]:<aid>:<CTAG>[:::LINECDE=<linecde>,][FMT=<fmt>,][TACC=<tacc>,][TAPTYPE=<taptype>,][SFBER=<sfber>,][SDBER=<sdber>,][SOAK=<soak>,][NAME=<name>,][CMDMDE=<cmdmde>,][SYNCMSG=<syncmsg>,][SENDDUS=<senddus>,][ADMSSM=<admssm>,][SABIT=<sabit>][:<pst>[,<sst>]];

ED-EC1 syntax:

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

Is changed to:

ED-EC1[:<TID>]:<aid>:<CTAG>[:::PJMON=<pjmon>,][LBO=<lbo>,][SOAK=<soak>,][SFBER=<sfber>,][SDBER=<sdber>,][NAME=<name>,][AISONLPBK=<aisonlpbk>,][CMDMDE=<cmdmde>,][EXPTRC=<exptrc>,][TRC=<trc>,][TRCMODE=<trcmode>,][TRCFORMAT=<trcformat>][:<pst>[,<sst>]];

ED-FFP-MOD2 syntax:

ED-FFP-MOD2:<aid>:<CTAG>[:::PROTID=<protid>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][PSDIRN=<psdirn>][:]

Is changed to:

ED-FFP-MOD2:<aid>:<CTAG>[:::PROTID=<protid>,][RVRTV=<rvrtv>],

ED-G1000 syntax:

ED-G1000[:<TID>]:<aid>:<CTAG>[:::MFS=<mfs>,][FLOW=<flow>,][LOWMRK=<int>,][HIWMRK=<int>,][NAME=<name>,][CMDMDE=<cmdmde>,][SOAK=<soak>][:<pst>[,<sst>]];

Is changed to:

ED-G1000[:<TID>]:<aid>:<CTAG>[:::MFS=<mfs>,][FLOW=<flow>,][LOWMRK=<int>,][HIWMRK=<int>,][AUTONEG=<autoneg>,][NAME=<name>,][CMDMDE=<cmdmde>,][SOAK=<soak>][:<pst>[,<sst>]];

ED-GIGE syntax:

ED-GIGE[:<TID>]:<aid>:<CTAG>[:::ADMINSTATE=<adminstate>,][LINKSTATE=<linkstate>,][MTU=<mtu>,][FLOWCTRL=<flowctrl>,][OPTICS=<optics>,][DUPLEX=<duplex>,][SPEED=<speed>,][NAME=<name>,][CMDMDE=<cmdmde>][:<pst>[,<sst>]];

Is changed to:

ED-GIGE[:<TID>]:<aid>:<CTAG>[:::ADMINSTATE=<adminstate>,][LINKSTATE=<linkstate>,][FLOWCTRL=<flowctrl>,][OPTICS=<optics>,][DUPLEX=<duplex>,][SPEED=<speed>,][NAME=<name>,][CMDMDE=<cmdmde>,][FREQ=<freq>,][LOSSB=<lossb>][:<pst>[,<sst>]];

ED-NE-GEN syntax:

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

Is changed to:

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

ED-POS syntax:

ED-POS[:<TID>]:<src>:<CTAG>[:::ENCAP=<encap>,][NAME=<name>,][CMDMDE=<cmdmde>,][SOAK=<soak>][:<pst>[,<sst>]];

Is changed to:

ED-POS[:<TID>]:<aid>:<CTAG>;

ED-T1 syntax:

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

Is changed to:

ED-T1[:<TID>]:<aid>:<CTAG>[:::LINECDE=<linecde>,][FMT=<fmt>,][LBO=<lbo>,][TACC=<tacc>,][TAPTYPE=<taptype>,][SOAK=<soak>,][SFBER=<sfber>,][SDBER=<sdber>,][SYNCMSG=<syncmsg>,][SENDDUS=<senddus>,][NAME=<name>,][CMDMDE=<cmdmde>,][AISONLPBK=<aisonlpbk>,][MODE=<mode>,][SYNCMAP=<syncmap>,][ADMSSM=<admssm>,][VTMAP=<vtmap>,][AISVONAIS=<aisvonais>,][AISONLOF=<aisonlof>,][INHFELPBK=<inhfelpbk>][:<pst>[,<sst>]];

ED-T3 syntax:

ED-T3[:<TID>]:<aid>:<CTAG>[:::FMT=<fmt>,][LINECDE=<linecde>,][LBO=<lbo>,][INHFELPBK=<inhfelpbk>,][TACC=<tacc>,][TAPTYPE=<taptype>,][SOAK=<soak>,][SFBER=<sfber>,][SDBER=<sdber>,][NAME=<name>,][CMDMDE=<cmdmde>][:<pst>[,<sst>]];

Is changed to:

ED-T3[:<TID>]:<aid>:<CTAG>[:::FMT=<fmt>,][LINECDE=<linecde>,][LBO=<lbo>,][INHFELPBK=<inhfelpbk>,][TACC=<tacc>,][TAPTYPE=<taptype>,][SOAK=<soak>,][SFBER=<sfber>,][SDBER=<sdber>,][NAME=<name>,][AISONLPBK=<aisonlpbk>,][CMDMDE=<cmdmde>][:<pst>[,<sst>]];

ED-VC3 syntax:

ED-VC3[:<TID>]:<src>:<CTAG>[:::RVRTV=<rvrtv>,][RVTM=<rvtm>,][HOLDOFFTIMER=<holdofftimer>,][TACC=<tacc>,][TAPTYPE=<taptype>,][CMDMDE=<cmdmde>,][EXPTRC=<exptrc>,][TRC=<trc>,][TRCMODE=<trcmode>][:<pst>[,<sst>]];

Is changed to:

ED-VC3[:<TID>]:<src>:<CTAG>[:::RVRTV=<rvrtv>,][RVTM=<rvtm>,][HOLDOFFTIMER=<holdofftimer>,][TACC=<tacc>,][TAPTYPE=<taptype>,][CMDMDE=<cmdmde>,][EXPTRC=<exptrc>,][TRC=<trc>,][TRCMODE=<trcmode>,][TRCFORMAT=<trcformat>][:<pst>[,<sst>]];

ED-VT1 syntax:

ED-VT1[:<TID>]:<aid>:<CTAG>[:::RVRTV=<rvrtv>,][RVTM=<rvtm>,][HOLDOFFTIMER=<holdofftimer>,][TACC=<tacc>,][TAPTYPE=<taptype>,][CMDMDE=<cmdmde>,][EXPTRC=<exptrc>,][TRC=<trc>,][TRCMODE=<trcmode>][:<pst>[,<sst>]];

Is changed to:

ED-VT1[:<TID>]:<aid>:<CTAG>[:::SFBER=<sfber>,][SDBER=<sdber>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][HOLDOFFTIMER=<holdofftimer>,][TACC=<tacc>,][TAPTYPE=<taptype>,][CMDMDE=<cmdmde>,][EXPTRC=<exptrc>,][TRC=<trc>,][TRCMODE=<trcmode>,][TRCFORMAT=<trcformat>][:<pst>[,<sst>]];

ED-VT2 syntax:

ED-VT2[:<TID>]:<src>:<CTAG>[:::RVRTV=<rvrtv>,][RVTM=<rvtm>,][HOLDOFFTIMER=<holdofftimer>,][TACC=<tacc>,][TAPTYPE=<taptype>,][CMDMDE=<cmdmde>,][EXPTRC=<exptrc>,][TRC=<trc>,][TRCMODE=<trcmode>,][:<pst>[,<sst>]];

Is changed to:

ED-VT2[:<TID>]:<src>:<CTAG>[:::SFBER=<sfber>,][SDBER=<sdber>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][HOLDOFFTIMER=<holdofftimer>,][TACC=<tacc>,][TAPTYPE=<taptype>,][CMDMDE=<cmdmde>,][EXPTRC=<exptrc>,][TRC=<trc>,][TRCMODE=<trcmode>,][TRCFORMAT=<trcformat>][:<pst>[,<sst>]];

ENT-EQPT syntax:

ENT-EQPT[:<TID>]:<aid>:<CTAG>::<aidtype>[:PROTID=<protid>,][PRTYPE=<prtype>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][CARDMODE=<cardmode>,][PEERID=<protid>,][REGENNAME=<regenname>,][PWL=<pwl>,][CMDMDE=<cmdmde>][:];

Is changed to:

ENT-EQPT[:<TID>]:<aid>:<CTAG>::<aidtype>[:PROTID=<protid>,][PRTYPE=<prtype>,][RVRTV=<rvrtv>,][RVTM=<rvtm>,][CARDMODE=<cardmode>,][PEERID=<protid>,][REGENNAME=<regenname>,][PWL=<pwl>,][CMDMDE=<cmdmde>,][RETIME=<retime>][:];

ENT-ROLL syntax:

ENT-ROLL-<MOD_PATH>:[<TID>]:<src>,<dst>:<CTAG>:::RFROM=<rfrom>,RTO=<rto>,RMODE=<rmode>,[FORCE=<force>];

Is changed to:

ENT-ROLL-<MOD_PATH>:[<TID>]:<from>,<to>:<CTAG>:::RFROM=<rfrom>,RTO=<rto>,RMODE=<rmode>,[CMDMDE=<cmdmde>];

SET-ATTR-SECUDFLT syntax:

SET-ATTR-SECUDFLT[:<TID>]::<CTAG>[::PAGE=<page>,][PCND=<pcnd>,][MXINV=<mxinv>,][DURAL=<dural>,][TMOUT=<tmout>,][UOUT=<uout>,][PFRCD=<pfrcd>,][POLD=<pold>,][PINT=<pint>,][LOGIN=<login>,][PRIVLVL=<uap>];

Is changed to:

SET-ATTR-SECUDFLT[:<TID>]::<CTAG>[::PAGE=<page>,][PCND=<pcnd>,][MXINV=<mxinv>,][DURAL=<dural>,][TMOUT=<tmout>,][UOUT=<uout>,][PFRCD=<pfrcd>,][POLD=<pold>,][PINT=<pint>,][LOGIN=<login>,][PRIVLVL=<uap>,][PDIF=<pdif>];

Miscellaneous syntax changes:

Syntax:

[:<TID>]:<aid>:<CTAG>;

Is changed to:

[:<TID>]::<CTAG>;

Response:

<aid>:<sc>,[<switchtype>]

Is changed to:

[<vendor>],[<netype>]

Command Response Changes

The following TL1 responses have changed in Release 6.0.x.

Note These changes apply to all ONS platforms.

RTRV-10GIGE response:

<aid>:,,[<role>],[<status>]:[<portname>],[<macaddr>],[<lbcl>],[<opt>],[<opr>],[<mfs>]:<pst>,[<sst>]

Is changed to:

<aid>:,,[<role>],[<status>]:[<portname>],[<macaddr>],[<lbcl>],[<opt>],[<opr>],[<mfs>],[<freq>],[<lossb>]:<pst>,[<sst>]

RTRV-DS3I response:

<aid>::<fmt>,<linecde>,<lbo>,[<tacc>],[<taptype>],[<sfber>],[<sdber>],[<soak>],[<name>]:<pst>,[<sst>]

Is changed to:

<aid>::<fmt>,<linecde>,<lbo>,[<tacc>],[<taptype>],[<sfber>],[<sdber>],[<soak>],[<soakleft>],[<name>],[<inhfelpbk>]:<pst>,[<sst>]

RTRV-E1 response:

<aid>::<linecde>,<fmt>,[<tacc>],[<taptype>],[<sfber>],[<sdber>],[<soak>],[<name>]:[<pst>],[<sst>]

Is changed to:

<aid>::<linecde>,<fmt>,[<tacc>],[<taptype>],[<sfber>],[<sdber>],[<soak>],[<soakleft>],[<name>],[<syncmsg>],[<senddus>],[<retime>],[<admssm>],[<providesync>],[<aisonlpbk>],[<saBit>]:[<pst>],[<sst>]

RTRV-E3 response:

<aid>::[<tacc>],[<taptype>],[<sfber>],[<sdber>],[<soak>],[<name>]:<pst>,[<sst>]

Is changed to:

<aid>::[<tacc>],[<taptype>],[<sfber>],[<sdber>],[<soak>],[<soakleft>],[<name>]:<pst>,[<sst>]

RTRV-E4 response:

<aid>::[<payload>],[<sfber>],[<sdber>],[<soak>],[<name>]:<pst>,[<sst>]

Is changed to:

<aid>::[<payload>],[<sfber>],[<sdber>],[<soak>],[<soakleft>],[<name>]:<pst>,[<sst>]

RTRV-EC1 response:

<aid>::[<pjmon>],[<lbo>],[<rxequal>],[<soak>],[<soakleft>],[<sfber>],[<sdber>],[<name>],[<aisonlpbk>]:<pst>,[<sst>]

Is changed to:

<aid>::[<pjmon>],[<lbo>],[<rxequal>],[<soak>],[<soakleft>],[<sfber>],[<sdber>],[<name>],[<aisonlpbk>],[<exptrc>],[<trc>],[<inctrc>],[<trcmode>],[<trcformat>]:<pst>,[<sst>]

RTRV-EQPT response:

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

Is changed to:

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

RTRV-FSTE response:

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

Is changed to:

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

RTRV-GIGE response:

<aid>::[<adminstate>],[<linkstate>],[<mtu>],[<flowctrl>],[<optics>],[<duplex>],[<speed>],[<name>]:<pst>,[<sst>]

Is changed to:

<aid>:,,[<role>],[<status>]:[<adminstate>],[<linkstate>],[<mtu>],[<flowctrl>],[<optics>],[<duplex>],[<speed>],[<name>],[<freq>],[<lossb>]:<pst>,[<sst>]

RTRV-INV response:

<aid>,<aidtype>::[<plugtype>],[<pn>],[<hwrev>],[<fwrev>],[<sn>],[<clei>],[<twl1=nwl in code>],[<twl2= wl1 in code>],[<twl3=wl2 in code>],[<twl4=wl3 in code>],[<pluginvendorid>],[<pluginpn>],[<pluginhwrev>],[<pluginfwrev>],[<pluginsn>],[<ilossref>],[<productId>],[<versionId>],[<fpgaVersion>]

Is changed to:

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

RTRV-STM1E response:

<aid>::[<payload>],[<syncmsg>],[<senddus>],[<sfber>],[<sdber>],[<soak>],[<name>]:<pst>,[<sst>]

Is changed to:

<aid>::[<payload>],[<syncmsg>],[<senddus>],[<sfber>],[<sdber>],[<soak>],[<soakleft>],[<name>]:<pst>,[<sst>]

RTRV-T1 response:

<aid>::[<linecde>],[<fmt>],[<lbo>],[<tacc>],[<taptype>],[<soak>],[<soakleft>],[<sfber>],[<sdber>],[<name>],[<syncmsg>],[<senddus>],[<retime>],[<aisonlpbk>]:<pst>,[<sst>]

Is changed to:

<aid>::[<linecde>],[<fmt>],[<lbo>],[<tacc>],[<taptype>],[<soak>],[<soakleft>],[<sfber>],[<sdber>],[<name>],[<syncmsg>],[<senddus>],[<retime>],[<aisonlpbk>],[<aisvonais>],[<aisonlof>],[<mode>],[<syncmap>],[<admssm>],[<providesync>],[<vtmap>],[<inhfelpbk>]:<pst>,[<sst>]

RTRV-VT2 response:

<aid>::[<sfber>],[<sdber>],[<rvrtv>],[<rvtm>],[<holdofftimer>],[<exptrc>],[<trc>],[<inctrc>],[<trcmode>],[<tacc>],[<taptype>],[<upsrpthstate>]:<pst>,[<sst>]

Is changed to:

<aid>::[<sfber>],[<sdber>],[<rvrtv>],[<rvtm>],[<holdofftimer>],[<exptrc>],[<trc>],[<inctrc>],[<trcmode>],[<trcformat>],[<tacc>],[<taptype>],[<upsrpthstate>]:<pst>,[<sst>]

SET-TOD response:

<year>,<month>,<day>,<hour>,<minute>,<second>,<tmtype>

Is changed to:

<year>,<month>,<day>,<hour>,<minute>,<second>,<difference>:<tmtype>

TL1 ENUM Changes

Note These changes apply to all ONS platforms.

TL1 ENUM Types Changed

The following enum types have been merged into the EQUIPMENT_TYPE enum type.

- EQUIPMENT_TYPE_15310
- EQUIPMENT_TYPE_15327
- EQUIPMENT_TYPE_15454

TL1 ENUM Items Added or Removed

The following section, including Table 1 through Table 29, highlights ENUM items changed (added or removed) for Release 6.0.x, by ENUM type.

Table 1 ADDRTYPE enum items added to Release 6.0.x

ENUM Name	ENUM Value
ADDRTYPE_ENUM_IP	“IP”
ADDRTYPE_ENUM_IPANDNSAP	“IP-AND-NSAP”
ADDRTYPE_ENUM_NSAP	“NSAP”

ADDRTYPE is used in the following commands:

- DLT-TADRMAP

Table 2 CARDMODE enum items added to Release 6.0.x

ENUM Name	ENUM Value
CARDMODE_DS1E1_DS1ONLY	“DS1E1-DS1ONLY”
CARDMODE_DS1E1_E1ONLY	“DS1E1-E1ONLY”

CARDMODE is used in the following commands:

- ED-EQPT
- ENT-EQPT

- RTRV-EQPT

Table 3 DL_TYPE enum items added to Release 6.0.x

ENUM Name	ENUM Value
DL_TYPE_ACCEPT	“ACPT”
DL_TYPE_CANC	“CANC”

DL_TYPE is used in the following commands:

- APPLY

Table 4 ENCODING enum items added to Release 6.0.x

ENUM Name	ENUM Value
ENCODING_ENUM_LV	“LV”
ENCODING_ENUM_RAWCISCO	“RAW-CISCO”
ENCODING_ENUM_RAWSTD	“RAW-STD”

ENCODING is used in the following commands:

- ENT-TADRMAP

Table 5 ENV_ALM enum items added to Release 6.0.x

ENUM Name	ENUM Value
ENV_ALM_ENV_ALM_ENGTRANS	“ENGTRANS”
ENV_ALM_ENV_ALM_FUELLEAK	“FUELLEAK”
ENV_ALM_ENV_ALM_GASALARM	“GASALARM”
ENV_ALM_ENV_ALM_HATCH	“HATCH”
ENV_ALM_ENV_ALM_LEVELCON	“LEVELCON”
ENV_ALM_ENV_ALM_LVDADSL	“LVDADSL”
ENV_ALM_ENV_ALM_LVDBYPAS	“LVDBYPAS”
ENV_ALM_ENV_ALM_PWRMJ	“PWRMJ”
ENV_ALM_ENV_ALM_PWRMN	“PWRMN”
ENV_ALM_ENV_ALM_PWR_139	“PWR-139”
ENV_ALM_ENV_ALM_PWR_190	“PWR-190”
ENV_ALM_ENV_ALM_RINGENMN	“RINGENMN”
ENV_ALM_ENV_ALM_RINGGENMJ	“RINGGENMJ”
ENV_ALM_ENV_ALM_RTACADSL	“RTACADSL”
ENV_ALM_ENV_ALM_RTACCRIT	“RTACCRIT”
ENV_ALM_ENV_ALM_RTACPWR	“RTACPWR”
ENV_ALM_ENV_ALM_RTACPWRENG	“RTACPWRENG”
ENV_ALM_ENV_ALM_RTBAYPWR	“RTBAYPWR”

Table 5 ENV_ALM enum items added to Release 6.0.x (Continued)

ENUM Name	ENUM Value
ENV_ALM_ENV_ALM_RTRVENG	“RTRVENG”
ENV_ALM_ENV_ALM_TEMP	“TEMP”
ENV_ALM_ENV_ALM_TREPEATER	“TREPEATER”

ENV_ALM is used in the following commands:

- RTRV-ALM-ENV
- RTRV-ATTR-ENV
- RTRV-COND-ENV
- SET-ATTR-ENV

Table 6 EQUIPMENT_TYPE enum items added to Release 6.0.x

ENUM Name	ENUM Value
EQUIPMENT_TYPE_ET_DS1_E1_56	“DS1-E1-56”
EQUIPMENT_TYPE_ET_FILLER	“FILLER”
EQUIPMENT_TYPE_ET_ML100FX	“ML100X-8”
EQUIPMENT_TYPE_ET_MRC_12	“MRC-12”
EQUIPMENT_TYPE_ET_OC192_XFP	“OC192-XFP”
EQUIPMENT_TYPE_ET_STM64_XFP	“STM64-XFP” (SDH Nomenclature of OC192-XFP)
EQUIPMENT_TYPE_ET_XCVXC10G	“XCVXC-10G”
EQUIPMENT_TYPE_ET_OPT_BST_E	“OPT-BST-E”

EQUIPMENT_TYPE is used in the following commands:

- CHG-EQPT
- ENT-EQPT

Table 7 EQPT_TYPE enum items added to Release 6.0.x

ENUM Name	ENUM Value
EQPT_TYPE_EQPT_ID_DS1_E1_56	“DS1-E1-56”
EQPT_TYPE_EQPT_ID_FILLER_CARD	“FILLER”
EQPT_TYPE_EQPT_ID_ML100FX	“ML100X-8”
EQPT_TYPE_EQPT_ID_MRC_12	“MRC-12”
EQPT_TYPE_EQPT_ID_OC192_XFP	“OC192-XFP”
EQPT_TYPE_EQPT_ID_STM64_XFP	“STM64-XFP” (SDH Nomenclature of OC192-XFP)
EQPT_TYPE_EQPT_ID_XCVXC10G	“XCVXC-10G”
EQPT_TYPE_EQPT_ID_OPT_BST_E	“OPT-BST-E”

EQPT_TYPE is used in the following command response:

- REPT_EVT

Table 8 FC_LINKRATE enum items dropped from Release 5.0.x

ENUM Name	ENUM Value
FC_LINKRATE_1GFC	“1GFC”
FC_LINKRATE_2GFC	“2GFC”

FC_LINKRATE is used in the following commands:

- RTRV-FC

Table 9 FC_LINKRATE enum items added to Release 6.0.x

ENUM Name	ENUM Value
FC_LINKRATE_1GBPS	“1GBPS”
FC_LINKRATE_2GBPS	“2GBPS”

FC_LINKRATE is used in the following commands:

- RTRV-FC

Table 10 FRAME_FORMAT enum items added to Release 6.0.x

ENUM Name	ENUM Value
FRAME_FORMAT_LT_JESF	“JESF”

FRAME_FORMAT is used in the following commands:

- ED-BITS
- ED-DS1
- ED-E1
- ED-T1
- RTRV-BITS
- RTRV-DS1
- RTRV-E1
- RTRV-T1

Table 11 LO_XC_MODE enum items added to Release 6.0.x

ENUM Name	ENUM Value
LO_XC_MODE_MIXED	“MIXED”
LO_XC_MODE_VC11	“VC11”
LO_XC_MODE_VC12	“VC12”
LO_XC_MODE_VT1	“VT1”
LO_XC_MODE_VT2	“VT2”

LO_XC_MODE is used in the following commands:

- ED-NE-PATH
- RTRV-NE-PATH

Table 12 LPBK_TYPE enum items dropped from Release 5.0.x

ENUM Name	ENUM Value
LPBK_TYPE_FE_CMD_ESF_PAYLD_LPBK	“PAYLOAD”

FC_LINKRATE is used in the following commands:

- RTRV-FC

Table 13 LPBK_TYPE enum items added to Release 6.0.x

ENUM Name	ENUM Value
LPBK_TYPE_FE_CMD_ESF_PAYLD_LPBK	“FE-CMD-ESF-PAYLOAD”
LPBK_TYPE_PAYLOAD_LPBK	“PAYLOAD”

LPBK_TYPE is used in the following commands:

- OPR-LPBK-MOD2
- RLS-LPBK-MOD2

Table 14 MOD2 enum items added to Release 6.0.x

ENUM Name	ENUM Value
MOD2_M2_VC11	“VC11”

MOD2 is used in the following commands:

- RTRV-FFP-MOD2
- RTRV-LNK-MOD2LNK
- RTRV-NE-APC
- RTRV-NE-WDMANS
- RTRV-TRC-OCH
- SCHED-PMREPT-MOD2

Table 15 MOD2ALM enum items added to Release 6.0.x

ENUM Name	ENUM Value
MOD2ALM_M2_VC11	“VC11”

MOD2ALM is used in the following commands:

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

Table 16 MOD2B enum items added to Release 6.0.x

ENUM Name	ENUM Value
MOD2B_M2_TSC	“TSC”
MOD2B_M2_VC11	“VC11”

MOD2B is used in the following commands:

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

Table 17 MOD_PATH enum items added to Release 6.0.x

ENUM Name	ENUM Value
MOD_PATH_M2_VC11	“VC11”

MOD_PATH is used in the following commands:

- ENT-VCG
- RTRV-CRS
- RTRV-PATH
- RTRV-TRC-OC48
- RTRV-VCG

Table 18 OPTICAL_WLEN enum items added to Release 6.0.x

ENUM Name	ENUM Value
OPTICAL_WLEN_WL_1310	“1310”
OPTICAL_WLEN_WL_1470	“1470”
OPTICAL_WLEN_WL_1490	“1490”
OPTICAL_WLEN_WL_1510	“1510”
OPTICAL_WLEN_WL_1530	“1530”
OPTICAL_WLEN_WL_1550	“1550”

Table 18 OPTICAL_WLEN enum items added to Release 6.0.x (Continued)

ENUM Name	ENUM Value
OPTICAL_WLEN_WL_1570	“1570”
OPTICAL_WLEN_WL_1590	“1590”
OPTICAL_WLEN_WL_1610	“1610”

OPTICAL_WLEN is used in the following commands:

- ED-10GIGE
- ED-DWDM-CLNT
- ED-EQPT
- ED-FC
- ED-GIGE
- ED-OCH
- ED-OCN-TYPE
- ENT-EQPT
- RTRV-10GIGE
- RTRV-DWDM-CLNT
- RTRV-EQPT
- RTRV-FC
- RTRV-GIGE
- RTRV-LNK-MOD2LNK
- RTRV-OCH
- RTRV-OCN-TYPE

Table 19 OPTICS enum items added to Release 6.0.x

ENUM Name	ENUM Value
OPTICS_OP_100_BASE_FX	“100_BASE_FX”
OPTICS_OP_100_BASE_LX	“100_BASE_LX”

OPTICS is used in the following commands:

- ED-GIGE
- RTRV-FSTE
- RTRV-G1000
- RTRV-GIGE

Table 20 PROTOCOLAID enum items added to Release 6.0.x

ENUM Name	ENUM Value
PROTOCOLAID_EMS	“EMS”
PROTOCOLAID_SHELL	“SHELL”
PROTOCOLAID_SNMP	“SNMP”
PROTOCOLAID_TL1	“TL1”

PROTOCOLAID is used in the following commands:

- ED-CMD-SECU

Table 21 PROTOCOLSTAT enum items added to Release 6.0.x

ENUM Name	ENUM Value
PROTOCOLSTAT_DISABLED	“DISABLED”
PROTOCOLSTAT_SECURE	“SECURE”
PROTOCOLSTAT_UNSECURE	“UNSECURE”

PROTOCOLSTAT is used in the following commands:

- ED-PROTOCOL

Table 22 REACH enum items added to Release 6.0.x

ENUM Name	ENUM Value
REACH_AUTOPROV	“AUTOPROV”
REACH_CX	“CX”
REACH_DX	“DX”
REACH_ER	“ER”
REACH_EW	“EW”
REACH_HX	“HX”
REACH_I1	“I1”
REACH_I2	“I2”
REACH_I3	“I3”
REACH_I5	“I5”
REACH_IR_1	“IR-1”
REACH_IR_2	“IR-2”
REACH_IR_3	“IR-3”
REACH_IR_5	“IR-5”
REACH_L1	“L1”
REACH_L2	“L2”
REACH_L3	“L3”

Table 22 REACH enum items added to Release 6.0.x (Continued)

ENUM Name	ENUM Value
REACH_L5	“L5”
REACH_LR	“LR”
REACH_LRM	“LRM”
REACH_LR_1	“LR-1”
REACH_LR_2	“LR-2”
REACH_LR_3	“LR-3”
REACH_LR_5	“LR-5”
REACH_LW	“LW”
REACH_LX	“LX”
REACH_MM	“MM”
REACH_MX	“MX”
REACH_P1L1	“P1L1”
REACH_S1	“S1”
REACH_S2	“S2”
REACH_S3	“S3”
REACH_S5	“S5”
REACH_SM	“SM”
REACH_SR	“SR”
REACH_SR_1	“SR-1”
REACH_SR_2	“SR-2”
REACH_SR_3	“SR-3”
REACH_SR_5	“SR-5”
REACH_SW	“SW”
REACH_SX	“SX”
REACH_T	“T”
REACH_V2	“V2”
REACH_V3	“V3”
REACH_VX	“VX”
REACH_ZX	“ZX”

REACH is used in the following commands:

- ED-10GIGE
- ED-DWDM-CLNT
- ED-FC
- ED-GIGE
- ED-OCN-TYPE

- RTRV-10GIGE
- RTRV-DWDM-CLNT
- RTRV-FC
- RTRV-GIGE
- RTRV-OCN-TYPE

Table 23 REQTYPE enum items added to Release 6.0.x

ENUM Name	ENUM Value
REQTYPE_ENH_24HR_BES	“ENH-24HR-BES”
REQTYPE_ENH_24HR_CSS_AND_LOFC	“ENH-24HR-CSS-AND-LOFC”
REQTYPE_ENH_24HR_ES	“ENH-24HR-ES”
REQTYPE_ENH_24HR_SES	“ENH-24HR-SES”
REQTYPE_ENH_24HR_UAS	“ENH-24HR-UAS”

REQTYPE is used in the following commands:

- RTRV-BFDLPM-MOD2

Table 24 RFILE enum items added to Release 6.0.x

ENUM Name	ENUM Value
RFILE_LOG	“RFILE-LOG”

RFILE is used in the following commands:

- COPY-IOSCFG
- COPY-RFILE

Table 25 SYNCMAP enum items added to Release 6.0.x

ENUM Name	ENUM Value
SYNCMAP_ASYNC	“ASYNC”
SYNCMAP_BYTE	“BYTE”

SYNCMAP is used in the following commands:

- ED-T1
- RTRV-T1

Table 26 SYNC_CLOCK_REF_QUALITY_LEVEL enum items dropped from Release 5.0.x

ENUM Name	ENUM Value
SYNC_CLOCK_REF_QUALITY_LEVEL_QREF_RES_SDH	“RES-SDH”

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

Table 27 TIDADRMODE enum items added to Release 6.0.x

ENUM Name	ENUM Value
TIDADRMODE_ENUM_ALL	“ALL”
TIDADRMODE_ENUM_DISC	“DISC”
TIDADRMODE_ENUM_IP	“IP”
TIDADRMODE_ENUM_NSAP	“NSAP”
TIDADRMODE_ENUM_PROV	“PROV”

TIDADRMODE is used in the following commands:

- RTRV-TADRMAP

Table 28 TRANSMODE enum items added to Release 6.0.x

ENUM Name	ENUM Value
TRANSMODE_AU3	“AU3”
TRANSMODE_AU4	“AU4”
TRANSMODE_SONET	“SONET”

TRANSMODE is used in the following commands:

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

Table 29 VTMAP enum items added to Release 6.0.x

ENUM Name	ENUM Value
VTMAP_GR253	“GR253”
VTMAP_INDUSTRY	“INDUSTRY”

VTMAP is used in the following commands:

- ED-T1
- RTRV-T1

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15327, Release 6.0*
- *Cisco ONS 15327 Software Upgrade Guide, Release 6.0*

Platform-Specific Documents

- *Cisco ONS 15327 Procedure Guide*
  Provides installation, turn up, test, and maintenance procedures
- *Cisco ONS 15327 Reference Manual*
  Provides technical reference information for SONET/SDH cards, nodes, and networks
- *Cisco ONS 15327 Troubleshooting Guide*
  Provides a list of SONET alarms and troubleshooting procedures, general troubleshooting information, and hardware replacement procedures
- *Cisco ONS SONET TL1 Command Guide*
  Provides a comprehensive list of TL1 commands

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.