



# Release Notes for Cisco ONS 15310-CL Release 6.0.3

---

August 2007



**Note**

---

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

---

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15310-CL. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to Release 6.0 of the *Cisco ONS 15310-CL Procedure Guide*, *Cisco ONS 15310-CL Reference Guide*, *Cisco ONS SONET TLI Command Guide*, and *Cisco ONS 15310-CL Troubleshooting Guide*. For the most current version of the Release Notes for Cisco ONS 15310-CL Release 6.0.3, visit the following URL:

[http://www.cisco.com/en/US/products/hw/optical/ps2006/prod\\_release\\_notes\\_list.html](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://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)

## Contents

- [Changes to the Release Notes, page 3](#)
- [Caveats, page 3](#)
- [Resolved Caveats for Release 6.0.x, page 4](#)
- [New Features and Functionality, page 5](#)
- [Related Documentation, page 37](#)
- [Obtaining Documentation, page 37](#)
- [Documentation Feedback, page 38](#)



---

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

Copyright © 2007 Cisco Systems, Inc. All rights reserved.

[Cisco Product Security Overview, page 39](#)

[Obtaining Technical Assistance, page 39](#)

[Obtaining Additional Publications and Information, page 41](#)

# Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15310-CL Release 6.0.3* since the production of the Cisco ONS 15310-CL 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 15310-CL. 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.

---

### 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.

## Data I/O Cards

### CSCsb40206

In Asymmetric configuration, with autonegotiation enabled and flow control selected, an ML-series card might fail to synchronize with, or to recognize the asymmetric flow control. This issue is under investigation.

## 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.

## 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 6.0.3.

## Maintenance and Administration

### CSCeg81602

A 100 second outage on DS1 traffic that is physically looped back, and in IS-AINS state, can occur during a span switch. With a loopback on the DS1 traffic a span switch will induce errors that raise a signal degrade (SD) on the DS1. The system then injects AIS due to the SD to keep from transitioning to IS from IS-AINS. To prevent this issue avoid using a physical loopback. This issue is resolved Release 6.0.

## Data I/O Cards

### CSCeh26707

Loss of Ethernet signal on one of the front ports takes longer than expected to be propagated to the remote port. Link integrity operates slower than expected for Ethernet failures (though it works as expected for SONET failures). To see this, any condition that causes an Ethernet loss of signal (removal of a front port Ethernet cable, for example) will invoke the Ethernet integrity function. This issue is resolved in Release 6.0.

### CSCeh28342

On ML-series in the ONS 15310-CL, when policing is enabled, the configured policed rate is not forwarded. This can occur when policing at a rate lower than 1 Mbps. The workaround is to set the policed rate higher than 1 Mbps, or to raise the configured policed rate until the desired rate is forwarded. This issue is resolved in Release 6.0.

## 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 is resolved in Release 6.0.

## New Features and Functionality

This section highlights new features and functionality for Release6.0.x. For complete documentation of each of the features of the ONS 15310-CL, consult the user documentation.

## New Software Features and Functionality

### Detectable Filler Card

As of Release 6.0, filler cards are detectable in CTC node view when installed in the ONS 15310-CL expansion slot. The filler card serves three functions: it prevents exposure to hazardous voltages and currents inside the ONS 15310-CL chassis, it eliminates electromagnetic interference (EMI) that might disrupt other equipment, and it directs the flow of cooling air through the chassis. If an expansion card (CE-100T-8 or ML-100T-8) is not plugged in, a filler card must be inserted in the expansion slot.

### Bridge and Roll

Release 6.0.x introduces bridge and roll for the ONS 15310-CL. 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.

## Protected Circuits

CTC allows you to roll the working or protect path regardless of which path is active. You can upgrade an unprotected circuit to a fully protected circuit or downgrade a fully protected circuit to an unprotected circuit with the exception of a path protection circuit. When using bridge and roll on path protection circuits, you can roll the source or destination, or both path selectors in a dual roll, but not a single path selector.

## 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), and access to line cards via IOS CLI (for cards in L2/L3 mode).

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
- Audit trail initiation support for IOS-based data cards in the L2/L3 mode (available over the Syslog/IOS CLI)
- 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, 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, 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 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, 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 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.

## IOS Security Enhancements

With Release 6.0.x the ML-Series card includes several security features. Some of these features can operate independent of the ONS node where the ML-Series card is installed. Others are configured using CTC or TL1.

Security features configured with Cisco IOS include:

- Cisco IOS login enhancements
- Secure Shell connection
- AAA/RADIUS stand alone mode
- Cisco IOS basic password

Security features configured with CTC or TL1 include:

- Disabled console port
- AAA/RADIUS relay mode

### Disabling the Console Port on the ML-Series Card

There are several ways to access the Cisco IOS running on the ML-Series card, including a direct connection to the console port, which is the RJ-11 serial port on the front of the card. As of Release 6.0, you can increase security by disabling this direct connection, which is enabled by default. This prevents console port input without preventing any console port output, such as Cisco IOS error messages.

You can disable console port access through CTC or TL1.

## Secure Login on the ML-Series Card

The ML-Series card supports the Cisco IOS login enhancements integrated into Cisco IOS Release 12.2(25)S and introduced in Cisco IOS Release 12.3(4)T. The enhancements allow users to better secure the ML-Series card when creating a virtual connection, such as Telnet, Secure Shell (SSH), or HTTP. The secure login feature records successful and failed login attempts for vty sessions on the ML-Series card. These features are configured using the Cisco IOS command-line interface (CLI).

## Secure Shell on the ML-Series Card

In previous releases the ML-Series card supported SSH version 1 (SSHv1) only. With Release 6.0.x the ML-Series card also supports SSH version 2 (SSHv2). SSHv2 offers security improvements over SSHv1 and is the default choice on the ML-Series card.

SSH has two applications, an SSH server and SSH client. The ML-Series card only supports the SSH server and does not support the SSH client. The SSH server in Cisco IOS software works with publicly and commercially available SSH clients.

The SSH server enables a connection into the ML-Series card, similar to an inbound Telnet connection, but with stronger security. Before SSH, security was limited to the native security in Telnet. SSH improves on this by allowing the use of Cisco IOS software authentication.

The ONS node also supports SSH. When SSH is enabled on the ONS node, the user must use SSH to connect to the ML-Series card for Cisco IOS CLI sessions. Telnet access to the ML-Series card is prevented when SSH is enabled on the ONS node except for connections through the console port of the ML-Series card. Disabling the console port on the ML-Series card will prevent this Telnet access.

## RADIUS on the ML-Series Card

RADIUS is a distributed client/server system that secures networks against unauthorized access. Clients send authentication requests to a central RADIUS server, which contains all user authentication and network service access information. The RADIUS host is normally a multiuser system running RADIUS server software from Cisco or another software provider.

Many Cisco products offer RADIUS support, including the ONS 15454, ONS 15454 SDH, ONS 15327, ONS 15310-CL, and ONS 15600. The ML-Series card also supports RADIUS.

The ML-Series card can operate either in RADIUS relay mode or in RADIUS stand alone mode (default). In either mode, the RADIUS messages from the ML-Series card are passed to a RADIUS server that is on the data communications network (DCN) used to manage the ONS node. For more information about RADIUS modes and operation on the ML-Series card 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.

## Manage Pluggable Port Modules

Release 6.0.x adds management for multirate (OC-3/OC-12) pluggable port modules (PPMs) in CTC for the 15310-CL-CTX.



#### Note

Single-rate SFPs are autoprovisioned in the PPM screen.

As of Release 6.0 you can provision or delete a multirate PPM, and you can provision or change optical line rates.



#### Note

You cannot delete a PPM if it is in service, part of a protection group, has a communications channel termination in use, is used as a timing source, has circuits, or has overhead circuits.

## Change Pluggable Port Module Service States

On the 15310-CL-CTX card, the PPM port is equivalent to an optical port. To change a PPM port's service state you can follow the same procedure as in changing any port's service state (refer to the user documentation for this procedure).

## Cisco Service Assurance Agent ML-Series Support

The Cisco Service Assurance Agent (SAA) is an application-aware synthetic operation agent that monitors network performance, especially IP SLAs. Performance can be measured between any Cisco device that supports this feature and any remote IP host (server), Cisco routing device, or mainframe host. Performance measurement statistics provided by this feature can be used for troubleshooting, for problem analysis, and for designing network topologies.

The Cisco SAA can be especially useful for enterprise and service provider networks, because it provides expanded measurement and management capabilities. In particular, the Cisco SAA is a reliable mechanism for accurately monitoring the metrics in SLAs.

Because Cisco SAA is accessible using SNMP, it also can be used in performance monitoring applications for network management systems (NMSs) such as CiscoWorks2000 (CiscoWorks Blue) and the Internetwork Performance Monitor (IPM). SAA notifications also can be enabled through Systems Network Architecture (SNA) network management vector transport (NMVT) for applications such as NetView.

For information on configuring the Cisco SAA to provide advanced network service monitoring information, see the “Network Monitoring Using Cisco Service Assurance Agent” chapter of the Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2.

## Cisco Service Assurance Agent on the ML-Series

As of Release 6.0, the ML-Series card has a complete IP SLA Cisco IOS subsystem and offers all the normal features and functions available in Cisco IOS Release 12.2S. It uses the standard IP SLA Cisco IOS CLI commands. SNMP support is equivalent to the support provided in the IP SLA subsystem 12.2(S), which is the rttMon MIB.

The following restrictions apply for ML-Series card operation with Cisco SAA.

The ML-Series card supports only features in the Cisco IOS 12.2S branch. It does not support functions available in future Cisco IOS versions, such as the IP SLA accuracy feature or the enhanced Cisco IOS CLI support with updated IP SLA nomenclature.

Setting the CoS bits is supported, but set CoS bits are not honored when leaving or entering the CPU when the sender or responder is an ONS 15454, ONS 15454 SDH or ONS 15310-CL platform. Set CoS bits are honored in intermediate ONS nodes.

On RPR, the direction of the data flow for the IP SLA packet might differ from the direction of customer traffic.

## 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 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 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 delete a firewall tunnel.

#### **RTRV-TUNNEL-FIREWALL**

- RETRIEVE-TUNNEL\_FIREWALL

This command is used to 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.

## New Card Support

The following new card is supported by TL1 in Release 6.0.x.

- Detectable filler card

## 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>],[OVRT=<ovwrt>],[FTTD=<fttd>];
```

Is changed to:

```
COPY-RFILE[:<TID>][:<src>]:<CTAG>::TYPE=<xfertype>,[SRC=<srcurl>],[DEST=<desturl>],[OVRT=<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=<ctid>],[CMDMDE=<cmdmde>][:<pst>[,<sst>]]
```

**ED-E1** syntax:

```
ED-E1[:<TID>]:<aid>:<CTAG>[:LINECDE=<linecde>],[FMT=<fmt>],[TACC=<tacc>],[T
APTYPE=<tatype>],[SFBER=<sfber>],[SDBER=<sdber>],[SOAK=<soak>],[NAME=<nam
e>],[CMDMDE=<cmdmde>][:<pst>[,<sst>]];
```

Is changed to:

```
ED-E1[:<TID>]:<aid>:<CTAG>[:LINECDE=<linecde>],[FMT=<fmt>],[TACC=<tacc>],[T
APTYPE=<tatype>],[SFBER=<sfber>],[SDBER=<sdber>],[SOAK=<soak>],[NAME=<nam
e>],[CMDMDE=<cmdmde>],[SYNCSMSG=<syncmsg>],[SENDDUS=<senddus>],[ADMSSM
=<admssm>],[SABIT=<sabit>][:<pst>[,<sst>]];
```

**ED-EC1** syntax:

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

Is changed to:

```
ED-EC1[:<TID>]:<aid>:<CTAG>[:PJMON=<pjmon>],[LBO=<lbo>],[SOAK=<soak>],[SF
BER=<sfber>],[SDBER=<sdber>],[NAME=<name>],[AISONLPBK=<aisonlpbk>],[CMDM
DE=<cmdmde>],[EXPTRC=<exptrc>],[TRC=<trc>],[TRCMODE=<trcmode>],[TRCFORM
AT=<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>],[SO
AK=<soak>][:<pst>[,<sst>]];
```

**ED-GIGE** syntax:

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

Is changed to:

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

**ED-NE-GEN** syntax:

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

Is changed to:

```
ED-NE-GEN[:<TID>]:<CTAG>[:<<NAME=<name>,][IPADDR=<ipaddr>],[IPMASK=<ipmask>],[DEFRTR=<defrtr>],[IIOPORT=<iioport>],[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=<tatype>],[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=<tatype>],[SOAK=<soak>],[SFBER=<sfber>],[SDBER=<sdber>],[SYNMSG=<synmsg>],[SENDUS=<sendus>],[NAME=<name>],[CMDMDE=<cmdmde>],[AISONLPBK=<aisonlpbk>],[MODE=<mode>],[SYNMAP=<synmap>],[ADMSSM=<admssm>],[VTMAP=<vmap>],[AISONAIS=<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=<tatype>],[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=<tatype>],[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=<tatype>],[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=<tatype>],[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=<tatype>],[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>],[TAPATYPE=<taptyp e>],[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>],[TAPATYPE=<taptyp e>],[CMDMDE=<cmdmde>],[EXPTR C=<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>],[TAPATYPE=<taptyp e>],[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>],[REG ENNAME=<regename>],[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>],[REG ENNAME=<regename>],[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>],[POL D=<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>],[POL D=<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>],[<netytype>]

## 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>]:<ps
t>,[<sst>]
```

Is changed to:

```
<aid>:.,[<role>],[<status>]:[<portname>],[<macaddr>],[<lbcl>],[<opt>],[<opr>],[<mfs>],[<fr
eq>],[<lossb>]:<pst>,[<sst>]
```

#### RTRV-DS3I response:

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

Is changed to:

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

#### RTRV-E1 response:

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

Is changed to:

```
<aid>::<linecde>,<fmt>,[<tacc>],[<tatype>],[<sfber>],[<sdber>],[<soak>],[<soakleft>],[<na
me>],[<syncmsg>],[<senddus>],[<retime>],[<admssm>],[<providesync>],[<aisonlpbk>],[<sa
Bit>]:[<pst>],[<sst>]
```

#### RTRV-E3 response:

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

Is changed to:

```
<aid>::[<tacc>],[<tatype>],[<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=w1 in code>,<twl3=w12 in code>,<twl4=w13 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>,<tatype>,<soak>,<soakleft>,<sfber>,<sdber>,<name>,<syncmsg>,<senddus>,<retime>,<aisonlpbk>:<pst>,<sst>
```

Is changed to:

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

**RTRV-VT2** response:

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

Is changed to:

```
<aid>::[<sfber>],[<sdber>],[<rvrtv>],[<rvtm>],[<holdofftimer>],[<exptrc>],[<trc>],[<inctrc>],[<trcmode>],[<trcformat>],[<tacc>],[<tatype>],[<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”

**Table 5** ENV\_ALM enum items added to Release 6.0.x (Continued)

ENUM Name	ENUM Value
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”
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"
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”

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

<b>ENUM Name</b>	<b>ENUM Value</b>
REACH_IR_3	"IR-3"
REACH_IR_5	"IR-5"
REACH_L1	"L1"
REACH_L2	"L2"
REACH_L3	"L3"
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_PIL1	"PIL1"
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** *SYNCPMAP enum items added to Release 6.0.x*

ENUM Name	ENUM Value
SYNCPMAP_ASYNC	“ASYNC”
SYNCPMAP_BYTE	“BYTE”

SYNCPMAP 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 15310-CL, Release 6.0*

### Platform-Specific Documents

- *Cisco ONS 15310-CL Procedure Guide*  
Provides installation, turn up, test, and maintenance procedures
- *Cisco ONS 15310-CL Reference Manual*  
Provides technical reference information for SONET/SDH cards, nodes, and networks
- *Cisco ONS 15310-CL 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

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can send comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

# Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)
- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

## Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



### Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2007, Cisco Systems, Inc.  
All rights reserved.