



# Getting Started

---

TL1 (Transaction Language One) is a subset of the input and output messages contained in the ITU (International Telecommunications Union) MML (Man-Machine Language). TL1 provides a standard set of messages that can be used for communicating between operating systems and network elements, and personnel and network elements. The Cisco ONS 15540 ESPx can support up to 32 concurrent TL1 sessions. For more information about TL1, refer to Telcordia document GR-833-CORE, *Network Maintenance: Network Element and Transport Surveillance Messages*.

This chapter provides information and procedures for getting started with TL1 including:

- [1.1 Setting Up TL1 Communication, page 1-2](#)
- [1.2 TL1 Command Syntax, page 1-3](#)
- [1.3 Autonomous Messages, page 1-4](#)
- [1.4 TL1 Commands by User Security, page 1-5](#)
- [1.5 Mixed Mode Timing Support, page 1-6](#)
- [1.6 TL1 Command Completion Behavior, page 1-6](#)
- [1.7 Command Completion Behavior for Retrieval Commands, page 1-7](#)


## 1.1 Setting Up TL1 Communication

The period during which a user is logged into the Cisco ONS 15540 ESPx is called a session. You can use Telnet to open a session (login). The TL1 PID (password) is masked when accessing a TL1 session. When you logout, you are closing a session. The Cisco ONS 15540 ESPx allows a maximum of 32 concurrent TL1 sessions.

### 1.1.1 Opening a TL1 Session

Use the following procedure to open a TL1 session through Telnet. In the procedure the Activate and Cancel User commands are shown in their input format. For more information about these and other commands and messages, see [Chapter 3, “TL1 Commands.”](#)

To access TL1 commands in a Telnet session with a PC running Windows, follow these steps:

- 
- Step 1** Type **cmd** at the DOS prompt and then click **OK**. (The same steps can also be done from a UNIX prompt.)
- Step 2** Type **TELNET <NODE IP ADDRESS OR NODE NAME> <PORT NUMBER>** and then press **Enter**.  
The node IP address or name refers to the IP address or name of the node that you want to communicate with. Port number is the port (2361, 3082, or 3083) where TL1 commands are understood. If the connection is successful, a screen opens with a prompt.
- Step 3** Open a TL1 session by typing **ACT-USER:[<TID>]:<UID>:<CTAG>::<PID>;**
- 
-  **Note** When the semicolon is typed, the command is issued immediately.
- 
- Step 4** Close a TL1 session by typing **CANC-USER:[<TID>]:<USERID>:<CTAG>;**
-

## 1.2 TL1 Command Syntax

TL1 commands conform to the following syntax:

```
a:b:c:d:e: ... z;
```

where:

“a” is the command code

“b” is the target identifier (TID)

“c” is the access identifier (AID) or the user identifier (UID)

“d” is the correlation tag (CTAG)

“e: ... z;” are other positions required for various commands

The TID, AID, UID, and CTAG route and control the TL1 command. Other parameters provide additional information required to complete the action requested by the command. TL1 command codes, parameter names, and parameter values can be either uppercase or lowercase exclusively or any combination of the two, unless specifically noted in the command description.

The TID is a unique name given to each system when it is installed. The name identifies the particular NE (network element) to which each command is directed. Each TID can have a maximum of 20 ASCII characters limited to letters, digits, and hyphens, but each TID must start with an alphabetic character. The presence of the TID is required in all input commands, but its value can be null (represented by two successive colons). The TID can be null when the operating system directly communicates with the target NE. The recommended value for the TID, when it is used, is the target’s CLI code.



### Note

If the TID contains any characters other than letters and digits, such as spaces, the text string form (enclosed in double quotes) must be used.

The AID is an access code used to identify and address specific objects within the Cisco ONS 15540 ESPx. These objects include individual pieces of equipment, transport spans, access tributaries, and other objects.

The CTAG is a unique identifier given to each input command by the user. When the Cisco ONS 15540 ESPx system responds to a specific command, it includes the command’s CTAG in the reply. Including the CTAG eliminates discrepancies about which response corresponds to which command. Valid CTAG values include strings of up to six characters comprised of identifiers (alphanumeric, beginning with a letter) or decimal numerals (a string of decimal digits with an optional non-trailing “.”).

The following specification characters are used throughout this document as vehicles for defining the syntax:

- < > enclose a symbol specifier, for example <CTAG>.
- [ ] enclose an optional symbol, for example [<TID>].
- “ ” enclose a literal character, for example an output format  
“SLOT-7:PLUGIN,TC,,,,,:\“EQUIPMENT PLUG-IN\”,TCC”
- ^ is a space, a literal blank character used only in examples of messages.

## 1.3 Autonomous Messages

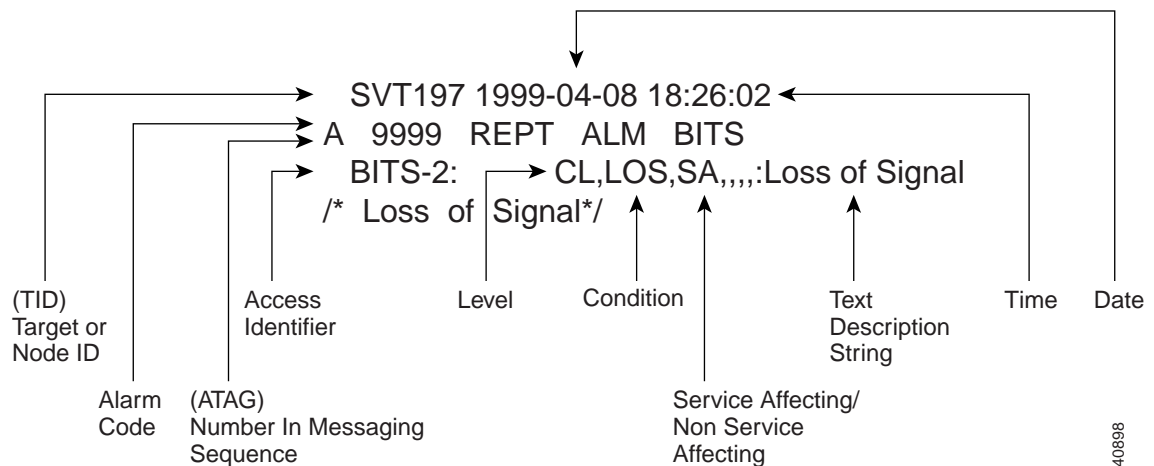
The autonomous TL1 messages are listed alphabetically in [Chapter 2, “TL1 Command Components”](#). [Figure 1-1](#) shows the autonomous message format. The autonomous message tag (ATAG) is used for message sequencing. The number is incremented by one for each autonomous message sent by the Cisco ONS 15540 ESPx. The Cisco ONS 15540 ESPx uses whole numbers 0000 to 9999.



### Note

Some autonomous messages (REPT DBCHG and REPT EVT SESSION, for example) differ slightly from the format shown in the third line of [Figure 1-1](#).

*Figure 1-1 Autonomous Message Format*



### 1.3.1 Alarm Codes

The alarm code indicates the severity of the autonomous message. Valid values for alarm codes in decreasing order of severity are as follows:

- \*C Critical alarm
- \*\* Major alarm
- \*^ Minor alarm
- A^ Non-alarm message

Critical, major, and minor correspond to the reporting of alarmed events. The non-alarm message designation is used when the NE is reporting non-alarmed events, periodic measurements, or results of previously scheduled diagnostics or audits. If multiple alarms are reported in the same message, the alarm code is the highest severity of those being reported.

The following example shows an output message that includes the critical alarm code:

```
AB7-56 1970-01-01 16:02:10
*C 100.100 REPT ALM EQPT
"SYSTEM:CR,HITEMP,NSA,,,,:\`High Temperature\`,TCC"
```

For more information about alarms, see the [“2.4 Errors”](#) section on page 2-8.

## 1.4 TL1 Commands by User Security

Table 1-1 specifies command access privileges for each user security level.

*Table 1-1 Command Access*

Command	Superuser	Provisioning	Maintenance	Retrieve
ALW-MSG-SECU	X			
ALW-USER-SECU	X			
APPLY	X			
COPY-RFILE	X			
DLT-USER-SECU	X			
ED-DAT	X			
ED-USER-SECU	X			
ENT-USER-SECU	X			
INH-MSG-SECU	X			
INH-USER-SECU	X			
REPT EVT SECU	X			
DLT-*_*	X	X		
ED-*_*	X	X		
ENT-*_*	X	X		
SET-*_*	X	X		
SET-TOD	X	X		
INIT-*_*	X	X	X	
OPR-*_*	X	X	X	
RLS-*_*	X	X	X	
RMV-*_*	X	X	X	
RST-*_*	X	X	X	
SW-*_*	X	X	X	
ACT-*_*	X	X	X	X
ALW-*_*	X	X	X	X
CANC-*_*	X	X	X	X
ED-PID	X	X	X	X
INH-*_*	X	X	X	X
REPT *_* <sup>1</sup>	X	X	X	X
RTRV-*_*	X	X	X	X

1. REPT EVT SECU applies to the Superuser only.

User security levels limit the amount of time a user can leave the system idle before the TL1 session is locked to prevent unauthorized users from making changes. Higher security levels have shorter timeouts. If provisioned, it only affects users who are not currently logged in. A user who is logged in has to log out and log back in before the new timeouts can take effect.

Table 1-2 shows security levels and their default timeouts.

*Table 1-2 Security Default Timeouts*

Security Level	Default Timeouts
Retrieve	Unlimited
Maintenance	60 minutes
Provisioning	30 minutes
Superuser	15 minutes

## 1.5 Mixed Mode Timing Support

Although TL1 supports mixed mode timing in this release, we strongly advise against its implementation. Mixed mode timing runs an inherent risk of creating timing loops. Refer to Telcordia document GR-436-CORE, *Digital Network Synchronization Plan*, for recommended synchronization planning.

## 1.6 TL1 Command Completion Behavior

When you enter a TL1 command, one of three completion codes is returned. The completion codes are: completed (COMPLD), partial (PRTL), and deny (DENY). You can specify an explicit, implicit, or explicit with implicit list as explained in the following sections.



### Note

The command completion behavior does not apply to the following commands: RTRV-CRS, RTRV-ALM, and RTVR-COND commands.

### 1.6.1 Explicit List of AIDs - No Wildcards

If a set of AIDs (access identifiers) is explicitly listed, including a set of just one AID, then each AID must complete successfully to return a COMPLD message. If more than one AID is in the set and at least one AID succeeds but all do not, then a PRTL with errors for each failed AID is returned. If all AIDs in the set fail, a DENY with errors for each failed AID is returned.

```
SLOT-1
FAC-2-1&FAC-3-3&FAC-4-2
```

## 1.7 Command Completion Behavior for Retrieval Commands

If you enter a RTRV-CRS command, then one of three completion codes is returned. They are completed (COMPLD), partial (PRTL), and deny (DENY). You can specify an explicit, implicit, or explicit with implicit list as explained in the following sections.

### 1.7.1 Explicit List of AIDs for Retrieval Commands - No Wildcards

For an explicit list of AIDs on a RTRV-EQPT command, an error code is returned for each AID that fails validation (for example, the user specifies STS-N-13 when SLOT-N only contains an OC-12) or for each AID where no matching cross-connection is found. To determine the completion code, follow the rules from the [“1.6.1 Explicit List of AIDs - No Wildcards” section on page 1-6](#). If the result is either PRTL or COMPLD, then a list of matching cross-connections will accompany the response.

