CHAPTER 1

ACT Commands

This chapter provides activate (ACT) commands for the Cisco ONS 15310-MA, Cisco ONS 15454, Cisco ONS 15454 M2, and Cisco ONS 15454 M6.

Note All commands supported on the Cisco ONS 15454 platform are also supported on Cisco ONS 15454 M2 and Cisco ONS 15454 M6 platforms.

1.1 ACT-USER

(Cisco ONS 15310-MA and Cisco ONS 15454) The Activate User (ACT-USER) command opens a session with the network element (NE).

Usage Guidelines

- Passwords are masked for the following security commands: ACT-USER, COPY-RFILE, COPY-IOSCFG, ED-PID, ENT-USER-SECU, and ED-USER-SECU. The password will be masked when accessing a TL1 session through any means. The Cisco Transport Controller (CTC) Request History and Message Log also show the commands as masked. When a password-masked command is reissued by double-clicking the command from CTC Request History, the password is masked in the CTC Request History and Message Log. The actual password that was previously issued is sent to the NE. To use a former command as a template only, single-click the command in CTC Request History. The command is placed in the Command Request text box, where you can edit the appropriate fields prior to reissuing it.
- For the ACT-USER command:

  ACT-USER:[TID]:[STRING]:CTAG::[STRING]

  - The syntax of the user ID (first [STRING]) and the password (second [STRING]) are not checked.
  - Invalid syntax for both the user ID and password is permitted, but the user can only log in if the user ID/password match what is in the database.
  - The user ID and password cannot exceed 10 characters.
- For the ACT-USER command, no error code is transmitted except to convey that the login is granted or denied. According to Telcordia TR-835, Appendix A, Section A.2, "... the error codes corresponding to ACT ... do not apply to the ACT-USER command because this command requires

that no error code be provided to the session request except to indicate that it has been denied. Before a session is established, a specific error code might reveal clues to an intruder attempting unauthorized entry."

- In some configurations, a new user must change his or her password after establishing a session for the first time before continuing. All TL1 commands except for ED-PID and CANC-USER are denied until the password is changed. When the password has been changed, a user can execute any command that his security level allows. If the user logs out without changing his password, each following session will DENY all commands, except ED-PID and CANC-USER, until the password is changed. Starting with Release 4.6, this feature can be turned on or off. The default is off.

Category Security

Security N/A

Input Format ACT-USER:[<TID>]:<UID>:<CTAG>::<PID>;

Input Example ACT-USER:PETALUMA:TERRI:100::MYPASSWD;

Table 1-1 Input Parameter Support

Parameter	Description	Cisco ONS 15454	Cisco ONS 15310-MA
<UID>	The user identifier (user ID) of the person logged in. UID can be any combination of up to 10 alphanumeric characters. UID is a string. It must not be null.	Y	Y
<PID>	The user password. PID is any combination of up to 10 alphanumeric characters. Passwords are encrypted for security reasons and will appear as asterisks (*). PID is a string. It must not be null.	Y	Y

Output Format

```
   SID DATE TIME
M  CTAG COMPLD
   "<UID>:<LASTLOGINTIME>,<UNSUCCESSFULLOGINS>"
;
```

Output Example

```
   TID-000 1998-06-20 14:30:00
M  001 COMPLD
   "TERRI:2003-01-02 14-04-49,0"
;
```

Output Parameters

<UID>	The user ID of the person logged in. The UID can be any combination of up to 10 alphanumeric characters. UID is a string. It must not be null.
<LASTLOGINTIME>	The date and time of the last successful connection to the NE (not including current login). LASTLOGINTIME is a string.
<UNSUCCESSFULLOGINS>	The number of unsuccessful login attempts since the last successful login. UNSUCCESSFULLOGINS is an integer.