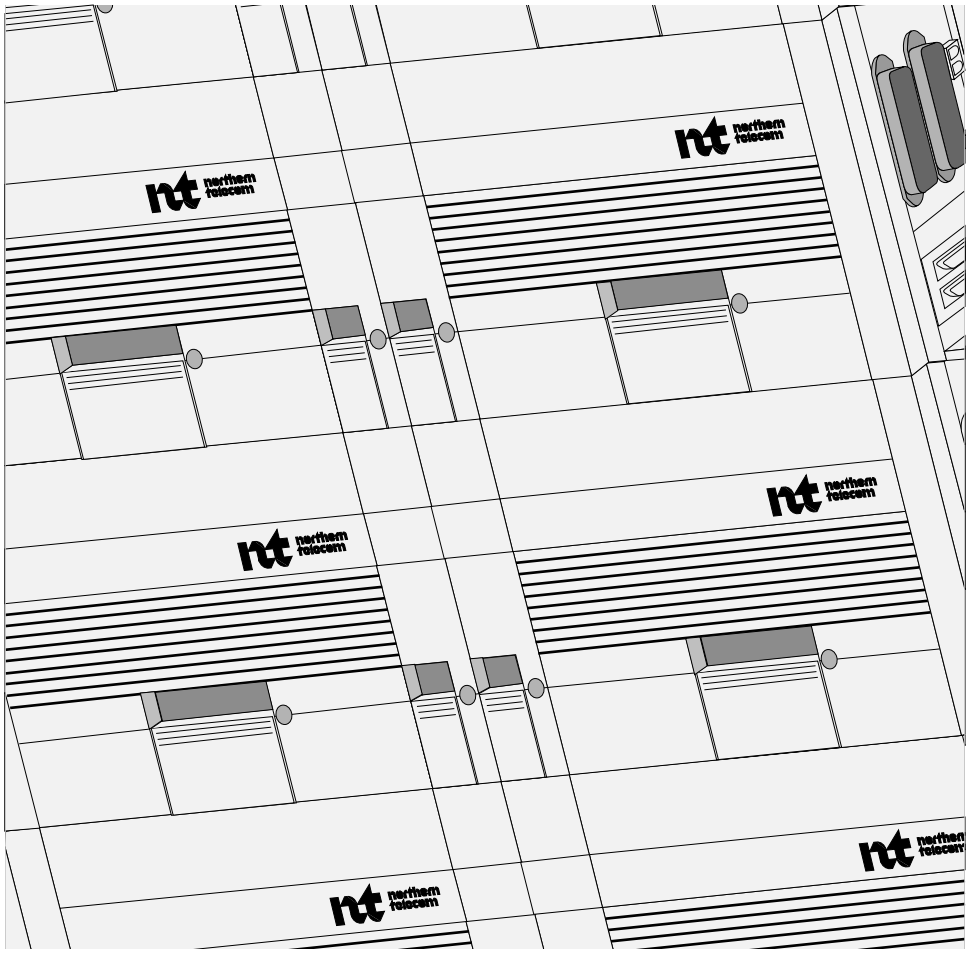
P0909010

SONET Products

AccessNode

TL1 Enhanced Security Quick Reference Guide

Issue 1.0 August 1999



NORTEL NETWORKS™

SONET Products

AccessNode

TL1 Enhanced Security Quick Reference Guide

Document number: P0909010
Document release: Issue 1.0
Date: August 1999

Publication history

August 1999

Initial release of the document, Issue 1.0, for AN17.11.

Contents

About this document

This document is a quick reference guide to the Transaction Language 1 (TL1) enhanced security commands. Topics covered include the following:

- an introduction to the basics of TL1 security
- an overview of the administrative functions of the Centralized User Administration (CUA) tool through a TL1 connection
- a brief description of each TL1 enhanced security command, its command syntax, and the response syntax
- instructions on how to enable and disable Security Mode for TL1 using the OS Connection Manager tool

Audience

This document is intended for the following groups:

- provisioners
- network administrators
- transmission standards engineers

References in this document

This document refers to the following document in the AccessNode documentation suite:

Operations, Administration, and Provisioning, Volume 4A

- *System Administration Procedures*, 323-3001-302

TL1 interface basics

Transaction Language 1 (TL1) is a set of generic messages that are exchanged between voice modules and operations systems (OSs) to support network surveillance, provisioning, and line/loop testing functions. TL1 also allows OSs to communicate with different vendor equipment through a common language protocol eliminating the need to support vendor-specific interfaces.

This chapter explains the basics of the TL1 interface.

Chapter contents

This chapter includes the following topics:

TL1 functions

The TL1 implementation on the AccessNode equipment allows the OS to perform the following functions:

- alarm surveillance
- performance monitoring
- tributary provisioning
- line and loop testing
- security administration

The AccessNode system uses the TL1 interface in an AccessNode Operations Controller (OPC) to allow an OS to monitor and control the group of Network Elements (NEs) under the OPC span of control.

TL1 message notation

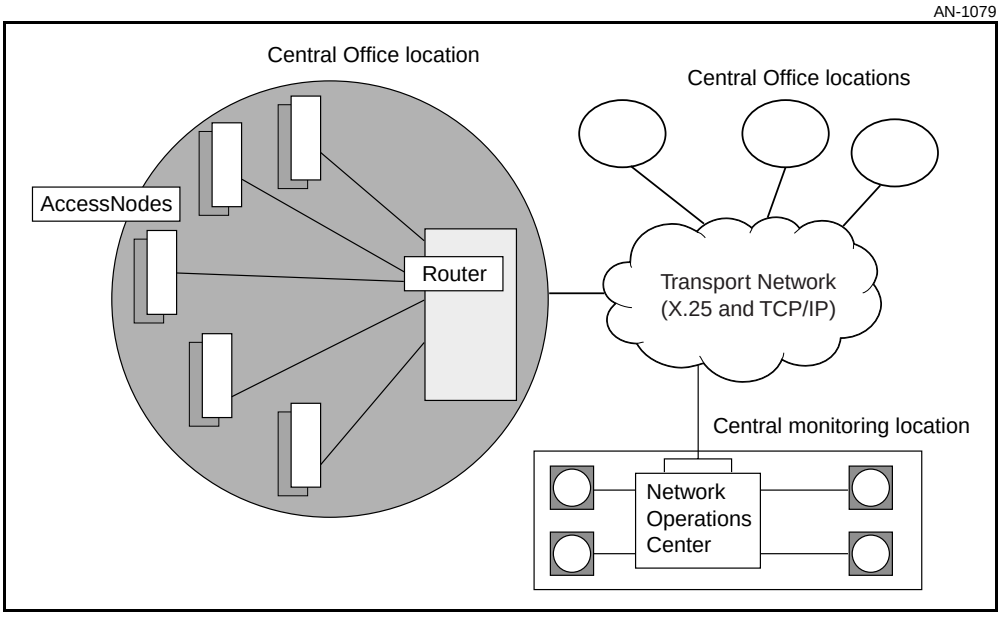
The following notation is used to define the syntax of the TL1 messages.

ASCII carriage return	cr
ASCII line feed	lf
ASCII space	^
designates optional expression	[ ]
variable expression	< >

TL1/OPC interfaces

The OPC, using TL1, acts as an OS gateway, or mediation device, for communication between the AccessNode network elements and external network OSs. The OSs can communicate through the OPC to the NEs using an X.25 connection or an Ethernet LAN. Figure 1-1 shows a typical OS network management configuration.

Figure 1-1
Typical OS network management configuration



Standards compliance

The TL1 interface on the AccessNode equipment complies with the following standards:

Bellcore

- Bellcore NMA OS release 3.4
- TR-NWT-000199 Issue 1, Memory Administration Messages
- TR-NWT-000831 Issue 3, Language for Operations Applications Messages
- TR-NWT-000833 Issue 4: Network Maintenance - Network Element and Transport Surveillance Messages
- TR-NWT-000834 Issue 4: Network Maintenance: Access and Testing Messages
- TR-TSY-000830 Issue 1, Operations Interworking
- SR-OPT-001665 Issue 2

X.25

The X.25 interface complies with the following standards:

- CCITT Recommendation X.25, CCITT Blue Book 1988
- ISO/IEC 8208 X.25 Packet Layer Protocol 1990

Ethernet

The Ethernet interface complies with the following standard:

- Institute of Electronics and Electrical Engineers (IEEE) 802.3

SARTS/TA201:XL

The AccessNode has been tested against the following Switched-Access Remote Test System (SARTS) and TA201:XL releases:

- SARTS Release GI10.0 and TA201:XL Release 7.0; extensive testing
- SARTS Release GI9.1 and TA201:XL Release 6 Version 6.1; brief testing
- SARTS Release GI8.1 and TA201:XL Release 7.0; brief testing
- SARTS Release GI8.1 and TA201:XL Release 6 Version 6.1; extensive testing

DARTS

The AccessNode has also been tested against Digital Analog Remote Test System (DARTS) Release 4.01 produced by Bell Sygma Telecom Solutions.

TL1 feature description

The TL1 interface in an AccessNode operations controller (OPC) provides surveillance and control, provisioning, and testing capabilities between AccessNode network elements (NEs) and a remote operations system (OS). In addition, it provides enhanced security administration.

Surveillance functions include real-time alarm reports, event reports, threshold crossing alerts, logs, and performance statistic reports. Control functions include manual and forced-switch capabilities on both the high-speed optical and low-speed tributary channels.

Provisioning functions include creating, editing, retrieving, and deleting DS0, DS1, DS3, DS0 cross-connect, and equipment objects.

Testing functions provide analog testing support for AccessNode voiceband and voiceband data circuits from external operating systems such as SARTS and DARTS.

Security functions provide the ability to add, edit, delete, and change user access privileges in the Centralized User Administration (CUA) database. See “User administration basics” on page 2-1 for details.

TL1 connectivity

You can configure OPC port 1 (port B) of the NEs equipped with an OPC as a VT100 user interface port or as an X.25 TL1 port. Refer to *System Administration Procedures,* 323-3001-302, in *Operations, Administration, and Provisioning,* Volume 4A, for instructions on the method of configuring the OPC port 1 for X.25 TL1 use.

OPC port 1 cannot be simultaneously used as a VT100 terminal user interface and an X.25 TL1 interface. However, once the port has been configured for TL1, it does not prevent access to the OPC user interface. Access to the OPC user interface can still be achieved through user interface ports 2 or 3, and through the Ethernet port located on the OPC module faceplate. Refer to *System Administration Procedures,* 323-3001-302, in *Operations, Administration, and Provisioning,* Volume 4A, for information on the Port Configuration tool.

Every OPC module contains an Ethernet 802.3 LAN port on the faceplate of the OPC. The Ethernet port on the OPC provides an interface for a third-party X11 terminal or workstation, providing an enhanced graphics interface to the OPC. The connector is a shielded RJ-45 connector. The data rate supported is 10 Mbit/s, with a distance limitation of 100 m.

Loss of communication

The time period for valid link failure or loss of communications detection is 3 minutes for surveillance and provisioning, and 1.25 minutes for line and loop testing.

Simultaneous sessions

The following limitations apply to TL1 sessions:

- You cannot run more than four concurrent TL1 sessions on an OPC. This limitation includes both surveillance and provisioning sessions and applies to both X.25 and TCP/IP sessions.
- You can run four surveillance sessions at the same time.
- You cannot run more than one provisioning session at a time.
- If four TL1 sessions are active, a maximum of two OPC user interface sessions can run at the same time. Table 1-1 on page 1-6 shows the correlation between the number of concurrent TL1 and OPC sessions.

  Note: The limitations do not apply to testing (SARTS/DARTS) sessions, nor do active testing sessions contribute to the combined total of OPS/NMA sessions.

Table 1-1
Concurrent TL1 and OPC sessions

Number of TL1 sessions	Maximum OPC user interface sessions
0 or 1	4
2 or 3	3
4	2
Note: Only one of the four TL1 sessions can be a provisioning (OPS) session.	

TL1 security

The OS provisioning and surveillance TL1 interfaces can run with security mode enabled or disabled:

- Security mode enabled—requires using the ACT-USER command to log in before other commands are accepted
- Security mode disabled—commands are accepted without using the ACT-USER command to log in (with the exception of the Security Administration commands)

These security modes are set from the OS Connection Manager (SLAT toolset) on the OPC. For instructions on setting the security modes, see “Use this procedure to enable and disable security mode.” on page 4-4.

Note 1: Only the root user can set the security mode. Other users can see the mode setting but will be unable to change it.

Note 2: Security mode affects the operation of provision and surveillance OS interfaces only. It does not affect testing OS interfaces or the operation of any of the user interfaces.

Security mode restrictions

Security mode operation applies only to the provisioning and the surveillance OS interfaces. The line test interface (SARTS/DARTS) is not affected by the security mode setting—it always operates with security mode disabled.

The security mode feature of the OS Connection Manager is not available through the OPCGUI software that runs on a PC. The radio buttons that are used to set the security mode are available only through the OPC user interface (character-mode or graphical-mode) from the OPC Desktop.

The security mode applies not only to X.25 connections but to any tool that uses the provisioning and surveillance OS interfaces, such as the tl1shell user interface as well as TL1 over TCP/IP, where provided.

Note: The tl1shell user interface should not be confused with the tl1ci tool. The tl1ci tool is a different interface which is used for AccessNode Express only. tl1ci always requires the use of the ACT-USER TL1 command to log in before accepting TL1 requests.

You can perform security administration tasks using TL1 commands or through the Centralized User Administration (CUA) user interface. Some tasks must be performed through the CUA user interface because those tasks are not supported in TL1.

Refer to “Guide to Centralized User Administration procedures” on page 2-2 of this book for a list of the appropriate sections in the *System Administration Procedures,* 323-3001-302, in *Operations, Administration, and Provisioning*, Volume 4A.

OS interface actions

When security mode is enabled, the provisioning and surveillance OS interfaces operate as follows:

- A valid X.25 connection triggers the appropriate OS interface.
- A tl1shell session is started with a connection to the OS interface specified on the tl1shell command line.
- The OS interface starts up and the connection remains up until the X.25 connection is dropped or the tl1shell session is closed.
- The OS interface rejects all commands until an ACT-USER command with a valid user name and password is received and processed.
- Once a valid ACT-USER command is received and processed, the user's access privileges for the target NE are compared against the TL1 request to determine whether the TL1 request meets the user's access privileges.

  Note: Users may be able to log in with the ACT-USER command yet be unable to perform any further commands because of their user access privilege setting.

- TL1 requests that meet the user's access privileges (such as a RTRV-T1 TL1 request when the user has read privileges for the target NE), are processed.
- TL1 requests that do not meet the user's access privileges (such as an ED-T1 TL1 request when the user has only read privileges for the target NE) are denied.

- Only users with Read/Write/Admin (RWA) user access privileges can use the ED-USER-SECU TL1 command. Any resulting changes generate event logs in the Event Browser user interface.
- Only the root user and users who are members of the admin group with Read/Write/Admin (RWA) user access privileges can use the ENT-USER-SECU and DLT-USER-SECU commands. Any resulting changes generate event logs in the Event Browser user interface.

With security mode disabled, only the root user and users who are members of the admin group can use any of the security administration TL1 commands (ENT-USER-SECU, ED-USER-SECU, DLT-USER-SECU, ACT-USER, and CANC-USER). Any other user will receive a DENY, regardless of their user privileges. Any user can issue any of the other TL1 commands appropriate to the OS interface (provisioning or surveillance) to which they are connected without using ACT-USER to log in. The ACT-USER command is required only for security administration when security mode is disabled.

When the provisioning and surveillance OS interface starts up, it logs the security mode detected in the system log file.

Upgrading your AccessNode software

When upgrading from a release of the AccessNode software that did not contain the OS security feature to a release that does contain the OS security feature, the security mode is disabled automatically to preserve backward compatibility. The root user must invoke the OS Connection Manager and change the security mode if enabled security mode is desired.

New installations will also default to security mode disabled and require the root user to enable security mode if that is desired.

The security mode is also saved during an OPC save/restore as well as with a backup OPC database synchronization. Upgrades from an AccessNode software release that supports TL1 security to a later release that also supports TL1 security will retain the security mode setting with the upgrade. That is, a system upgraded with security mode enabled will have the security mode set to Enabled after the upgrade is complete.

Figure 1-2 shows examples of TL1 security commands and responses.

Figure 1-2
TL1 security command examples

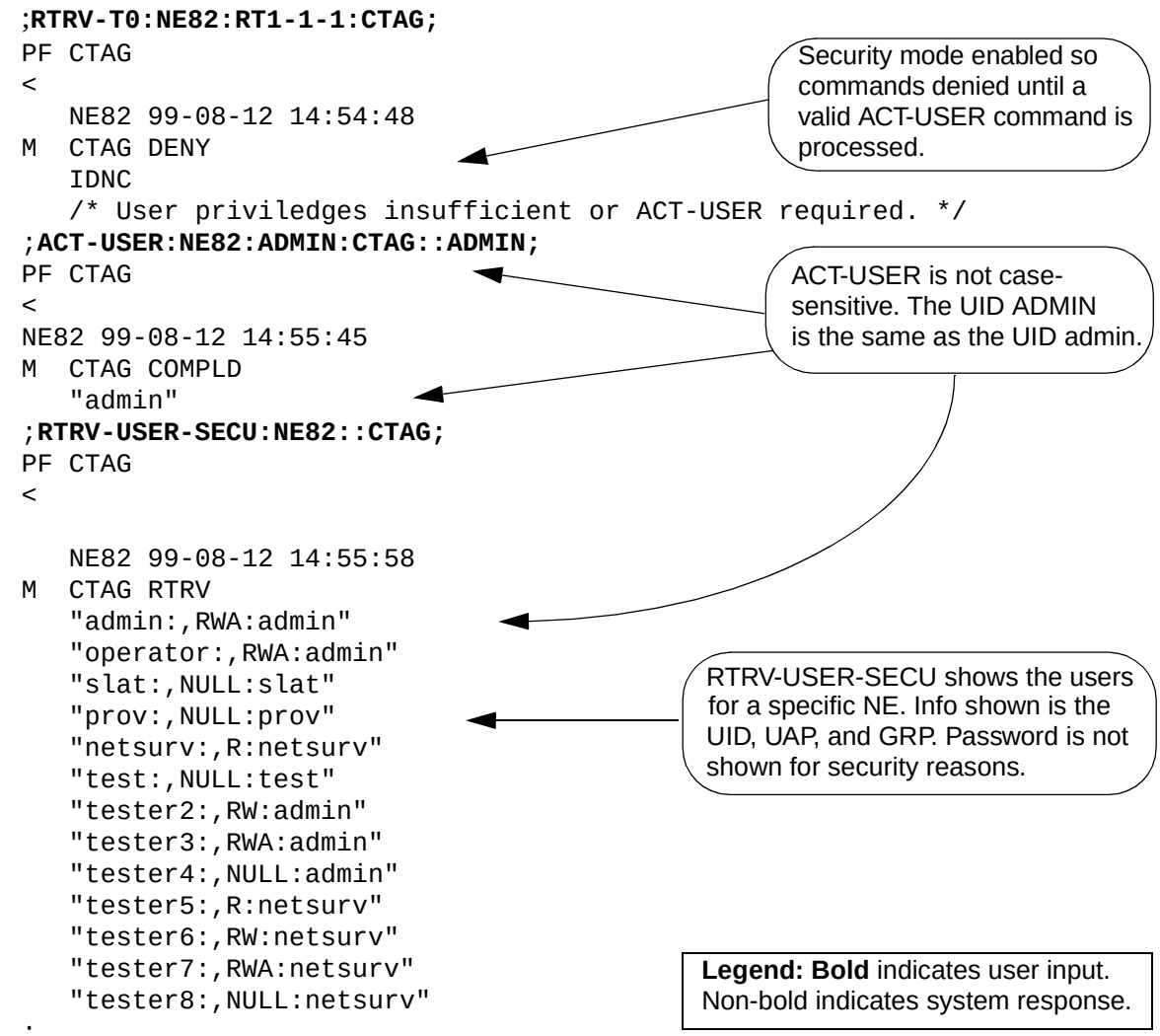
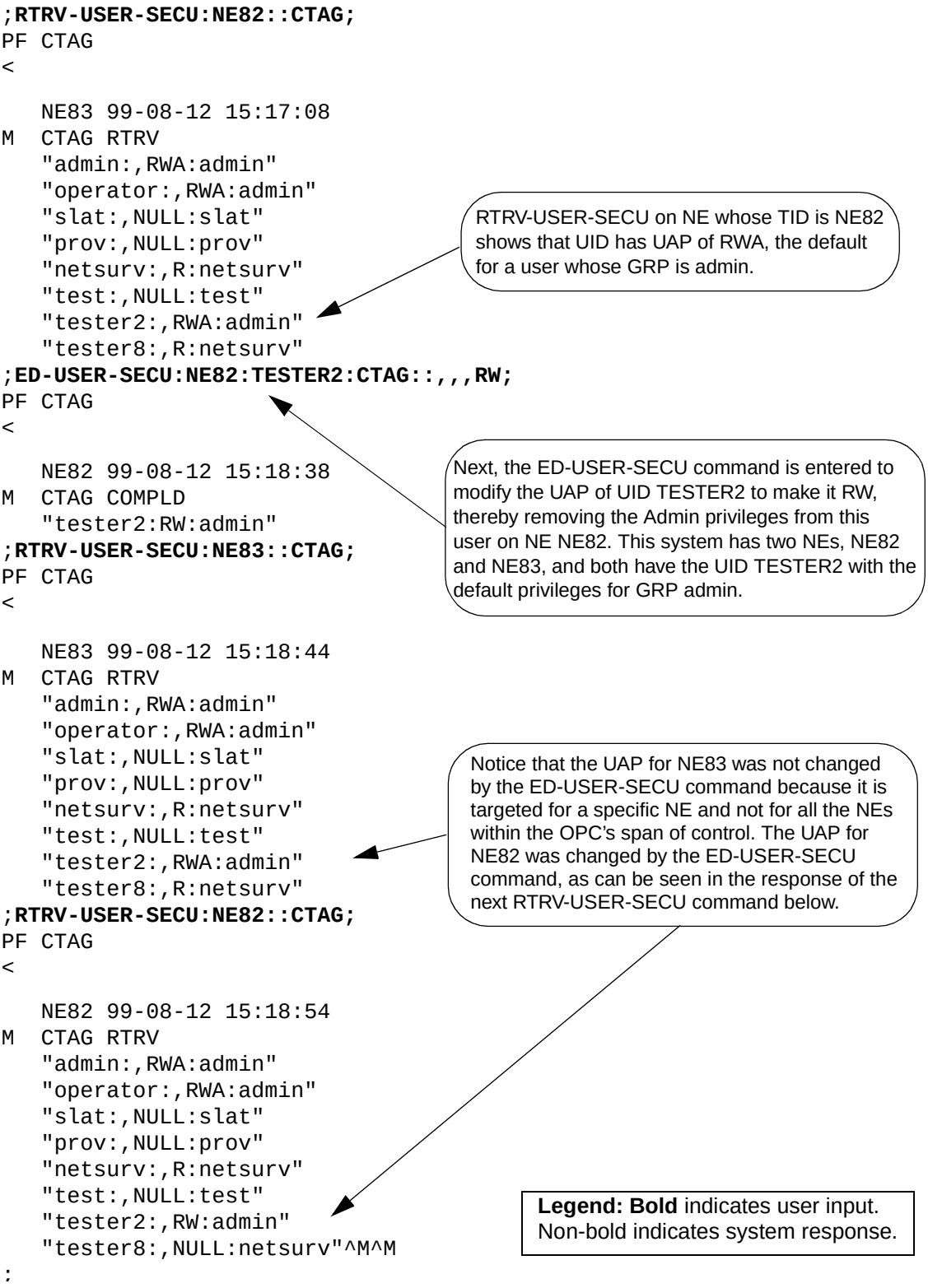


Figure 1-3 shows examples of TL1 user-modification commands.

Figure 1-3
TL1 user-modification command examples



TL1 messages

This section describes the TL1 message types, the common elements present in all TL1 messages, and the OPC response to TL1 non-autonomous requests.

TL1 message types

There are two types of TL1 messages: autonomous and non-autonomous. Autonomous messages are generated by the OPC as a result of activity on the NEs (such as alarms, protection switch activity, threshold alert, and warnings) and reported to the OS automatically. Autonomous messages are generated by the surveillance message set only (with the exception of one autonomous message provided by the line and loop testing interface).

Non-autonomous messages consist of a request from the OS and a response message from the OPC, and are generated by all message sets.

TL1 response header

The first two lines of all TL1 message responses have a common format. The first line always contains the target identifier (TID), which is the NE name, the date, and the time the TL1 response was sent to the OS. An example of the first line follows:

TID	Date and time of message	
FCOT1	92-08-13 13:39:32	1st line (NE name)

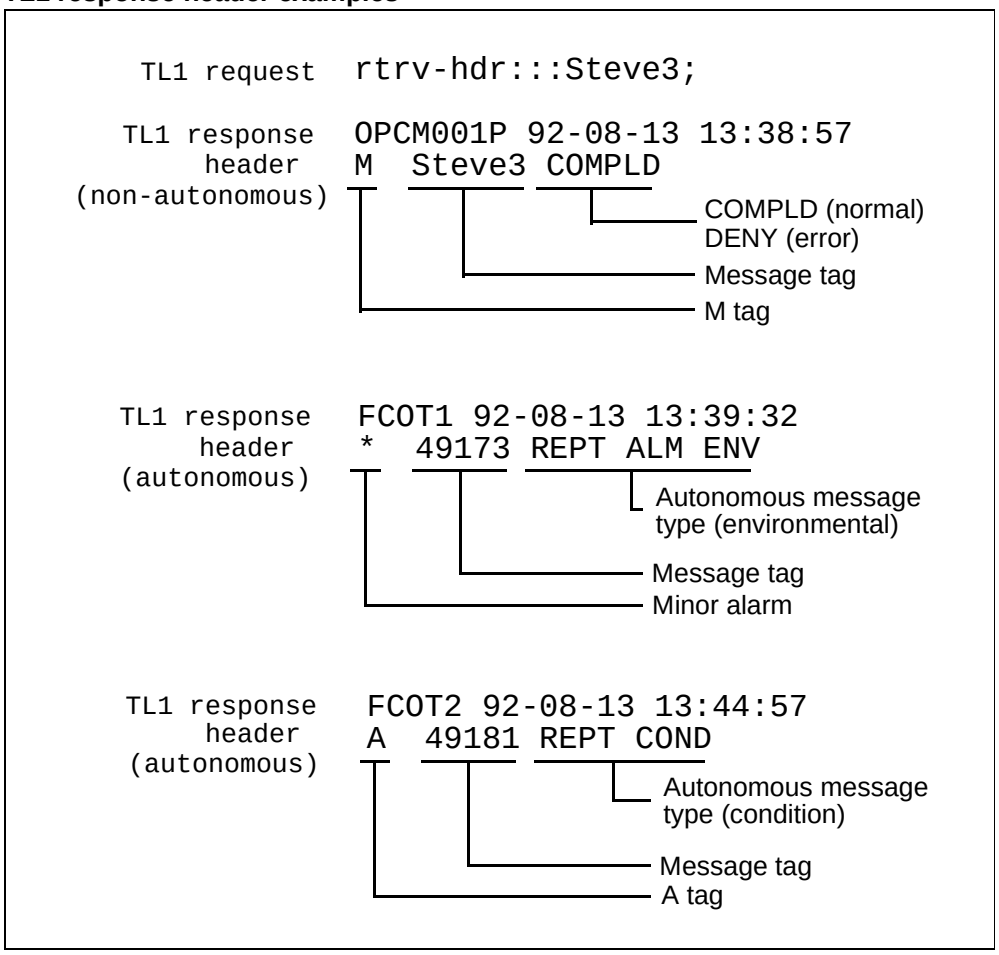
For non-autonomous messages, the second line always begins with an **M** tag followed by either COMPLD to indicate a normal response, or DENY to indicate an error response.

The second line of autonomous messages also contains a numerical message tag, which is automatically generated, and the TL1 message type. (The numerical message tag is the same correlation tag as the TL1 request for non-autonomous responses.)

The second line of TL1 messages is different for autonomous and non-autonomous messages. For autonomous messages, the second line in most messages begin with an **A** tag. Exceptions to this are the alarm messages which begin with an alarm code (which is an asterisk in one of the following examples).

Figure 1-4 presents three examples of TL1 response headers.

Figure 1-4
TL1 response header examples



TL1 case sensitivity

In line and loop testing messages, all TL1 parameter fields are case sensitive. In surveillance and provisioning, only some fields are case sensitive. The only TL1 parameter that is not case sensitive is the Second Command Code Modifier (SCCM) used in surveillance messages. Some TL1 message types, for instance RTRV-HDR, are not case sensitive.

For example:

```
rtrv-alm-com:FCOT1::Ctag12::MN,CONTCOM,NSA;
```

and

```
RTRV-ALM-COM:FCOT1::Ctag12::MN,CONTCOM,NSA;
```

are both valid TL1 non-autonomous messages. However,

```
rtrv-alm-com:FCOT1::Ctag12::MN,contcom,NSA;
```

is not a valid TL1 message.

TL1 acknowledgment messages

When a TL1 non-autonomous message is issued to the OPC, an acknowledgment message is sent back to the OS before the actual TL1 response. This acknowledgment indicates that the TL1 request has actually been received by the OPC. The four possible TL1 acknowledgment messages are listed in the following table.

Acknowledgment	Indicates that
PF	the TL1 request has been received and a print out (response) follows
NA	although the TL1 request was received, no TL1 response will be sent back because the OS interface was not initialized when the command was received. The command should be retried after waiting approximately 15 seconds. If an NA is returned after three tries, the OPC may be inactive.
RL	the TL1 request cannot be handled and to retry later (applicable to provisioning only)
OK	the data link between the OPC and OS is working properly (applicable to line and loop testing only)

Acknowledgment request format

The format of the acknowledgment request is as follows:

PF cr lf
<

For provisioning and line and loop testing, the “PF” and “NA” messages are followed by a correlation tag (CTAG) associated to the issued command.

Target identifier TL1 parameter

In non-autonomous TL1 messages, the target identifier (TID) specifies the network element for which a message is intended. It is equivalent to the source identifier (SID) in autonomous TL1 messages. Both the TID and the SID have the same possible values: a defined name, the network element name, or the network element identification number (network element ID).

- Defined name. You can define a name of up to 20 characters for the TID alias. For the testing interface, you assign the name through the OS Connection Manager at the OPC. For the non-testing interfaces, you define the name through tidmap, an OPC Session Manager UNIX command. See *System Administration Procedures*, 323-3001-302, in *Operations, Administration, and Provisioning*, Volume 4A, for directions.

Note: When you define the name, you must manually synchronize it between the primary operations controller (OPC) and the backup OPC. See *System Administration Procedures*, 323-3001-302, in *Operations, Administration, and Provisioning,* Volume 4A, for information on the Commissioning Mngr tool.

- Network element name. If you do not define a name for a non-testing interface, the OPC assigns the network element name as the TID alias when you bring up the interface for the first time. If you do not define a name for a testing interface, the network element name is not assigned as the TID alias. You can, however, use the network element name as the TID.

  Note 1: The network element name must meet the TL1 requirement of containing only letters, digits, hyphens (-), underscores (_), and periods. Spaces (blanks) are invalid. For example, `SHELF 1` is invalid, but `SHELF_1` is valid.

  Note 2: Because Switched-Access Remote Test System (SARTS) does not accept TIDs longer than 10 characters, you must define a TID name if the network element name exceeds 10 characters.

  Note 3: If you change the network element name, the TID alias does not change.

- Network element ID. If the network element does not have a name or if the name contains invalid TL1 characters, the OPC assigns the network element ID as the TID alias.

Table 1-2 summarizes the order of each identifier for non-testing interfaces.

Table 1-2
TL1 network element identification

TID value	Non-testing interfaces
defined name	TID
network element name	default for TL1 TID if the TID is not defined
network element ID	default for TL1 TID if the TID is not defined and the network element name is undefined or invalid

Each network element has only one TID. The OPC does not have a TID.

User administration basics

This chapter provides an overview of the administrative functions of the Centralized User Administration (CUA) tool through a TL1 connection. The admin user group tool set on the active OPC contains the CUA tool.

Chapter contents

This chapter includes the following topics:

Guide to Centralized User Administration procedures

For information on performing other administrative functions using the Centralized User Administration (CUA) tool, refer to the following sections in the *System Administration Procedures*, 323-3001-302, in *Operations, Administration, and Provisioning,* Volume 4A.

Procedure		See	Available using TL1?
4-1	Creating a new user account	page 4-9	Yes
4-2	Creating a new user account by duplicating the current attributes of an existing user	page 4-15	
4-3	Changing an existing user account	page 4-23	Partial (UAP only)
4-4	Deleting a user account	page 4-30	Yes
4-5	Changing user account passwords	page 4-35	Yes
4-6	Enabling or disabling user accounts	page 4-39	Yes
4-7	Creating a new user group	page 4-44	
4-8	Deleting a user group	page 4-51	
4-9	Changing user group attributes	page 4-55	
4-10	Creating a new toolset	page 4-61	
4-11	Changing an existing toolset	page 4-66	
4-12	Deleting a toolset	page 4-71	
4-13	Creating auto-start tools for user groups	page 4-74	
4-14	Managing system parameters	page 4-79	
4-15	Moving users between user groups	page 4-85	Yes
4-16	Sorting the users list	page 4-88	
4-17	Filtering the users list	page 4-91	
4-18	Auditing user profile data	page 4-95	
4-19	Scheduling a user profile audit	page 4-99	
4-20	Transferring user profile data to the backup OPC	page 4-103	
4-21	Listing all authorized userIDs on the NE	page 4-105	Yes

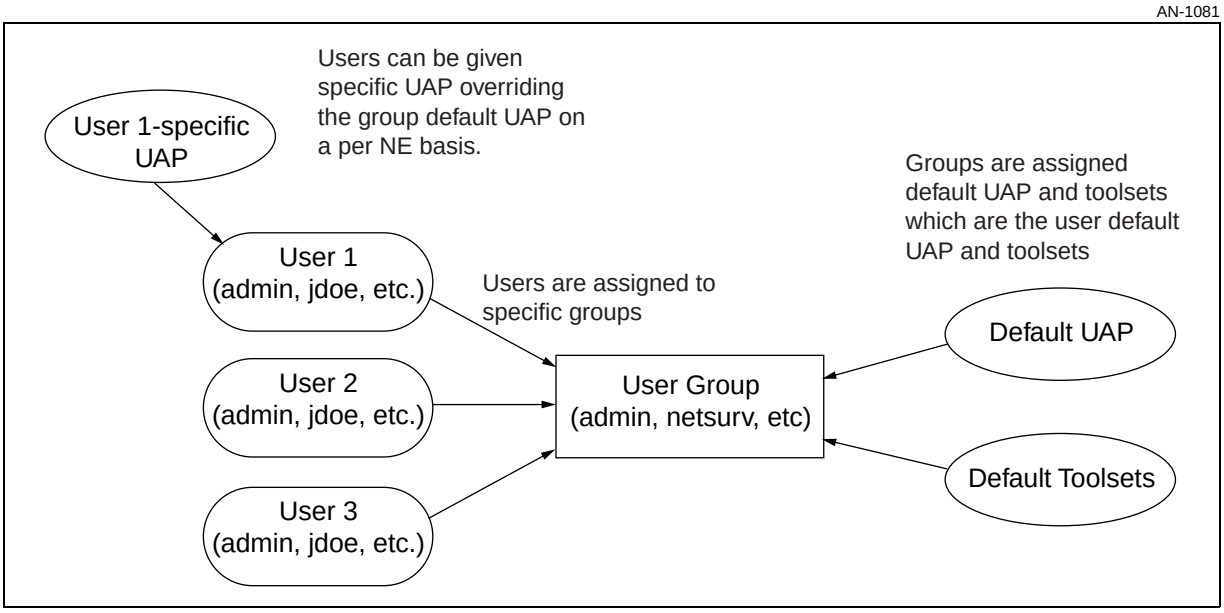
—continued—

Procedure		See	Available using TL1?
4-22	Listing all users logged in to the NE	page 4-107	
4-23	Listing all users logged in to the NE and the device	page 4-109	
4-24	Displaying the userID logged in at a terminal	page 4-110	
4-25	Logging out another userID	page 4-112	
—end—			

Using TL1 to administer OPC user accounts

User accounts belong to user groups. These groups can be default user groups in the CUA tool, or they can be other user groups that were created through the CUA tool. Each user group has access to various toolsets. Figure 2-1 illustrates these concepts.

Figure 2-1
User/group access privilege assignments

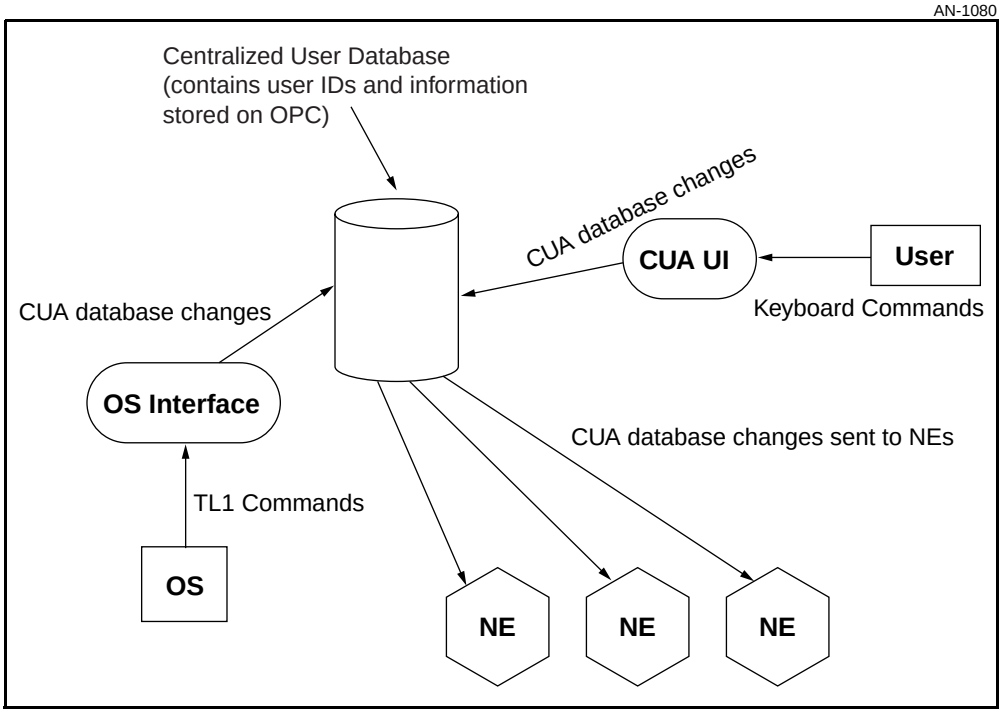


The CUA tool lets you do the following:

- create and manage user accounts and user groups through the OPC user interface
- control network element access privileges, userIDs, and user passwords that access that OPC user interface
- define user accounts that have read, write, and administrative privileges for the network elements in the OPC span of control
- assign OPC UI toolsets to specific groups and users

Figure 2-2 shows the interaction of the OS interface and the CUA when TL1 commands are issued.

Figure 2-2
Interaction of OS interface and CUA



Note: When you create or change a user's password using the CUA tool, you must use lowercase alphanumeric characters. The OS interface always converts the UID, PID, and GRP to lowercase before matching them against the CUA database.

Table 2-1 shows the maximum number of CUA tool accounts available.

Table 2-1
Maximum number of CUA tool user accounts

User account allocation	Maximum number of accounts
user accounts for a network element	32
user accounts in a user group	100
user accounts for all network elements in a span of control	200

Users in the admin and root user groups can perform user administration functions through TL1 as well as through the CUA tool.

> ***Note:*** The CUA tool cannot be open and in use when TL1 commands that modify users are being issued. These commands are: ENT-USER-SECU, ED-USER-SECU, and DLT-USER-SECU. If the CUA tool is open when these commands are being sent to the OS interface, the TL1 command is denied.

A user profile, as defined in the CUA tool, is made up of several parameters. Each user belongs to a user group. The user has Read, Read/Write, Read/Write/Admin, or no access privileges for the network elements in its span of control. In the TL1 syntax:

- uap denotes network element privileges (or user access privileges)
- grp denotes the user group
- uid denotes the user identifier
- pid denotes the user password (or password identifier)

In order for the first TL1 administrator to open a TL1 administration session, that user must belong to an existing admin user account or must be the root user. After that, additional TL1 administrators can be added, modified, and deleted through either the TL1 interface or through the CUA tool.

Table 2-2
CUA accessibility and access classes mapped to TL1 user access privileges (UAP)

NE accessibility	NE access class	UAP
Yes	Read	R
Yes	Read/Write	RW
Yes	Read/Write/Admin	RWA
—continued—		

Table 2-2 (continued)
CUA accessibility and access classes mapped to TL1 user access privileges (UAP)

NE accessibility	NE access class	UAP
No	Read	Null
No	Read/Write	Null
No	Read/Write/Admin	Null
—end—		

Table 2-3 shows which TL1 commands are valid for each group with various user access privileges assigned.

Table 2-3
Valid TL1 commands for various UAP assignments with security mode enabled

Group (default UAP)	Access Privilege (UAP)	OPC Login	NE Login	RTRV-USER-SECU ED-USER-SECU (NE target)	ENT-USER-SECU DLT-USER-SECU (OPC target)	RTRV-	Other
Admin (RWA)	Read (R)	Y	Y	N	N	Y	N
	Read/Write (RW)	Y	Y	N	N	Y	Y
	Read/Write Admin (RWA)	Y	Y	Y	Y	Y	Y
	NULL (No access)	Y	N	N	N	N	N
Netsurv (R)	Read (R)	Y	Y	N	N	Y	N
	Read/Write (RW)	Y	Y	N	N	Y	Y
	Read/Write Admin (RWA)	Y	Y	Y	N	Y	Y
	NULL (No access)	Y	N	N	N	N	N
—continued—							

Table 2-3 (continued)
Valid TL1 commands for various UAP assignments with security mode enabled

Group (default UAP)	Access Privilege (UAP)	OPC Login	NE Login	RTRV-USER-SECU ED-USER-SECU (NE target)	ENT-USER-SECU DLT-USER-SECU (OPC target)	RTRV-	Other
Test (NULL)	Read (R)	Y	Y	N	N	Y	N
	Read/Write (RW)	Y	Y	N	N	Y	Y
	Read/Write Admin (RWA)	Y	Y	Y	N	Y	Y
	NULL (No access)	Y	N	N	N	N	N
Prov (NULL)	Read (R)	Y	Y	N	N	Y	N
	Read/Write (RW)	Y	Y	N	N	Y	Y
	Read/Write Admin (RWA)	Y	Y	Y	N	Y	Y
	NULL (No access)	Y	N	N	N	N	N
SLAT (NULL)	Read (R)	Y	Y	N	N	Y	N
	Read/Write (RW)	Y	Y	N	N	Y	Y
	Read/Write Admin (RWA)	Y	Y	Y	N	Y	Y
	NULL (No access)	Y	N	N	N	N	N
—end—							

TL1 Security administration commands

Chapter contents

This chapter includes the following topics:

ACT-USER

Use the Activate User (ACT-USER) command to identify yourself to the OS interface when:

- security mode is enabled and you want to use any TL1 command, or
- security mode is disabled and you want to use the security administration commands to create, modify, or delete users or user access privileges

You can open a TL1 session using ACT-USER from either the surveillance or provisioning TL1 interfaces. The UID specified in the ACT-USER command identifies you to the system. See "User administration basics" on page 2-1 for information on user identifiers, user access privileges, and groups when the security mode is enabled.

The security mode is set from the OS Connection Manager (SLAT toolset) on the OPC. For instructions on setting the security mode, see "Use this procedure to enable and disable security mode." on page 4-4.

Note 1: Only the root user can set the security mode. Other users can see the mode setting but will be unable to change it.

Note 2: When you create or change a user's password using the CUA tool, you must use lowercase alphanumeric characters. The OS interface always converts the UID, PID, and GRP to lowercase before matching against the CUA database.

Before you enter this command, do the following:

- obtain a user identifier (uid) that belongs to the appropriate user groups
- obtain a user password (pid). Passwords have the following restrictions:
  - — passwords must be exactly eight characters. Valid characters are a to z, 0 to 9, $, and _ (underscore).
  - — the first character must be alphabetic
  - — passwords must not contain the associated userID
  - — passwords must contain at least one of the following: a numeric character, $, or _ (underscore)
  - — passwords assigned by the system administrator have an associated accreditation period
  - — passwords are not case-sensitive and are always forced to lower case before being verified

Input syntax

```
ACT-USER:[TID]:<UID>:<CTAG>::<PID>;CRLF
```

Table 3-1
ACT-USER command syntax descriptions

Field	Description
TID	Target identifier (optional). TID specifies the network element to which the command is directed. If the TID is specified, it must be a valid identifier in the OPC span of control.
UID	User identifier of a user. When security mode is disabled, the user must be in either the admin or root user group.
CTAG	Correlation tag, an alphanumeric identifier to correlate the command and response messages.
PID	Password for the user.

Example

To activate the user account ADMIN on network element STREETER, type:

```
ACT-USER:STREETER:ADMIN:IL123::SESAME;
```

Response syntax

The following sections show the syntax for a normal response and an error response.

Normal response

The following syntax is the normal response to the ACT-USER command:

```
crlf
lf
^^^<sid>^<date>^<time> crlf
M^^<ctag>^COMPLD crlf
^^^"<uid>" crlf
;
```

Table 3-2
ACT-USER response syntax descriptions

Field	Description
sid	Source identifier
date	TL1 message origination date
time	TL1 message origination time
ctag	Correlation tag
uid	User identifier

Error response

The following syntax is the error response to the ACT-USER command:

```
crlf
lf
^^^<sid>^<date>^<time> crlf
M^^<ctag>^DENY crlf
^^^"<uid>" crlf
;
```

CANC-USER

Use the Cancel User (CANC-USER) command to cancel or clear the current ACT-USER session. The CANC-USER command is only used to cancel the current ACT-USER session. It cannot be used to cancel another user's session.

> ***Note:*** The CANC-USER command will log out the current session whether or not a UID is entered. The connection will stay up and will not be dropped by the NE.

Input syntax

```
CANC-USER:[TID]:[UID]:<CTAG>;CRLF
```

Table 3-3
CANC-USER command syntax descriptions

Field	Description
TID	Target identifier (optional). TID specifies the network element to which the command is directed. If the TID is specified, it must be a valid identifier in the OPC span of control.
UID	User identifier (optional). If the UID is specified, it must specify the current user. If the UID is not specified, the current user is assumed.
CTAG	Correlation tag, an alphanumeric identifier to correlate the command and response messages.

Example input

To log out user TYLER from the network element KNOXVILLE, type:

```
CANC-USER:KNOXVILLE:TYLER:TN777;
```

Response syntax

The following sections show the syntax for a normal response and an error response.

Normal response

The following syntax is the normal response to the CANC-USER command:

```
crlf
lf
^^^<sid>^<date>^<time> crlf
M^^<ctag>^COMPLD crlf
^^^"<uid>" crlf
```

Table 3-4
CANC-USER response syntax descriptions

Field	Description
sid	Source identifier
date	TL1 message origination date
time	TL1 message origination time
ctag	Correlation tag
uid	User identifier

Error response

The following syntax is the error response to the CANC-USER command:

```
crlf
lf
^^^<sid>^<date>^<time> crlf
M^^<ctag>^DENY crlf
^^^"<uid>" crlf
```

DLT-USER-SECU

Use the Delete User Security (DLT-USER-SECU) command to delete a user account from the Centralized User Administration (CUA) tool.

Note 1: Whether security mode is enabled or disabled, only users of group admin or root with RWA access privileges can execute this command.

Note 2: You cannot modify user accounts if an operations controller (OPC) CUA session is in progress. If you try to do so, the response will be a DENY.

OPC users

When you delete a user account being used for an operations controller (OPC) session, be aware of the following consequences:

- The current OPC session is not disturbed.
- The user cannot log in again after logging out.

NE users

When you delete a user account being used for a network element (NE) session, be aware of the following consequences:

- The current NE session is not disturbed.
- The user's password immediately expires.
- The user account is deleted from the OPC.
- The user cannot log in to the NE again.
- The user cannot log in to the OPC to change the password.
- The user account is deleted from the NE when the Centralized User Administration audit is performed.

Input syntax

```
DLT-USER-SECU:[TID]:<UID>:<CTAG>;CRLF
```

Table 3-5
DLT-USER-SECU command syntax descriptions

Field	Description
TID	Target identifier (optional). If you specify the TID, it must be a valid identifier in the OPC span of control. The TID has no significance when used with this command.
UID	User identifier (account name) of the user to be deleted.
CTAG	Numeric identifier (correlation tag) to associate the command to the response message

Example input

To delete the user account MIKE, type:

```
DLT-USER-SECU:CALABOGIE:MIKE:123;
```

Response syntax

The following sections show the syntax for a normal response and an error response.

Normal response

The following syntax is the normal response to the DLT-USER-SECU command:

```
crlf
lf
^^^<sid>^<date>^<time> crlf
M^^<ctag>^<COMPLD crlf
;
```

Table 3-6
DLT-USER-SECU response syntax descriptions

Field	Description
sid	Source identifier
date	TL1 message origination date
time	TL1 message origination time
ctag	Correlation tag

Error response

The following syntax is the error response to the DLT-USER-SECU command:

```
crlf
lf
^^^<sid>^<date>^<time> crlf
M^^<ctag>^<DENY crlf
;
```

ED-USER-SECU

Use the Edit User Security (ED-USER-SECU) command to edit the security parameters for a Centralized User Administration (CUA) tool user account. You can change the following parameters:

- user id (uid)
- group (grp)
- password (pid)
- user access privilege (uap), for each network element in the span of control

Enter only the data parameters that you want to change.

Note 1: When security mode is enabled, any user with RWA access privileges can execute this command. When security mode is disabled, only users of group admin or root can execute this command.

Note 2: You cannot modify user accounts if an operations controller (OPC) CUA session is in progress. If you try to do so, the response will be a DENY.

If you disable a user's access to a network element (NE) and the user account is being used for an NE session, be aware of the following consequences:

- The account is deleted from the NE but not from the CUA database on the OPC.
- The current NE session is not disturbed.
- The user's password immediately expires.
- The user cannot log in to the NE again.
- The user account is deleted from the NE when the Centralized User Administration audit is performed, but remains in the CUA database on the OPC.
- When security mode is enabled, the user can log in using the ACT-USER command but is unable to execute any command other than CANC-USER.

Note: Refer to Figure 1-3 on page 1-10 for an example of the ED-USER-SECU command.

Input syntax

```
ED-USER-SECU:<TID>:<UID>:<CTAG>:[NGRP]:,[NPID],,[NUAP];CRLF
```

Note: When you create or change a user's password using the CUA tool, you must use lowercase alphanumeric characters. The OS interface always converts the UID, PID, and GRP to lowercase before matching against the CUA database.

Table 3-7
ED-USER-SECU command syntax descriptions

Field	Description
TID	Target identifier of the network element where you want to change the user's security parameters.
UID	User identifier for the user that you want to change.
CTAG	Correlation tag.
NGRP	New group for this user. This parameter is optional. If you specify a group, it must exist in the CUA (for example, ADMIN).
NPID	New password for this user. This parameter is optional.
NUAP	New user access privilege for this user. This parameter is optional. The options are: **R** read access only **RW** read/write access only **RWA** read/write/admin access **NULL** no access

Example input

To modify the UAP of UID tester2 at NE82 to be RW, type the following command:

```
ED-USER-SECU:NE82:TESTER2:CTAG::,,,RW;
```

Response syntax

The following sections show the syntax for a normal response and an error response.

Normal response

The following syntax is the normal response to the ED-USER-SECU command:

```
crlf
lf
^^^<sid>^<date>^<time> crlf
M^^<ctag>^COMPLD crlf
^^^<uid>:<uap>:<grp>" crlf
;
```

Table 3-8
ED-USER-SECU response syntax descriptions

Field	Description
sid	Source identifier
date	TL1 message origination date
time	TL1 message origination time
ctag	Correlation tag
uid	User identifier
uap	User access privilege for the listed user account
grp	User group that contains the listed user account

Error response

The following syntax is the error response to the ED-USER-SECU command:

```
crlf
lf
^^^<sid>^<date>^<time> crlf
M^^<ctag>^DENY crlf
^^^<uid>:<uap>:<grp>" crlf
;
```

ENT-USER-SECU

Use the Enter User Security (ENT-USER-SECU) command to add a user account to the Centralized User Administration (CUA) tool. You need to specify the following parameters:

- user id (uid)
- group (grp)
- password (pid)
- user access privileges (uap) for each network element in the span of control

You cannot use TL1 to add a user account if an operations controller (OPC) CUA session is in progress.

Note 1: Whether security mode is enabled or disabled, only users of group admin or root with RWA access privileges can execute this command.

Note 2: You cannot modify user accounts if an operations controller (OPC) CUA session is in progress. If you try to do so, the response will be a DENY.

Note 3: The user account created will be propagated to all NEs within the OPC's span of control. To customize the user's account privileges for each NE, use the ED-USER-SECU command.

Before you start this procedure, you must

- establish an active TL1 administration session
- obtain the user id (uid) of the new user account
- obtain the user group (grp) to contain the new user account
- obtain the user access privileges (uap) for the new user account
- obtain the password (pid) for the new user account. Passwords must be exactly eight characters. Valid characters are a to z, 0 to 9, $, and _ (underscore).
  - — the first character must be alphabetic
  - — passwords must not contain the associated userID
  - — passwords must contain at least one of the following: a numeric character, $, or _ (underscore)
  - — passwords assigned by the system administrator have an associated accreditation period

Note: The uid, grp, and pid parameters are always forced to lower case before being verified.

Input syntax

```
ENT-USER-SECU:[TID]:<UID>:<CTAG>:<GRP>:<PID>,,<UAP>;CRLF
```

Table 3-9
ENT-USER-SECU command syntax descriptions

Field	Description
TID	Target identifier (optional). If you specify a TID, it must be a valid identifier in the OPC span of control. The TID has no significance when used with this command.
UID	User identifier for the user to be added. This user identifier must be unique to the CUA.
CTAG	Correlation tag
GRP	Group to contain the added user. This value must be a valid group in the CUA (such as ADMIN or SLAT).
PID	Password for the new user account.
UAP	User access privilege for the new user account. The options are: **R** read access only **RW** read/write access only **RWA** read/write/admin access **NULL** no access TL1 applies these privileges to each network element in the span of control as a default. Use the ED-USER-SECU command to make NE-specific changes.

Example input

To create a user account called SIMPSONC, with a password of FORTY234, and user access privilege of RWA, type:

```
ENT-USER-SECU:TOLEDO:SIMPSONC:T456::FORTY234,,RWA;
```

Response syntax

The following sections show the syntax for a normal response and an error response.

Normal response

The following syntax is the normal response to the ENT-USER-SECU command:

```
crlf
lf
^^^<sid>^<date>^<time crlf
M^^<ctag>^COMPLD crlf
^^^"<uid>:<pid>:<uap>" crlf
;
```

Table 3-10
ENT-USER-SECU response syntax descriptions

Field	Description
sid	Source identifier
date	TL1 message origination date
time	TL1 message origination time
ctag	Correlation tag
uid	User identifier
pid	Password for the new user account
uap	User access privilege for the listed user account. The options are: **R** read access only **RW** read/write access only **RWA** read/write/admin access **NULL** no access

Error response

The following syntax is the error response to the ENT-USER-SECU command:

```
crlf
lf
^^^<sid>^<date>^<time crlf
M^^<ctag>^DENY crlf
^^^"<uid>:<pid>:<uap>" crlf
;
```

RTRV-USER-SECU

Use the Retrieve User Security (RTRV-USER-SECU) command to retrieve the security parameters for a user account. You cannot retrieve a user's password.

If you issue a request to retrieve all users for a specified network element, the TL1 response lists both active and expired accounts.

Note 1: When security mode is enabled, any user with RWA access privileges can execute this command. When security mode is disabled, only users of group admin or root can execute this command.

Note 2: The response to this command is NE-specific.

Input syntax

```
RTRV-USER-SECU:<TID>:[UID]:<CTAG>;CRLF
```

Table 3-11
RTRV-USER-SECU command syntax descriptions

Field	Description
TID	Target identifier (required). The TL1 response includes user access privileges for the target identifier.
UID	User identifier (optional). If you specify the UID, the TL1 response includes the security parameters for the user. If you do not specify the UID, the TL1 response includes the security parameters for all user accounts.
CTAG	Correlation tag.

Example input

To retrieve security parameters for one account, type:

```
RTRV-USER-SECU:ARCADIA:ANNITTA:123;
```

To retrieve security parameters for all accounts, type:

```
RTRV-USER-SECU:CAPTIVA:ALL:123;
```

Response syntax

The following sections show the syntax for a normal response and an error response.

Normal response

The following syntax is the normal response to the RTRV-USER-SECU command:

```
crlf
lf
^^^<sid>^<date>^<time> crlf
M^^<ctag>^RTRV crlf
^^^"<uid>:,<uap>:<grp>" crlf
;
```

Table 3-12
RTRV-USER-SECU response syntax descriptions

Field	Description
sid	Source identifier
date	TL1 message origination date
time	TL1 message origination time
ctag	Correlation tag
uid	User identifier
uap	User access privilege for the listed user account. The options are: **R** read access only **RW** read/write access only **RWA** read/write/admin access **NULL** no access
grp	User group that contains the listed user account

Error response

The following syntax is the error response to the RTRV-USER-SECU command:

```
crlf
lf
^^^<sid>^<date>^<time> crlf
M^^<ctag>^DENY crlf
^^^"<uid>:,<uap>:<grp>" crlf
;
```

OS Connection Manager

Use the OS Connection Manager tool to define and manage OS connection profiles and to enable and disable security mode for TL1.

Chapter contents

This chapter includes the following topics:

Guide to OS Connection Manager procedures

For information on performing other system administration procedures using the OS Connection Manager, refer to the following sections in the *System Administration Procedures*, 323-3001-302, in *Operations, Administration, and Provisioning,* Volume 4A.

Procedure		See
13-1	Enabling and disabling security mode for TL1	page 13-3
13-2	Connecting to an operations system	page 13-4
13-3	Disconnecting from an operations system	page 13-6
13-4	Resetting a virtual connection to an operations system	page 13-8
13-5	Creating an operations system connection profile	page 13-11
13-6	Modifying an operations system connection profile	page 13-14
13-7	Deleting an operations system connection profile	page 13-17
13-8	Modifying the protocol identifier for an operations system connection	page 13-20
13-9	Assigning or modifying target identifiers for testing	page 13-23
13-10	Assigning or modifying target identifiers for surveillance and provisioning	page 13-27
	—end—	

OS Connection Manager main window

The OS Connection Manager main window appears when you select the tool in the session manager. Within the main window, communications sessions to an OS can be connected, disconnected, or reset. You can use menu commands on the main window to access the OS Connection Profile dialog and the Protocol ID dialog.

For information on performing other system administration procedures using the OS Connection Manager, refer to the sections in the *System Administration Procedures*, 323-3001-302, in *Operations, Administration, and Provisioning*, Volume 4A, referenced in the preceding table.

Note: The root user can now also enable or disable security mode for TL1 from the main window. Users other than root cannot change the security mode—the Enabled and Disabled buttons are only available to the root user.

Procedure 4-1
Enabling and disabling security mode for TL1

Use this procedure to enable and disable security mode.

Requirements

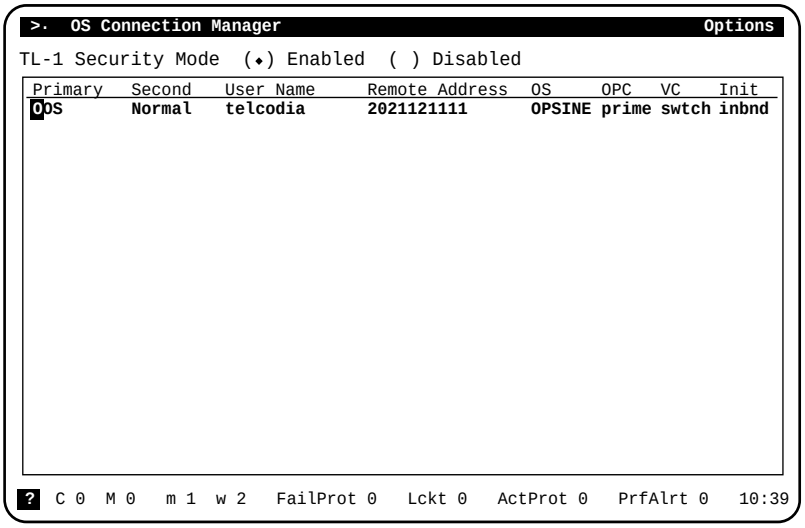
Before starting this procedure, the following requirements must be met:

- You must have the root userID and password that permit access to the operations controller (OPC) and to open the OS Connection Manager tool.
- You must be familiar with the command conventions for the interface you are using (CMT or graphical).

Action

Step	Action
1	Log in to the OPC and open the OS Connection manager tool. The OS Connection Manager tool main window is displayed.

SC-10413



2	Do one of the following: • To enable security mode, select the Enabled radio button • To disable security mode, select the Disabled radio button ***Note:*** The security mode is updated as soon as the radio button is selected.
3	Continue with the OS Connection manager operations you want to perform. Refer to “Guide to OS Connection Manager procedures” on page 4-2.

—continued—

Procedure 4-1 (continued)
Enabling and disabling security mode for TL1

Step	Action
	Note 1: Any OS interface session that is running when the security mode is changed will be unaffected by the change. When the session is restarted, the new setting will take effect. The OS interface checks the security mode setting when it starts up. ***Note 2:*** Security mode affects the operation of provision and surveillance OS interfaces only. It does not affect testing OS interfaces or the operation of any of the user interfaces. **—end—**

SONET Products

AccessNode

TL1 Enhanced Security Quick Reference Guide

Document number: P0909010
Document release: Issue 1.0
Date: August 1999
Printed in Canada

NORTEL NETWORKS™