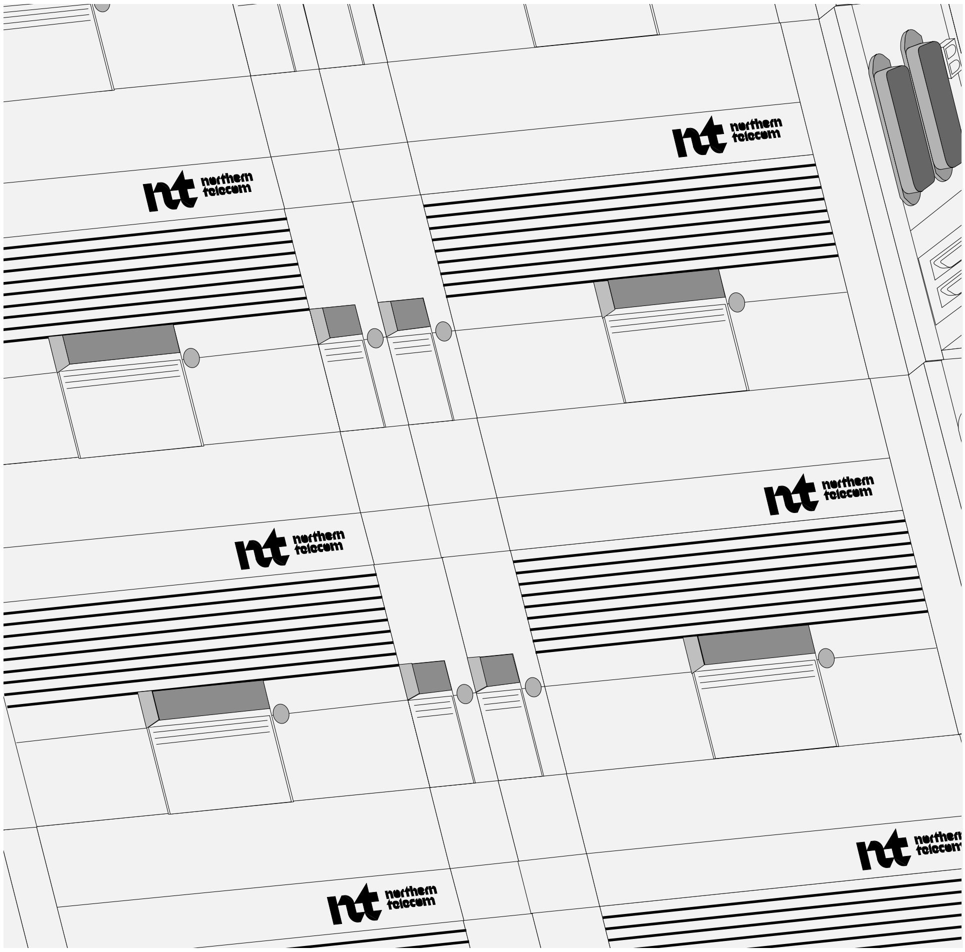
NT4K00LA **323-3001-302**

SONET Products

AccessNode

System Administration Procedures

Issue 4.0 October 1999



NORTEL NETWORKS™

SONET Products

AccessNode

System Administration Procedures

Document number: 323-3001-302
Document release: Issue 4.0
Date: October 1999

Printed in Canada

All information contained in this document is subject to change without notice. Nortel Networks reserves the right to make changes to equipment design or program components, as progress in engineering, manufacturing methods, or other circumstances may warrant.

Publication history

October 1999

AN17.20 Standard release of the document, Issue 4.0.

August 1999

AN17.11 release of document, Issue 3.0. Added information on enabling and disabling security mode for TL1 commands to Chapter 13.

June 1999

AN17 Standard release of the document, Issue 2.0.

February 1999

AN16 Standard release of the document, Issue 1.0. Changes include the following:

- added OPC Alarm Provisioning tool to Chapter 4
- added procedures for configuring and enabling TIRS to Chapter 2
- added procedure for Root1 User to Chapter 4
- added information for Password Notification/Physical Port Intrusion feature to Chapter 4

June 1998

AN15 Standard 01.01 release of the document. This book was edited to make the content easier to understand.

September 1997

AN14 Standard 01.01 release of the document. For this release, the following information has been added:

- user ID restrictions added to Procedures 4-1 and 4-2
- read-only Connection Manager information added to Procedures 4-10 and 4-11
- TID information modified in Procedure 13-8
- Procedure 13-9 added

July 1996

Standard 01.01 AN12 release of the document.

November 1995

Standard 02.01 AN11 release of the document.

May 1995

Update to Standard AN10 release of the document. Note 1 on page 1-21 is updated.

April 1995

Standard AN10 release of the document.

March 1995

Release of AN08 formal addendum.

December 1994

Standard AN08 release of the document.

November 1994

Reissue of AN07 standard.

April 1994

Standard AN07 release of the document.

May 1993

Standard FWP06 release of the document.

Contents

About this document

This document contains provisioning and operating instructions for an AccessNode. Tasks include configuring operations controller (OPC) ports for available services, provisioning and maintaining centralized security, provisioning user interface ports, specifically parallel telemetry points, and customizing network elements.

This document describes each task as a set of instructions. The instructions are presented as a series of numbered procedures. Procedures are grouped into chapters according to the type of function being performed.

The document is organized into chapters according to natural groupings of administration tasks.

Audience

This document is for maintenance technicians and experienced installers from Nortel Networks or other telephone operating companies.

How to use this document

This document has the system administration process and procedures for AccessNode. As a guide for using this document, it is recommended that you start with Chapter 1. Chapter 1 provides an overview of the process using flowcharts and document task lists.

The document task list in Chapter 1 points you to the correct procedure and page number for each task that you need to perform. By following the document task list in Chapter 1, you are only performing only those tasks that are needed for your specific system.

Chapters in this document also include procedures that are performed occasionally, but are not included in the overall flow.

Warnings and safety precautions

To avoid injury, follow all danger warnings provided with this product, as well as safety procedures established by your company.

To avoid damage to equipment or service interruptions, follow all caution notices provided with this product, as well as procedures established by your company.

Samples of danger and caution notices follow.

DANGER
Risk of personal injury
A danger notice informs you of a risk of personal injury.

CAUTION
Risk of service interruption or equipment damage
A caution notice informs you of a risk of service interruption or equipment damage.

DANGER
Risk of electric shock
This notice advises you of a possible electrical hazard. When you see this notice, proceed with care to avoid personal injury.

OPC procedures

You can use a graphical terminal for the OPC procedures in this document (even though the procedures are based on a character-mode terminal). If you use a graphical terminal, you must substitute the graphical equivalent of the character-mode keystrokes used in the procedures. See the Graphical Reference card that is provided in the sleeve of this volume.

The commands, parameter, and response conventions used in OPC procedures are provided in *OPC User Interface Description*, 323-3001-301, in this volume.

References in this document

This document refers to the following documents in the AccessNode documentation library.

Description, Volume 2A

- *Alarms and Surveillance Description*, 323-3001-104

Operations, Administration, and Provisioning, Volume 4A

- *Network Element User Interface Description*, 323-3001-300
- *OPC User Interface Description*, 323-3001-301
- *Data Administration Procedures*, 323-3001-304

Operations, Administration, and Provisioning, Volume 4B

- *Line Card Provisioning Procedures*, 323-3001-315

Maintenance, Volume 5A

- *Alarm and Trouble Clearing Procedures*, 323-3001-543

Maintenance, Volume 5C

- *Network Surveillance Procedures*, 323-3001-510

Separately bound documents

- *TL1 Interface Description*, 323-3001-190
- *Bay in Central Office Installation Manual—TBM*, 323-3001-202

In addition, this document refers to the following documents.

- *DMS-100 Subscriber Carrier Module-100 Access Translations Guide*, 297-2741-350
- *DMS-100 XPM Translations Reference Manual*, 297-8321-815.

Overview of system administration

This chapter has the general information required for the system administration process and procedures. The flowcharts and document task lists in this chapter give an overall view of the process.

This chapter also includes information on equipment cautions and notices.

Chapter contents

This chapter includes the following topics:

Equipment cautions and notices

This section has the warnings and precautions for personal safety and for proper handling and operation of equipment.

Static electricity

Static electrical charges can build up on your body if you walk a short distance. This buildup of static electricity can damage some circuit packs if it is not properly discharged first. Circuit packs that are sensitive to damage by static electricity should be packaged in antistatic material. The following precautions are recommended.

Handling circuit packs

Units that are sensitive to static electricity have the following label on their antistatic shipping bags:

ATTENTION
OBSERVER LES PRECAUTIONS
POUR LA MANIPULATION DES
DISPOSITIFS SENSIBLES AUX
CHARGES STATIQUES

ATTENTION
OBSERVE PRECAUTIONS
FOR HANDLING
ELECTROSTATIC
SENSITIVE DEVICES

To avoid static electrical damage when handling circuit packs, follow these rules:

- Do not remove circuit packs from their antistatic packages unless you are using antistatic protection, such as wearing an antistatic wrist strap. The wrist strap is attached to a long cord, which must terminate at a good ground source, so static buildup is harmlessly discharged. Alternative antistatic methods include conductive carpet, conductive shoes, or heel grounders. Use the equipment recommended by your company.
- Handle each circuit pack by the faceplate or stiffener. Do not touch electrical connections, pins, or soldered surfaces.
- Protect optical connectors by covering them with clean dust caps.

Storing and transporting circuit packs

When storing and transporting circuit packs, follow these rules:

- Never transport, stack, or store circuit packs without first replacing them in their antistatic material and shipping package.

  Note: Proper packaging is especially important for heavier dual-card units, like the integrated remote test unit (IRTU). This packaging avoids physical damage and accumulation of dirt or dust on goldplated contacts. Be careful not to damage any parts when placing the circuit pack in its packaging.

- Avoid storing circuit packs in areas where the relative humidity can exceed 95% and where the temperature can exceed 70°C, because circuit packs can warp or corrode.

Laser radiation

AccessNode equipment and associated optical test sets use laser sources that emit light energy into fiber cables. This energy is within the red (visible) and infrared (invisible) regions of the electromagnetic spectrum.

Laser products are subject to federal and state or provincial regulations, and local practices. Regulation 21 CFR 1040 of the U.S. Bureau of Radiological Health requires manufacturers to certify each laser product as Class I, II, III, or IV, depending upon the characteristics of the laser radiation emitted. In terms of health and safety, Class I products present the least hazard (none at all), while Class IV products present the greatest hazard.

DANGER
Risk of eye damage
At all times when handling optical fibers, follow the safety procedures recommended by your company.

Read and observe the following precautions to decrease the risk of exposure to laser radiation.

Although Nortel Networks optical products have a Class I certification, hazardous exposure to laser radiation can occur when fibers connecting system components are disconnected or broken. Certain procedures carried out during testing require the handling of optical fibers without dust caps and therefore increase the risk of exposure. Exposure to either visible or invisible laser light can damage your eyes under certain conditions.

Comply with the caution label at the right, which is on the optical interface card, near the optical connector.

Caution
Avoid direct exposure to beam. Invisible light can blind. Keep all optical connectors capped.

Handling optical fibers

During service, maintenance, repair, or removal of cables or equipment, follow these rules:

- Avoid direct exposure to fiber ends or optical connector ends. Laser radiation may be present and can damage your eyes.
- Follow the manufacturer’s instructions when using an optical test set. Incorrect calibration or control settings can result in hazardous levels of radiation.

Splicing optical fibers

During the splicing of any fiber cable, you might have to look at the fibers using an eye loupe (a small magnifier). Take the following precautions:

- Power off all laser sources related to those fibers, and make sure they remain off (whether located at the central office, subscriber premises, or remote location).
- Disconnect any optical test sets from the fibers (whether locally or remotely connected).
- Use only the optical instruments approved by your company.

Repairing optical fibers

When an accidental break in the fiber feeder cable occurs, take the following steps:

- Notify both central-office and field-repair personnel of the problem.
- Identify to central-office personnel what fibers are damaged.
- Power off all laser sources related to the damaged fibers (whether located at the central office, subscriber premises, or remote location).

Equipment warning label

The following warning label shown below is in the top left corner on the back cover of the equipment.

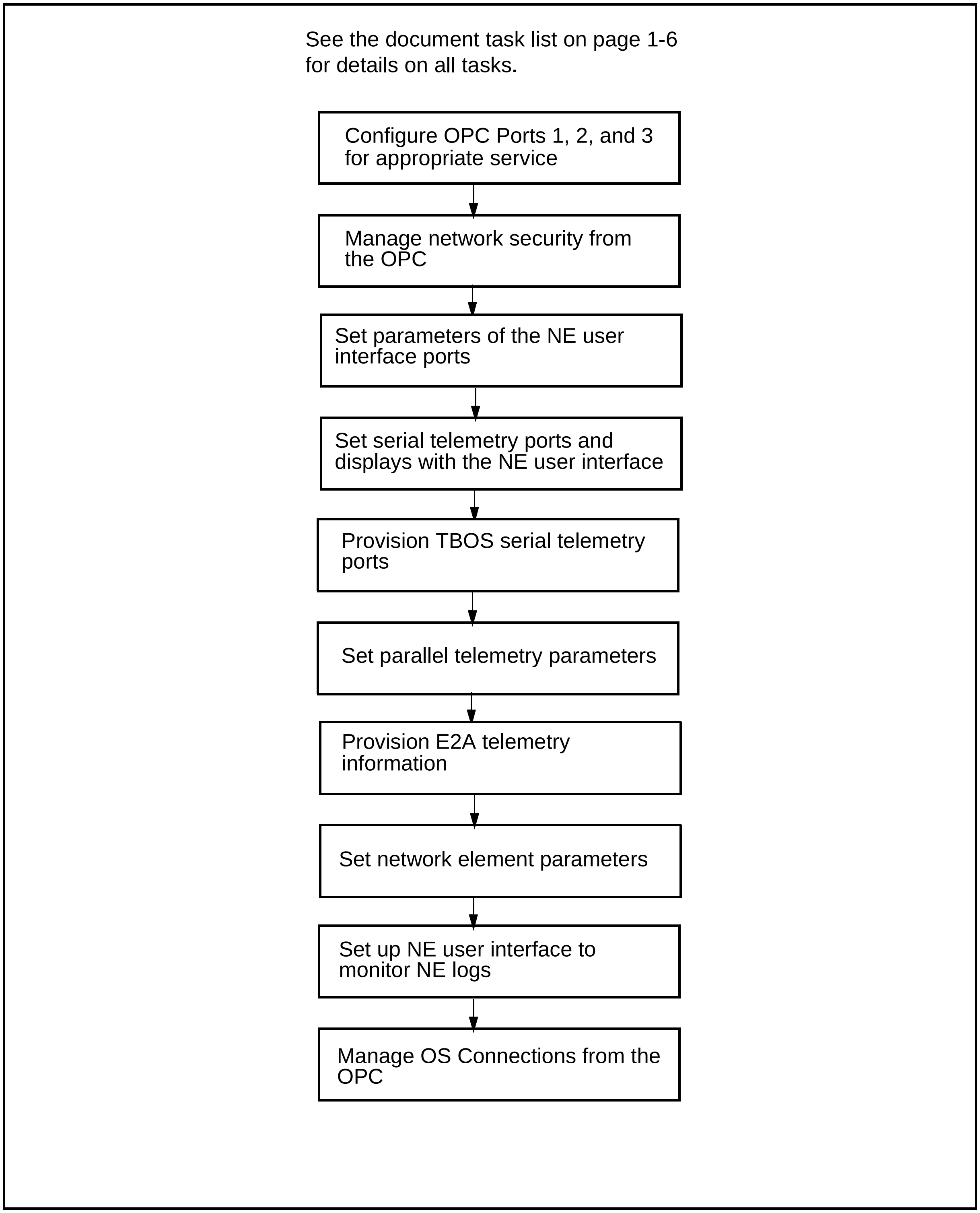
> To be installed only in restricted access areas
> (dedicated equipment rooms, equipment closets,
> or the like) in accordance with articles 110-16,
> 110-17, and 110-18 of the National Electrical Code,
> ANSI/NFPA No. 70.

How to use the flowchart and task list

The following flowchart and task list detail the system administration process and procedures. Use the flowchart and task list to perform the AccessNode system administration procedures in this document.

Note: The chapters in this document also include procedures that are performed occasionally, but are not included in the overall flow.

Figure 1-1
Administering an AccessNode system


See the document task list on page 1-6
for details on all tasks.
Configure OPC Ports 1, 2, and 3 for appropriate service
Manage network security from the OPC
Set parameters of the NE user interface ports
Set serial telemetry ports and displays with the NE user interface
Provision TBOS serial telemetry ports
Set parallel telemetry parameters
Provision E2A telemetry information
Set network element parameters
Set up NE user interface to monitor NE logs
Manage OS Connections from the OPC

Document task list

The following task is for the system administrator to follow when setting up a new user. (It does not include tasks that the system administrator performs to maintain the user after the initial setup. These occasional tasks can are in the chapter task lists of the appropriate chapter, and are performed as required.)

Task	Procedure	See
Configuring OPC Ports 1, 2, and 3 for appropriate service		
Configuring for X25 connection (without TL1)		
— Completing X.25 interface worksheet	-	page 2-10
— Defining and enabling an X.25 configuration	2-1	page 2-16
— Connecting the cable	2-9	page 2-64
Configuring for X25 connection (with TL1)		
— Completing X.25 interface worksheet	-	page 2-10
— Defining and enabling an X.25 configuration	2-1	page 2-16
— Managing virtual circuit profiles (for TL1 over X.25)	2-8	page 2-61
— Connecting the cable	2-9	page 2-64
— Rebooting the OPC (for TL1 over X.25)	see 323-3001-304	-
Configuring for printer connection		
— Configuring an OPC port to support a printer	2-3	page 2-27
— Configuring the printer	see printer documentation	
— Connecting the cable	2-9	page 2-64
Configuring for terminal connection		
— Configuring an OPC port to support a terminal	2-2	page 2-24
— Connecting the cable	2-9	page 2-64
Configuring for X.3 PAD connection		
— Defining X.3 PAD configuration parameters	2-4	page 2-32
— Configuring an OPC port to support X.3 PAD	2-4	page 2-32
Configuring for PPL connection		
— Configuring an OPC port to support PPL	2-5	page 2-43
— Configuring a modem	2-6	page 2-52
Accessing TL1 by Ethernet		
— Creating a user account for a TL1 interface	3-1	page 3-2
— Logging in and out of the TL1 interface using telnet	3-2	page 3-4

—continued—

Task	Procedure	See
Managing network security from the OPC		
Creating a new user account	4-1	page 4-17
Creating a user group (if necessary)	4-8	page 4-38
Setting parameters of the network element (NE) user interface ports		
Changing the user interface port parameters	7-3	page 7-4
Activating or deactivate a user interface port	7-5	page 7-7
Setting serial telemetry ports and displays with the NE user interface		
Activating or deactivate an E2A TBOS port	8-3	page 8-5
Adding or changing an E2A TBOS port display	8-4	page 8-6
Deleting a display from an E2A TBOS port	8-5	page 8-8
Enabling or disabling a TBOS port display	8-6	page 8-9
Provisioning TBOS serial telemetry ports		
Assigning a display to a TBOS port	15-2	page 15-6
Deleting a display from a TBOS port	15-3	page 15-9
Assigning a remote alarm	15-4	page 15-11
Setting parallel telemetry parameters		
Enabling or disabling a telemetry input point	9-3	page 9-5
Provisioning the alarm severity of the telemetry inputs	9-4	page 9-7
Provisioning the telemetry input service impact (SA or NSA)	9-5	page 9-9
Changing the telemetry output port settings	9-9	page 9-15
Provisioning E2A telemetry information		
Assigning an alarm to a signal distribution point	10-2	page 10-8
Deleting an alarm from a signal distribution point	10-3	page 10-11
Assigning the default alarm to a signal distribution point	10-4	page 10-13
Setting network element parameters		
Changing a scheduled shelf event or exercise	11-4	page 11-5

—continued—

Task	Procedure	See
Setting up NE user interface to monitor NE logs		
Connecting a log output device and configure a user interface port for a log output device	12-1	page 12-2
Setting the NE log format	12-2	page 12-5
Enabling or disabling user interface (UI) ports (1 or 2) for printing logs	12-3	page 12-6
Starting and stopping log output to a terminal	12-8	page 12-13
Managing OS Connections from the OPC (optional)		
Connecting to an operations system	13-2	page 13-4
Disconnecting from an operations system	13-3	page 13-5
Resetting a virtual connection to an operations system	13-4	page 13-6
Creating an OS connection profile	13-5	page 13-7
Modifying an OS connection profile	13-6	page 13-9
Deleting an OS connection profile	13-7	page 13-10
—end—		

Configuring OPC ports for X.25, terminal, or printer operation

The operations controller (OPC) supports X.25, VT100 terminal, or printer connectivity through serial ports OPC Ports 1, 2, and 3. The default configuration of OPC Port 1 is for a terminal. This chapter describes how to reconfigure OPC Ports 1, 2, or 3.

Chapter contents

This chapter includes the following topics:

OPC supported systems

Table 2-1 identifies the available ports and the labels for OPC-supported systems. See Figure 2-1 on page 2-3 through Figure 2-3 on page 2-5 for port locations.

Table 2-1
Available ports and labels for OPC-supported systems

Shelf type	OPC slot	Port 1	Port 2	Port 3
Transport bandwidth manager (TBM)	5	OPC Port 1 (J09)	OPC Port 2 (J07)	-
Access bandwidth manager (ABM)	1 or 5	OPC Port 1 (J07)	OPC Port 2	OPC Port 3
System line-up and test operations controller (SLAT OPC)	N/A	Port B	ESP 1	ESP 2

> ***Note:*** The OPC port on the SLAT OPC may be labeled port B.

In systems where more than one serial port is available, the OPC supports the following:

- at most, one serial port for X.25 operation
- at most, one serial port for terminal operation
- at most, one serial port for printer operation

Figure 2-1
Port location for TBM

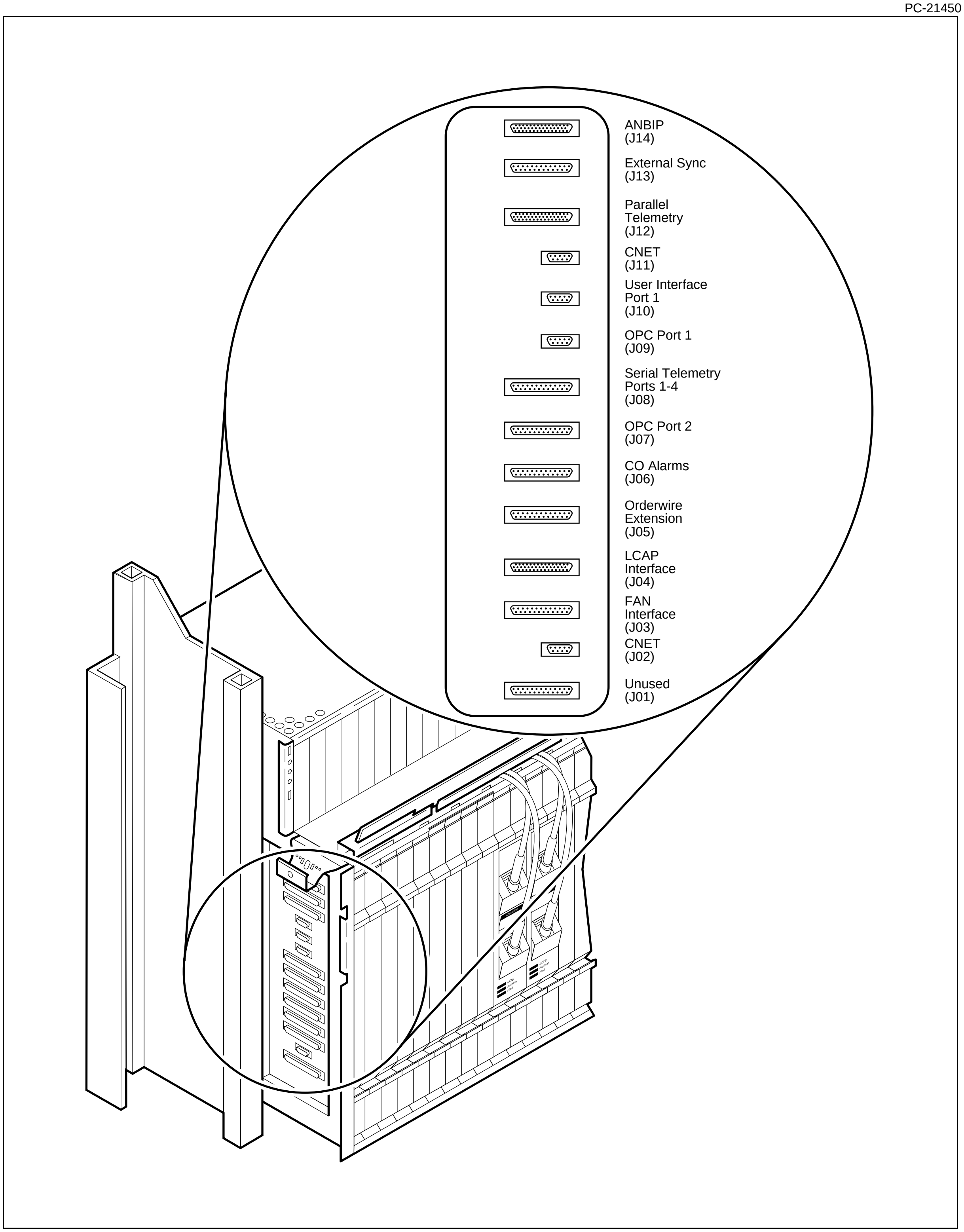


Figure 2-2
Port location for ABM shelf

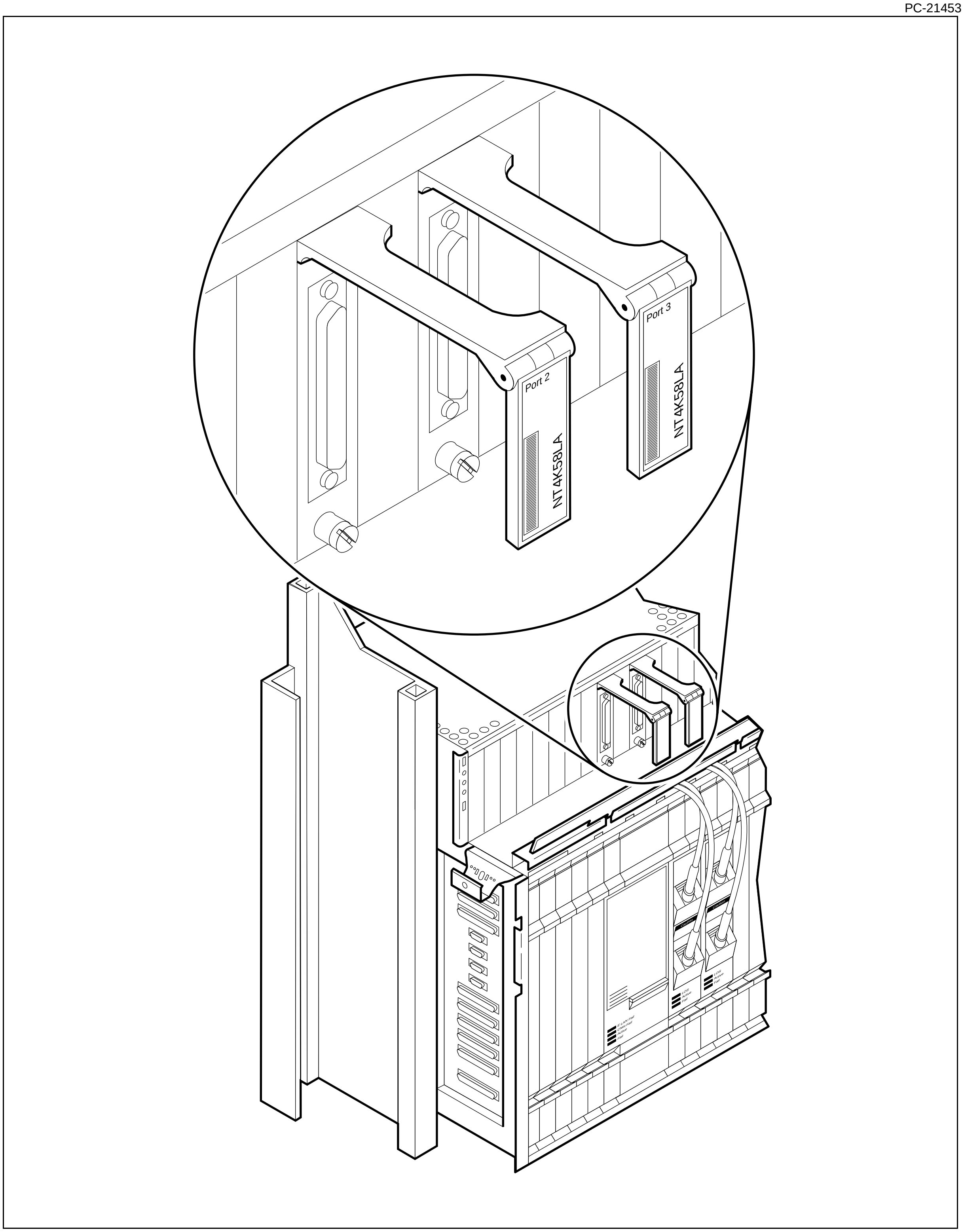
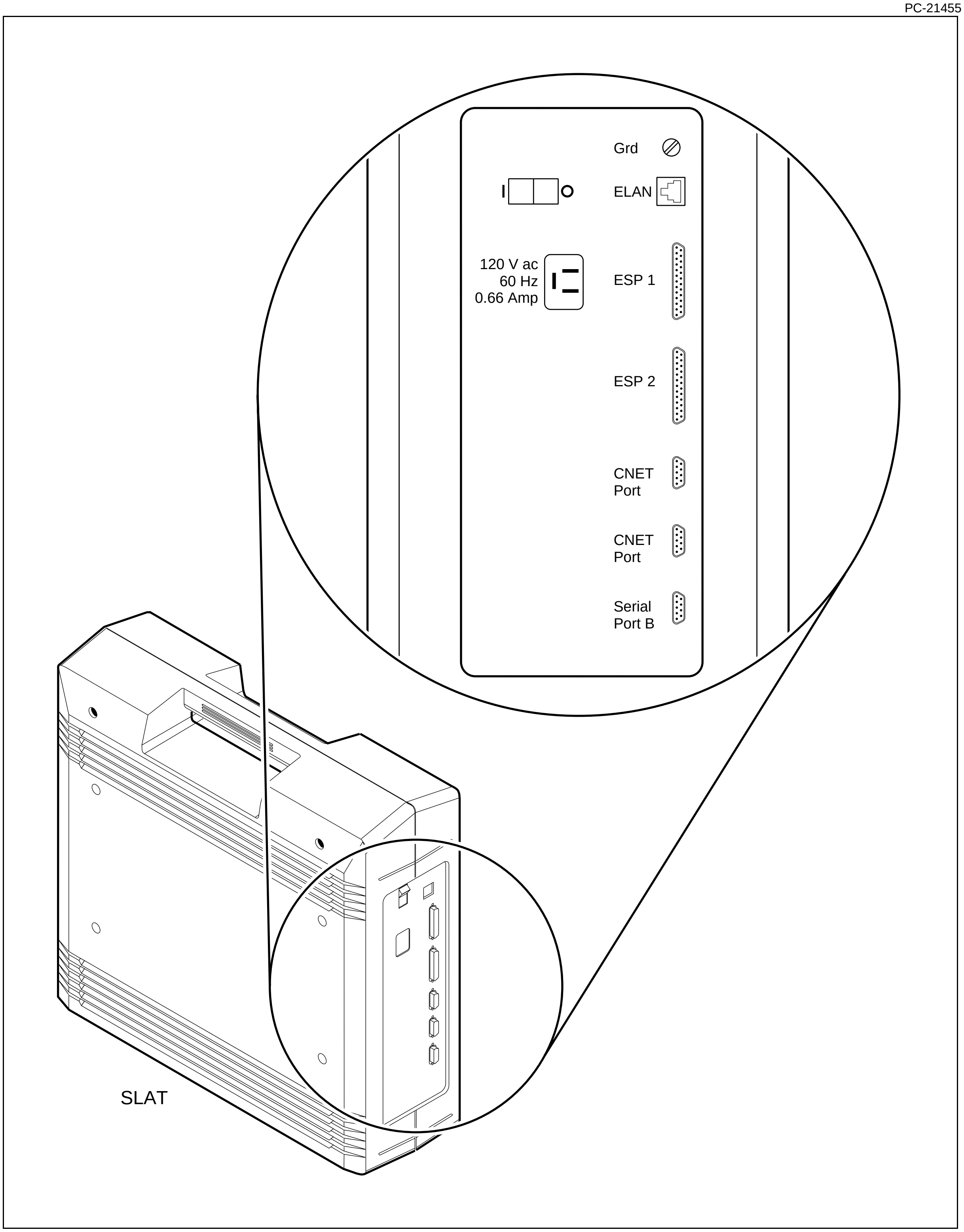


Figure 2-3
Port location for SLAT OPC



Chapter task lists

This chapter includes the following tasks. Other tables in this section list tasks that must be completed in a specific order.

Procedure	Task	See
2-1	Defining and enabling an X.25 configuration	page 2-16
2-2	Configuring an OPC port to support a VT-100 terminal	page 2-24
2-3	Configuring an OPC port to support a printer	page 2-27
2-4	Configuring an OPC port to support X.3 PAD	page 2-32
2-5	Configuring an OPC port to support electronic software delivery (PPL connection)	page 2-43
2-6	Configuring a modem for electronic software delivery (PPL connection)	page 2-52
2-7	Unconfiguring an OPC port	page 2-59
2-8	Managing virtual circuit profiles	page 2-61
2-9	Connecting the cable	page 2-64
2-10	Configuring the TL1 Interface Router Service over X.25	page 2-65
2-11	Configuring the TL1 Interface Router Service over TCP/IP	page 2-74

Configure an OPC port for X.25 communications

Perform the following tasks, in the order shown, to configure an OPC port for X.25 communications without TL1.

Procedure	Task	See
	Complete X.25 interface worksheet	page 2-10
2-1	Defining and enabling an X.25 configuration	page 2-16
2-9	Connecting the cable	page 2-64

Perform the following tasks, in the order shown, to configure an OPC port for X.25 communications with TL1.

Procedure	Task	See
	Complete X.25 interface worksheet	page 2-10
2-1	Defining and enabling an X.25 configuration	page 2-16
2-8	Managing virtual circuit profiles	page 2-61
2-9	Connecting the cable	page 2-64
	Reboot the OPC (for TL1 over X.25) in *Data Administration Procedures*, 323-3001-304, in this volume	

Modify X.25 communications on an existing configuration

Perform the following tasks to modify X.25 communications parameters on an existing configuration.

Procedure	Task	See
2-1	Defining and enabling an X.25 configuration	page 2-16

Configure an OPC port for VT100 access

Perform the following tasks to configure an OPC port for VT100 terminal access.

Procedure	Task	See
2-2	Configuring an OPC port to support a VT-100 terminal	page 2-24
2-9	Connecting the cable	page 2-64

Configure an OPC port for printing

Perform the following tasks to configure an OPC port for printing. See *Network Surveillance Procedures*, 323-3001-510, in *Maintenance*, Volume 5C, for information about the printing of the event logs and alarms.

Procedure	Task	See
2-3	Configuring an OPC port to support a printer	page 2-27
	Configure the printer	(see printer documentation)
2-9	Connecting the cable	page 2-64

Modify configuration for X.3 PAD connection

If X.3 PAD is currently configured, changes to the X.3 PAD configuration do not take effect until the service is first unconfigured, then configured again.

Perform the tasks in the following table to configure a port for X.3 PAD connection.

> ***Note:*** After the X.3 PAD configuration has been transferred to the backup OPC, the service must also be unconfigured and then configured again at the backup OPC. Perform Procedure 2-4 on page 2-32 and Procedure 2-7 on page 2-59 after you log in to the backup OPC.

Procedure	Task	See
2-4	Defining X.3 PAD configuration parameters	page 2-32
2-4	Configuring an OPC port to support X.3 PAD	page 2-32
2-7	Unconfiguring an OPC port	page 2-59

Configure a port for a PPL connection

Perform the tasks in the following table to configure a port for electronic software delivery (PPL connection).

Procedure	Task	See
2-5	Configuring an OPC port to support PPL	page 2-43
2-9	Connecting the cable	page 2-64

Modify services

Perform the tasks in the following table to modify services.

Procedure	Task	See
2-4	Configuring an OPC port to support X.3 PAD	page 2-32
2-7	Unconfiguring an OPC port	page 2-59

Configure the TL1 Interface Router Service over X.25

Perform the tasks in the following table to configure the TL1 Interface Router Service over X.25.

Procedure	Task	See
2-10	Configuring the TL1 Interface Router Service over X.25	page 2-65

Configure the TL1 Interface Router Service over TCP/IP

Perform the tasks in the following table to configure the TL1 Interface Router Service over TCP/IP.

Procedure	Task	See
2-11	Configuring the TL1 Interface Router Service over TCP/IP	page 2-74

Complete X.25 interface worksheet

You can specify X.25 configuration parameters. If the default value is appropriate for your installation, you do not have to change it. Do not change default values for

- parameters with the value N/A in the column "Typical OPC value" (these are not used by the OPC port)
- the following parameters: Device name, Programmatic Access Name, and Network Type

Table 2-2 lists the X.25 configuration parameters that can be specified. Make sure your network provider supports the values listed in the Typical OPC value column. If not, see "Selected X.25 parameter descriptions" on page 2-13, and select an alternative value. Record the selected value in the table. When performing Procedure 2-1 on page 2-16, use the values you have identified.

Table 2-2
X.25 configuration parameters

Parameter	Default value	Typical OPC value	Your value
Global parameters			
X.121 Address	none		
X.121 Packet Address	none	same as X.121 address	
Device Name	/dev/x25_0	/dev/x25_0	
Programmatic Access Name	scc0	scc0	
Level 2 parameters			
Level 2 Window	7	7	
Retransmission timer (T1 ms)	3000	3000	
Idle time (T3 ms)	60000	60000	
Idle probe timer (T4 ms)	0	0	
Retransmission count (N2)	20	10	
Frame size in octets (N1)	149	263	
IP parameters			
IP address	none	N/A	
IP subnet mask	none	N/A	
Idle timer	600	N/A	
Hold timer	300	N/A	
MTU size	2048	N/A	

—continued—

Table 2-2 (continued)
X.25 configuration parameters

Parameter	Default value	Typical OPC value	Your value
Level 3 parameters			
Network type	DTE_84	DTE_84	
Flow control	off	on	
Throughput class	off	on	
Fast select	disabled	disabled	
Reverse charging	disabled	disabled	
PVC packet size in (octets)	128	N/A	
PVC packet size out (octets)	128	N/A	
PVC window size in	2	N/A	
PVC window size out	2	N/A	
PVC throughput class in	11	N/A	
PVC throughput class out	11	N/A	
Default packet size in (octets)	128	128	
Default packet size out (octets)	128	128	
Default window size in	2	2	
Default window size out	2	2	
Default throughput class in	11	10	
Default throughput class out	11	10	
Negotiation packet size in (octets)	128	256	
Negotiation packet size out (octets)	128	256	
Negotiation window size in	2	2	
Negotiation window size out	2	2	
Negotiation throughput class in	11	10	
Negotiation throughput class out	11	10	
Maximum number of circuits	0	8	
Number of permanent virtual circuit (PVC)	0	0	
Number of switched virtual circuit (SVC)	0	8	
Number of inbound SVC	0	0	

—continued—

Table 2-2 (continued)
X.25 configuration parameters

Parameter	Default value	Typical OPC value	Your value
Starting LCI for SVC	not applicable	1	
Number of outbound SVC	0	0	
—end—			

Selected X.25 parameter descriptions

The following descriptions indicate the range of alternative values that selected parameters can accept. These values are useful when your network provider cannot provide the exact service defined by the parameter values listed in Table 2-2 on page 2-10. Select a value as close to the recommended value as possible, unless otherwise noted. This information is not intended to define the function of the parameter. Parameters that are not described below must be specified as shown in the “Typical OPC value” column of the table.

X.121 address

The value for X.121 address is assigned by the network provider. It is a maximum of 14 decimal digits, and can contain no other characters.

Level 2 window

This parameter takes a value within the range of 1 to 7. Use the largest value supported by the network provider, within this range.

Retransmission timer (T1)

This parameter can have a value between 1 000 and 12 000 ms.

Idle timer (T3)

The value of the Idle timer should be greater than the product of the Retransmission timer and the Retransmission count (T1 x N2). It must be less than 13 000 000. A value of 0 disables the timer; otherwise, the minimum value is 1 000 ms.

Idle probe timer (T4)

This parameter can have a value between 0 and the value set for timer T3. A value of 0 disables the timer.

Note: If the timer is disabled, make sure the data circuit is providing a “keep alive signal”; otherwise, the OPC will drop the connection after a specified time interval (approximately 60 seconds).

Retransmission count (N2)

Retransmission count can have a value in the range 0 to 255.

Frame size

Generally, the Frame size takes a value equal to the largest level 3 packet size plus 7. If fast select is disabled and the largest packet size is 128 octets, you can use a value of 149. If fast select is enabled or the maximum packet size is 256 octets, you must use the value 263.

Packet size

Packet size can be 128 or 256. However, you must specify 128 when flow control is off.

Window size

Window size must be in the range 1 to 7. Use the value of 2 only if flow control is on.

Throughput class

Throughput describes the maximum amount of data that can be sent through the network.

The throughput class parameter value must be in the range 3 to 13, and is based on the following table:

Throughput class	Baud rate
13	64000
12	48000
11	19200
10	9600
9	4800
8	2400
7	1200
6	600
5	300
4	150
3	75

Note 1: It is recommended that you set the throughput class at a baud rate equal to the modem setting.

Note 2: For Ports 1 or 3, the maximum baud rate is 9600 (or throughput class of 10); for port 2, the maximum baud rate is 48 000 (or throughput class of 12).

Sample X.25 configuration file

The following page contains the contents of a sample X.25 configuration file named X25INIT_TEMPLATE, which is located in the /etc directory. This file contains X.25 configuration parameters that are typical for the OPC port.

```
#
# X.25 Initialization File
#
#
# Global Parameters
#
x.121                       123456789000
device                      /dev/x25_0
name                        scc0
#
# Level 2 Parameters
#
t1                          3000
t3                          60000
framesize                   263
n2                          10
l2window                    7
#
# Level 3 Parameters
#
networktype                 DTE_84
#
# Circuit Table Definition
#
# LCI                       TYPE        HOW MANY
lci 1                       svc         8
max_circuits                8
#
# Flow Control, Throughput Class, Fast Select and Reverse Charge Settings
#
flowcontrol                 on
thruputclass                on
fast_select_accept          disabled
reverse_charge              disabled
def_inpacketsize            128
def_outpacketsize           128
def_inwindow                2
def_outwindow               2
def_inthruputclass          10
def_outthruputclass         10
neg_inpacketsize            256
neg_outpacketsize           256
neg_inwindow                2
neg_outwindow               2
neg_inthruputclass          10
neg_outthruputclass         10
```

Procedure 2-1
Defining and enabling an X.25 configuration

Use this procedure to define the X.25 configuration parameters for your operation. You must know the specifications of the X.25 service offered by your local X.25 network provider. Your X.25 subscription profile defines the specifications.

Port configuration from the OPC involves an interactive program that displays menus and prompts to guide you through the process of specifying configuration parameters. The following procedure tells you how to invoke the program. After you invoke the program, the program then prompts you to supply the necessary parameter values. If the program terminates abnormally, it might create a configuration file that will not support X.25 communications. In this situation, you must re-execute this procedure from the beginning.

Information is provided at the beginning of this chapter about parameters that you might need to change. Values for these parameters must be negotiated with your network provider. An X.25 interface worksheet is provided on page 2-10 to assist you with this negotiation.

If you can use the UNIX vi editor, you can edit the X.25 configuration file (x25init_scc0) directly to alter the configuration parameters. To assist you, a sample file is available in the /etc directory. Its filename is X25INIT_TEMPLATE. Its contents are reproduced on page 2-14. Modification of the x25init_scc0 file using vi is not supported by this procedure.

When you see the ↵ character, press Return.

—continued—

Procedure 2-1 (continued)
Defining and enabling an X.25 configuration

Requirements

Before performing this procedure, you must do the following:

- Obtain the root or admin userID and password.
- Obtain the values of the basic parameters that define the X.25 service which is provided by your carrier; these parameters are described on page 2-13.
- Fill out the X.25 interface worksheet on page 2-10.

Action

Step **Action**

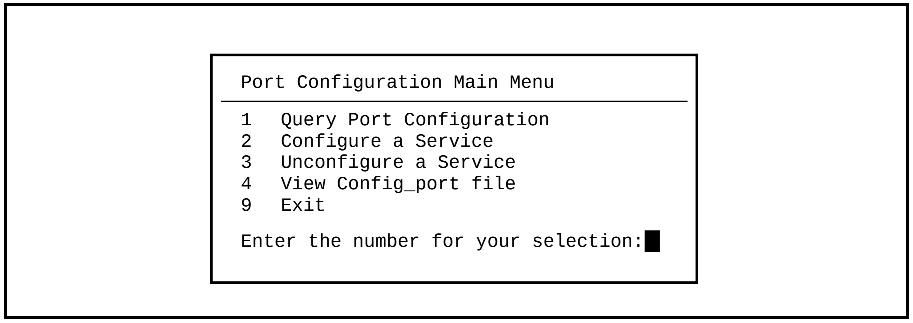
1 Log in to the OPC.

If you do not know how to do this, see the procedures in *User Interfaces Description*, 323-3001-301, in this volume.

If you are logging in as	Then
root	*The UNIX prompt, opc>, appears. Enter the following command:* **config_port**
admin	*The User Session Manager appears. Move to the Port Configuration tool, then press* ***Ctrl_A*** *(or Keypad* ***0****).*

The Port Configuration main menu appears.

PC-22029



```
Port Configuration Main Menu

1   Query Port Configuration
2   Configure a Service
3   Unconfigure a Service
4   View Config_port file
9   Exit

Enter the number for your selection:█
```

2 To display OPC port configuration, enter:

1 ↵

The port configurations appear. If ports 2 and 3 are available, these ports are listed.

3 Record the port configurations, then press **Enter** to return to the main menu.

—continued—

Procedure 2-1 (continued)
Defining and enabling an X.25 configuration

Step **Action**

Configuring a service and X.25

4 Configure a service by entering:

2 ↵

The Configure a service menu appears.

1	Terminal
2	Printer
3	X.25
4	X.3 PAD
5	PPL
8	Return to Main menu
9	Exit

5 Configure X.25 by entering:

3 ↵

The Configure X.25 menu appears.

1	View X.25 parameters
2	Enter X.25 parameters
3	Enable X.25
8	Return to Configure menu
9	Exit

6 View X.25 parameters by entering:

1 ↵

X.25 configuration parameters appear.

—continued—

Procedure 2-1 (continued)

Defining and enabling an X.25 configuration

Step **Action**

7 Compare the X.25 parameters values on your X.25 interface worksheet with the values on the screen, then press **Return** to return to the configure X.25 menu.

If the values are	Then go to
different	step 8
the same	step 23

8 Enter X.25 parameters by entering:

2 ↵

The following messages and prompts appear. If an X.25 configuration file already exists, you are prompted to confirm the creation of a new one. If necessary, confirm by entering **Y** ↵*.*

```
The X.25 configuration file (/etc/x25init_scc0) already
exists.
Do you want to create a new configuration file? (Yes/No):
yes
moving /etc/x25init_scc0 to /etc/x25init_scc0.bak
/etc/x25init: release_id is “hpx10ac,07/26/93,00:01”
Fri Sep 08:11:59 EDT#Canada 1993
```

To properly configure X.25 you *must* know the following information:

- X.121 Address
- X.25 Programmatic Access Name
- Circuit Table Definition

```
Do you wish to begin configuring X.25 parameter values?
[y/n]:
```

—continued—

Procedure 2-1 (continued)
Defining and enabling an X.25 configuration

Step **Action**

Defining parameter values

9 To begin defining parameter values, enter:

y ↵

The following menu appears:

1	Global parameters
2	Level 2 parameters
3	Level 3 parameters
4	IP parameters
5	Display all parameters
6	Exit configuration program and create file
7	Abort configuration program; file will not be created.

10 To select global parameters, enter:

1 ↵

The global parameters appear. Default values are in square brackets following the parameter name. A menu containing two entries appears.

11 To modify global parameters, enter:

1 ↵

Each of the global parameters appears in turn. You can enter a value, or accept the default value by pressing ***Return****.*

12 Respond to the prompts as required. To change the default value, enter a new value, then press **Return**. To accept the default value, press **Return**. For parameters that do not have a default, you must specify a value.

After you respond to all displayed parameters, the current values of all global parameters appear, and a menu containing two entries appears.

13 To return to the menu shown in step 9, enter:

2 ↵

—continued—

Procedure 2-1 (continued)
Defining and enabling an X.25 configuration

Step **Action**

14 To select level 2 parameters, enter:

2↵

The level 2 parameters appear. Default values are in square brackets following the parameter name. A menu containing two entries appears.

15 To modify level 2 parameters, enter:

1 ↵

*Each of the level 2 parameters appears in turn. You can enter a value, or press **Return** to accept the default value.*

16 Respond to the prompts as required. To change the default value, enter a new value, then press **Return**. To accept the default value, press **Return**. For parameters that do not have a default, you must specify a value.

After you respond to all displayed parameters, the current values of all level 2 parameters are displayed, and a menu containing two entries appears.

17 To return to the menu shown in step 9, enter:

2 ↵

18 To select level 3 parameters, enter:

3 ↵

The level 3 parameters appear. Default values are in square brackets following the parameter name. A menu containing two entries appears.

19 To modify level 3 parameters, enter:

1 ↵

*Each of the level 3 parameters appears in turn. You can enter a value, or press **Return** to accept the default value.*

—continued—

Procedure 2-1 (continued)
Defining and enabling an X.25 configuration

Step **Action**

20 Respond to the prompts as required. To change the default value, enter a new value, then press **Return**. To accept the default value, press **Return**. For parameters that do not have a default, you must specify a value.

After you respond to all displayed parameters, the current values of all level 3 parameters are displayed, and a menu containing two entries appears.

21 To return to the menu shown in step 9, enter:

2 ↵

Creating the configuration file

22 To create the configuration file, enter:

6 ↵

The configuration file is created, the program terminates, and the Configure X.25 menu appears.

23 Enable X.25 by entering:

3 ↵

If your hardware configuration supports multiple OPC ports, a message prompting you to select a port appears.

```
Port Number (B, 1, 2, 3):
```

24 Select a port that is not already configured to enable X.25 on by entering:

<port #>

where

<port #> **B, 1, 2,** or **3**

A confirmation message appears.

```
X.25 operation is being configured on port x.
Do you wish to continue? (Yes/No):
```

25 Confirm by entering:

y ↵

The following message appears:

```
X.25 configuration successful on port x.
Insert the appropriate X.25 cable on port x.
```

The Configure X.25 menu appears after a short period.

—continued—

Procedure 2-1 (continued)
Defining and enabling an X.25 configuration

Step	**Action**

Configuring other services or exiting

26 You have defined X.25 parameters and enabled X.25. You can exit or continue defining other services.

If you want to	Then
configure another service (X.3 PAD, PPL (electronic software delivery), terminal, or printer)	Enter: **8** ↵ *The Configure a service menu appears.* Repeat this procedure for that device.
exit	Enter: **9** ↵ *The program ends and the UNIX prompt, opc>, appears.*

—end—

Procedure 2-2
Configuring an OPC port to support a VT-100 terminal

Use this procedure to configure an operations controller (OPC) port to support a VT-100 terminal.

Values specified using this procedure are permanent, unless changed again using this procedure. Values are retained during a kernel upgrade.

When you see the ↵ character, press Return.

> ***Note:*** To allow communication with the OPC, make sure the terminal configuration parameters are as follows: character length = 8 bits, parity = none.

Requirements

To do this procedure, you must complete the following:

- Obtain the root or admin userID and password.

Action

Step **Action**

1 You can continue a config_port session initiated in Procedure 2-1 on page 2-16. Or, if a config_port session is not running, you must start one.

If you are	Then go to
starting a config_port session	step 2
continuing from step 25 of Procedure 2-1 on page 2-16	step 6

2 Log in to the OPC.

If you do not know how to do this, see *User Interfaces Description*, 323-3001-301, in this volume.

If you are logging in as	Then
root	The UNIX prompt, opc>, appears. Enter the following command: **config_port** ↵
admin	The User Session Manager appears. Move to the Port Configuration tool, then press **Ctrl_A** (or Keypad **0**).

The Port Configuration main menu appears.

—continued—

Procedure 2-2 (continued)
Configuring an OPC port to support a VT-100 terminal

Step **Action**

3 Configure a service by entering:

2 ↵

The Configure a service menu appears.

1	Terminal
2	Printer
3	X.25
4	X.3 PAD
5	PPL
8	Return to Main menu
9	Exit

4 Configure a terminal by entering:

1 ↵

If your hardware configuration supports multiple OPC ports, you are prompted to select an unconfigured port.

For example: Port Number (B, 1, 3):

5 Select a port from the displayed options by entering:

<port #> ↵

where

<port #> **B**, **1**, or **3**

If you attempt to configure more than one port for terminal operation, the configuration operation fails and the following message appears:

```
Terminal operation is already configured on port x.
It is not possible to have more than one terminal
configured at any given time.
```

```
Port x remains configured as terminal.
```

If the configuration operation is successful, the following messages appear. The Configure a service menu appears after a short period.

```
Terminal operation is being configured on port x.
```

```
Do you wish to continue? (Yes/No): yes
```

```
Terminal configuration successful on port x.
Insert the appropriate cable on port x.
```

—continued—

Procedure 2-2 (continued)

Configuring an OPC port to support a VT-100 terminal

Step **Action**

The Configure a service menu appears.

1	Terminal
2	Printer
3	X.25
4	X.3 PAD
5	PPL
8	Return to Main menu
9	Exit

6 Select a service or exit.

If you want to	**Then go to**
configure an OPC port to support a VT100 terminal	go to Procedure 2-2 on page 2-24
configure an OPC port to support a printer	go to Procedure 2-3 on page 2-27
configure an OPC port to support X.3 communications	go to Procedure 2-4 on page 2-32
configure an OPC port to support PPL	go to Procedure 2-5 on page 2-43
exit	enter 9. *The UNIX prompt, opc>, appears.*

—end—

Procedure 2-3
Configuring an OPC port to support a printer

Use this procedure to configure an operations controller (OPC) port to support a printer. Two parameters, baud rate and mode, must be specified when you are configuring port 1 to support a printer. The specified values must be compatible with the selected printer, and its settings.

Baud rate

Baud rate is the speed at which characters are transmitted between the OPC and the printer. The speed at which a printer can accept characters is defined in the operating manual for that printer. A value within the range given in the manual must be selected from the possible port configuration values, which include 300, 1200, 2400, 4800, or 9600. This value must be specified in Procedure 2-2.

Mode

Mode indicates how the printer controls the flow of characters arriving from the OPC; that is, how the printer tells the OPC to stop sending characters, when it is temporarily unable to handle them. The serial interface section of the printer operating manual should define this capability.

If the printer supports both the digital terminal ready (DTR) and clear to send (CTS) control signals, then the port should be configured with Mode = simple. If the printer supports only the TX and RX signals, then OPC Port 1 must be configured with Mode = direct. In the latter case, you may have to select a hardware configuration in the printer. Use the DIP switch, located inside the printer, which must be positioned to select the XON/XOFF protocol.

Printer configuration

Table 2-3 lists the printer configuration you must use to communicate with the OPC, regardless of baud rate and mode:

Table 2-3
Required printer configuration

Interface	RS-232 serial
Character length	8 bits
Parity	none
Character set	Standard ASCII

Values specified using this procedure are permanent, unless changed again using this procedure. Values are retained during a kernel upgrade.

—continued—

When you see the ↵ character, press Return.

Requirements

To do this procedure, you must complete the following:

- Obtain the root or admin userID and password.

Action

Step **Action**

1 You can continue a config_port session initiated in Procedure 2-1 on page 2-16. Or, if a config_port session is not running, you must start one.

If you are	Then go to
starting a config_port session	step 2
continuing from step 25 of Procedure 2-1 on page 2-16	step 6

2 Log in to the OPC.

If you do not know how to do this, see *User Interfaces Description*, 323-3001-301, in this volume.

If you are logging in as	Then
root	The UNIX prompt, opc>, appears. Enter the following command: **config_port** ↵
admin	The User Session Manager appears. Move to the Port Configuration tool, then press **Ctrl_A** (or Keypad **0**).

The Port Configuration main menu appears

—continued—

Procedure 2-3 (continued)
Configuring an OPC port to support a printer

Step **Action**

3 Configure a service by entering:

2 ↵

The Configure a service menu appears.

1	Terminal
2	Printer
3	X.25
4	X.3 PAD
5	PPL
8	Return to Main menu
9	Exit

4 Configure a printer by entering:

2 ↵

If your hardware configuration supports multiple OPC ports, you are prompted to select an unconfigured port.

For example: Port Number (B, 1, 3):

5 Select a port from the displayed options by entering:

<port #> ↵

where

<port #> **B**, **1**, or **3**

The Baud rate menu appears.

1	300 baud
2	1200 baud
3	2400 baud
4	4800 baud
5	9600 baud
8	Return to Configure menu
9	Exit

—continued—

Procedure 2-3 (continued)
Configuring an OPC port to support a printer

Step **Action**

6 Select a baud rate from the menu by entering its corresponding number, then press **Return**.

The Printer Mode menu appears.

1	Simple
2	Direct
8	Return to Configure menu
9	Exit

7 Select a printer mode from the menu by entering its corresponding number, then press **Return**.

A confirmation message appears. If the port was already configured a warning message also appears to confirm the configuration operation.

8 If necessary, confirm the operation by entering **y** ↵.

The Configure a service menu appears after a short period.

```
Warning: Configuration on port 1 is changing from terminal
to printer.
Do you wish to continue? (Yes/No): yes
Terminal operation has been removed from port 1.
Printer configuration successful on port 1.
Insert the appropriate cable on port 1.
```

The Configure a service menu appears.

1	Terminal
2	Printer
3	X.25
4	X.3 PAD
5	PPL
8	Return to main menu
9	Exit

—continued—

Procedure 2-3 (continued)
Configuring an OPC port to support a printer

Step	**Action**
9	Select a service or exit.

If you want to	**Then go to**
configure an OPC port to support a VT100 terminal	go to Procedure 2-2 on page 2-24
configure an OPC port to support a printer	go to Procedure 2-3 on page 2-27
configure an OPC port to support X.3 communications	go to Procedure 2-4 on page 2-32
configure an OPC port to support PPL	go to Procedure 2-5 on page 2-43
exit	enter 9. *The UNIX prompt, opc>, appears.*

If the printer fails to operate

If you complete the port and printer configuration procedures and the printer does not print, do the following:

- Make sure the printer is plugged in and the power switch is turned on.
- Make sure the cable between the OPC and the printer is firmly connected.
- If the port is configured for mode simple, make sure the printer is enabled, by entering the following command at the opc> prompt while logged in as root. If the printer is configured on OPC port 1, enter **`/usr/bin/enable/ pr1`** ↵. If the printer is configured on port 3, enter **`/usr/bin/enable/ pr3`** ↵.

If characters are being dropped

If characters are not printing, you may be experiencing a flow control problem. To avoid this condition, do the following:

- Make sure flow control is enabled on your printer.
- Reduce the baud rate of the port, as specified in step 6 of Procedure 2-3 on page 2-30.
- Select draft print quality on your printer.

—end—

Procedure 2-4
Configuring an OPC port to support X.3 PAD

Use this procedure to configure an operations controller (OPC) port to support X.3 PAD.

Values specified using this procedure are permanent, unless changed again using this procedure. Values are retained during a kernel upgrade.

When you see the ↵ character, press Return.

> ***Note:*** To allow X.3 PAD and TL1 to share the same X.25 port, you must make sure the protocol identifier (PID) for each is unique. If the TL1 also uses a PAD, a unique PID cannot be assigned. X.3 PAD automatically uses the PID defined by international standards. The PID for TL1 can be defined using the OS Connection Manager, after which the OPC must be rebooted.

Requirements

To do this procedure, you must complete the following:

- Obtain the root or admin userID and password.

Action

Step	Action

1 You can continue a config_port session initiated in Procedure 2-1 on page 2-16. Or, if a config_port session is not running, you must start one.

If you are	Then go to
starting a config_port session	step 2
continuing from step 25 of Procedure 2-1 on page 2-16	step 4

2 Log in to the OPC.

—continued—

Procedure 2-4 (continued)
Configuring an OPC port to support X.3 PAD

Step **Action**

If you do not know how to do this, see *User Interfaces Description*, 323-3001-301, in this volume.

If you are logging in as	Then
root	The UNIX prompt, opc>, appears. Enter the following command: **config_port** ↵
admin	The User Session Manager appears. Move to the Port Configuration tool, then press **Ctrl_A** (or Keypad **0**).

The Port Configuration main menu appears.

3 Configure a service by entering:

2 ↵

The Configure a service menu appears.

1	Terminal
2	Printer
3	X.25
4	X.3 PAD
5	PPL
8	Return to Main menu
9	Exit

—continued—

Procedure 2-4 (continued)
Configuring an OPC port to support X.3 PAD

Step	Action

4 Configure X.3 PAD on a port already running X.25 by entering:

4 ↵

The Configure X.3 PAD support menu appears.

1	View/Modify parameters
2	Enable X.3 PAD support
8	Return to Configure menu
9	Exit

5 View and/or Modify X.3 PAD parameters by entering:

1↵

The View or Modify X.3 PAD Configuration menu appears.

1	Display the X.3 PAD configuration
2	Modify the X.3 PAD configuration
3	Save the X.3 PAD configuration after modify
8	Return to main menu
9	Exit

If you want to	Then go to
display X.3 PAD configuration	step 6
modify X.3 PAD configuration	step 8

6 Display X.3 PAD configuration parameters by entering:

1 ↵

The following list of parameters and their current values appear.

Note: If configured previously, configured values appear. If not, nothing appears.

—continued—

Procedure 2-4 (continued)

Configuring an OPC port to support X.3 PAD

Step **Action**

Table 2-4 lists the default values for X.3 parameters.

Table 2-4
Default values for X.3 parameters

X3 PARAMETERS		**CURRENT VALUE X.121= address**	
1	Escape from data transfer	0	(escape not allowed)
2	Echo	0	(Echo off)
3	Data forwarding character	94	(line) 127 (raw)
4	Idle timer delay	0	(line) 1 (raw)
5	Ancillary device control	1	(use X-ON & X-OFF)
6	PAD service signal	5	(use prompt PAD & PAD service signal)
7	Procedure on break	21	(TX interrupt & break indication, no output)
8	Discard output	0	(normal delivery)
9	Padding after return	0	(no padding)
10	Line folding	0	(no line folding)
11	Binary speed	14	(9600 bps)
12	Flow control of the PAD	1	(use X-ON & X-OFF)
13	Linefeed after RETURN	0	(no linefeed insertion)
14	Linefeed padding	0	(no padding after linefeed)
15	Editing	0	(no editing in data transfer)
16	Character delete	8	(Control H)
17	Line delete	21	(Control U)
18	Line display	18	(Control R)
19	Editing PAD service signal	2	(PAD service signal for display terminal)
20	Echo mask	0	(no echo mask)
21	Parity treatment	0	(no parity checking or generation)
22	Page wait	0	(disabled). <Press RETURN to continue.>

—continued—

Procedure 2-4 (continued)
Configuring an OPC port to support X.3 PAD

Step **Action**

7 Exit the display by pressing **Return**.

8 Modify an X.3 PAD configuration by entering:

2 ↵

The Modify X.3 PAD Configuration menu appears.

1	Add a new X.121 address
2	Modify X.3 parameters for an existing X.121 address
3	Delete an X.121 address
8	Return to previous menu
9	Exit

9 Select an operation.

If you want to	**Then go to**
add a new X.121 address	step 10
modify X.3 parameters (for an existing X.121 address)	step 12
delete an X.121 address	step 21
save your modifications	step 24

Adding a new X.121 address

10 Add a new X.121 address by entering:

1 ↵

The following message and address prompt appear.

```
The X.121 address is made up of up to 14 digits (0-9); an
optional wildcard character, '?', may be used to match one
or more unspecified characters. Entering just a '?' for
the address allows any X.121 address to connect to the
OPC.
Enter the X.121 address ('q' to return to menu):
```

—continued—

Procedure 2-4 (continued)
Configuring an OPC port to support X.3 PAD

Step **Action**

11 Enter the new X.121 address, then press **Return**.

The following prompt appears.

```
Do you wish to modify the default X.3 parameters for this
address (yes/no)?
```

If you	**Then go to**
want to modify X.3 parameters of an existing X.121 address	Enter **2** ↵ *A list of current X.121 addresses appears.* Go to step 12.
want to modify X.3 parameters of a new address	Enter: **y** ↵ *A subset of X.3 parameters, which can be modified, appears.* Go to step 13.
do not want to modify X.3 parameters	Go to step 19.

Modifying an X.121 address

12 Enter the X.121 address to modify.

A list of X.3 parameter values appears.

13 Enter the number of the parameter to be changed.

A prompt appears for the new value.

14 Enter the new value.

15 Repeat steps 13 and 14 to change additional parameters.

16 When all changes have been made, exit the list by pressing the q key.

You are prompted to enter another X.121 address.

17 To enter another address, then go to step 11. Otherwise, go to step 18.

18 Return to the Modify X.3 PAD Configuration menu by entering:

q ↵

Go to step 9.

—continued—

Procedure 2-4 (continued)
Configuring an OPC port to support X.3 PAD

Step **Action**

19 Reject the prompt by entering:

n ↵

The following message appears:

```
The new X.121=1234567890 has been added to the X.3 PAD
configuration.
The X.121 address is made up of up to 14 digits (0-9); an
optional wildcard character, ‘?’, may be used to match one
or more unspecified characters. Entering just a ‘?’ for
the address allows any X.121 address to connect to the
OPC.
```

```
Enter the X.121 address (‘q’ to return to menu):
```

To enter additional addresses repeat steps 11 to 18.

20 Return to the Modify X.3 PAD Configuration menu by entering:

q ↵

Deleting an X.121 address

21 Delete an X.121 address by entering:

3 ↵

The following prompt appears.

```
Enter the X.121 address to delete (‘q’ to return to menu):
```

22 Enter the X.121 address you want to delete, then press **Return**.

To delete more addresses, repeat steps 21-22.

23 To return to the Modify X.3 PAD Configuration menu, enter:

8 ↵

Saving your modifications

24 To save the modifications to the X.3 PAD configuration, enter:

3↵

The following prompt appears.

```
X.3 PAD configuring has been saved.
```

—continued—

Procedure 2-4 (continued)
Configuring an OPC port to support X.3 PAD

Step **Action**

25 Return to the Configure X.3 PAD menu by entering:

8 ↵

The X.3 PAD menu appears.

If this configuration is	Then go to
a modification to an existing X.3 PAD configuration	Procedure 2-7 on page 2-59
the initial X.3 PAD configuration	step 26

Enabling X.3 PAD support

26 Enable X.3 PAD support by entering:

2 ↵

The following warning message and prompt appear.

```
Warning: In order for X.3 PAD and TL1 to share the X.25
connection, TL1 must be configured to use an X.25
‘protocol-id’. Please check the Northern Telecom
documentation for the proper procedures on configuring
TL1.

Do you wish to continue? (Yes/No):
```

27 Confirm by entering:

y ↵

The following message, and the Configure X.3 PAD support menu appears.

```
X.3 PAD configuration successful.
```

1	View/Modify parameters
2	Enable X.3 PAD support
8	Return to Configure menu
9	Exit

Note: If configuration fails, check the error message. If the error is TL1-related, exit and correct the error.

—continued—

Procedure 2-4 (continued)

Configuring an OPC port to support X.3 PAD

Step **Action**

28 Return to the Configure menu by entering:

8 ↵

The Configure a service menu appears.

1	Terminal
2	Printer
3	X.25
4	X.3 PAD
5	PPL
8	Return to Main menu
9	Exit

Go to step 9.

Configuring PPL

29 Configure electronic software delivery (PPL) over a port configured for a terminal. Determine if a port is configured for a terminal by displaying the Port Configuration main menu to see which port is configured as a terminal. Enter:

1↵

If a port is	**Then go to**
not configured for terminal	step 30
configured for terminal	Procedure 2-5 on page 2-43

30 Configure a terminal by entering:

1 ↵

If your hardware configuration supports multiple OPC ports you are prompted to select an unconfigured port.

For example: Port Number (B, 1, 3):

—continued—

Procedure 2-4 (continued)

Configuring an OPC port to support X.3 PAD

Step **Action**

31 Select a port from the displayed options by entering:

<port #> ↵

where

<port #> **B**, **1**, or **3**

If you attempt to configure more than one port for terminal operation, the configuration operation fails and the following message appears:

```
Terminal operation is already configured on port x.
It is not possible to have more than one terminal
configured at any given time.

Port x remains configured as terminal
```

If the configuration operation is successful, the following messages appear. The Configure a service menu appears after a short period.

```
Terminal operation is being configured on port x.

Do you wish to continue? (Yes/No): yes

Terminal configuration successful on port x.
Insert the appropriate cable on port x.
```

The Configure a service menu appears.

1	Terminal
2	Printer
3	X.25
4	X.3 PAD
5	PPL
8	Return to Main menu
9	Exit

32 Attach the modem to the specified port (B, 1, or 3) using the cable identified in Procedure 2-9, “Connecting the cable” on page 2-64. The modem must be preconfigured for 9600 baud, and able to use the AT command set. See Procedure 2-9 on page 2-64 for details.

—continued—

Procedure 2-4 (continued)
Configuring an OPC port to support X.3 PAD

Step	Action
33	Select a service or exit.

If you want to	Then go to
configure an OPC port to support a VT100 terminal	go to Procedure 2-2 on page 2-24
configure an OPC port to support a printer	go to Procedure 2-3 on page 2-27
configure an OPC port to support X.3 communications	go to Procedure 2-4 on page 2-32
configure an OPC port to support PPL	go to Procedure 2-5 on page 2-43
exit	enter 9. *The UNIX prompt, opc>, appears.*

—end—

Procedure 2-5
Configuring an OPC port to support electronic software delivery (PPL connection)

Use this procedure to configure an operations controller (OPC) port to support electronic software delivery, referred to as PPL (point-to-point link).

> ***Note:*** This procedure must be performed before the electronic software delivery transfer operation (see *Commissioning and Testing*, Volume 3) can be completed.

Values specified using this procedure are permanent, unless changed again using this procedure. Values are retained during a kernel upgrade.

When you see the ↵ character, press Return.

Requirements

To do this procedure, you must complete the following:

- Obtain the root or admin userID and password.

Action

Step	Action
1	You can continue a config_port session initiated in Procedure 2-1 on page 2-16. Or, if a config_port session is not running, you must start one.

If you are	Then go to
starting a config_port session	step 2
continuing from step 25 of Procedure 2-1 on page 2-16	step 3

Step	Action
2	Log in to the OPC.

—continued—

Procedure 2-5 (continued)
Configuring an OPC port to support electronic software delivery (PPL connection)

Step **Action**

If you do not know how to do this, see *User Interfaces Description*, 323-3001-301, in this volume.

If you are logging in as	**Then**
root	The UNIX prompt, opc>, appears. Enter the following command: **config_port** ↵
admin	The User Session Manager appears. Move to the Port Configuration tool, then press **Ctrl_A** (or Keypad **0**).

The Port Configuration main menu appears.

3 Configure a service by entering:

2 ↵

The Configure a service menu appears.

1	Terminal
2	Printer
3	X.25
4	X.3 PAD
5	PPL
8	Return to Main menu
9	Exit

—continued—

Procedure 2-5 (continued)

Configuring an OPC port to support electronic software delivery (PPL connection)

Step **Action**

4 Configure electronic software delivery (PPL) by entering:

5 ↵

The Configure PPL Support menu appears.

1	View parameters
2	Modify parameters
3	Enable PPL login
4	Enable and Dial-out to PPL host
8	Return to Configure menu
9	Exit

5 Select an operation.

If you want to	Then go to
view parameters	step 6
modify parameters	step 7
enable PPL login	step 20
enable and dial-out to PPL host	step 24
exit	enter 9. *The UNIX prompt, opc>, appears.*

—continued—

Procedure 2-5 (continued)
Configuring an OPC port to support electronic software delivery (PPL connection)

Step Action

Viewing parameters

6 View parameters by entering:

1 ↵

If PPL parameters are not defined, the following message appears:

```
Parsing /usr/lib/ppl/ppl.remotes file.
No PPL hosts defined.
Press Return to continue.
```

If PPL parameters are defined, the parameters are displayed similar to the following:

```
Remote Host     Local Host     Type       Phone Number
bmerha02        slat6          DIALIN     #
```

If PPL parameters	Then go to
have not been defined	step 7
are not correct	step 7
are correct	step 20

Modifying parameters

7 Modify parameters by entering:

2 ↵

The Modify PPL Configuration menu appears.

1	Add a new PPL host
2	Modify an existing PPL host
3	Delete a PPL host
4	Edit /usr/lib/ppl/ppl.remotes file
8	Return to previous menu
9	Exit

8 Determine what you want to do from the following table.

If you want to	Then go to
add a new PPL host	step 9
modify an existing PPL host	step 10

—continued—

Procedure 2-5 (continued)
Configuring an OPC port to support electronic software delivery (PPL connection)

Step **Action**

Adding a new PPL host

9 Add a new PPL host by entering:

1 ↵

The Add a PPL host screen appears.

```
Add a PPL host:
Enter remote hostname ():
Enter remote SLIP address ():
Enter local hostname ():
Enter local SLIP address (47.35.15.9):
Enter network mask (255.255.255.0):
The possible connection types are
1 DIALIN
2 DIALOUT
3 DIALIN & DIALOUT
4 DIRECT
Enter connection type (1):
Enter phone number of the remote site ():
```

Go to step 12.

Modifying an existing PPL host

10 Modify an existing PPL host by entering:

2 ↵

The following prompt to select the PPL host to modify appears:

```
Modify PPL host entry:
The following hosts have been defined:
host 02, host 03
Enter remote host to modify ():
```

—continued—

Procedure 2-5 (continued)
Configuring an OPC port to support electronic software delivery (PPL connection)

Step **Action**

Modifying an existing PPL host

11 Enter the PPL host that requires modification and press Return key.

The Modify PPL host entry screen appears.

```
Modify PPL host entry:
Enter remote hostname (bmerha02):
Enter remote SLIP address (47.45.4.39):
Enter local hostname (slat6):
Enter local SLIP address (47.35.15.9):
Enter network mask (255.255.255.0):
The possible connection types are
1 DIALIN
2 DIALOUT
3 DIALIN & DIALOUT
4 DIRECT
Enter connection type (1):
Enter phone number of the remote site ():
```

12 If necessary, enter the remote host name, press **Return**. Otherwise, to accept the displayed value, press **Return** only.

13 Enter the remote SLIP address, press **Return**. Otherwise, to accept the displayed value, press **Return** only.

14 Enter the local host name, press **Return**. Otherwise, to accept the displayed value, press **Return** only.

15 Enter the local SLIP address, press **Return**. Otherwise, to accept the displayed value, press **Return** only.

16 Enter the network mask, press **Return**. Otherwise, to accept the displayed value, press **Return** only.

17 Enter the connection type, press **Return**. Otherwise, to accept the displayed value, press **Return** only.

If the connection type is	**Then**
Dial-out	Enter the phone number of the remote site and press **Return**. Go to step 18. *The configuration parameter appears and you are prompted to confirm the data.*
other than Dial-out	*The configuration parameter appears and you are prompted to confirm the data.* Go to step 18.

—continued—

Procedure 2-5 (continued)
Configuring an OPC port to support electronic software delivery (PPL connection)

Step **Action**

18 Confirm the data by entering:

y ↵

*If the data is incorrect, enter **n**, then press **Return**.*

A list of configuration entries appear followed by the Modify PPL Configuration menu. The newly defined entry should appear.

19 Return to the Configure menu by entering:

8 ↵

Enabling PPL login parameters

20 Enable the PPL host.

If the host is	Then go to
Dial-in	step 21
Dial-out	step 24

21 Enable PPL Dial-in by entering:

3 ↵

Enable PPL login:

A prompt to select a port appears. If the selected port is already configured, the following statement appears: “X operation is already configured on port a. It is not possible to have more than one X configured at any given time.” Select a different port.

```
The following hosts have been defined for DIALIN:
bmerha02
Which host is allowed to login ():
```

22 Enter the name of the host you want to enable.

A prompt for password appears.

```
Processing...
Creating user ‘ppl1’...
Please choose a new password for the PPL user:
New password:
```

23 Enter the password, up to 8 characters, that the remote terminal user must use to log in to the OPC, then press **Return**. Confirm the password by entering it again and pressing **Return**.

A message confirms that PPL dial-in has been enabled. The Configure PPL support menu re-appears.

—continued—

Procedure 2-5 (continued)
Configuring an OPC port to support electronic software delivery (PPL connection)

Step **Action**

```
Creating PPL login script...
Done. PPL login has been enabled.

PPL configuration successful on port x.
```

Configure PPL support:

1	View parameters
2	Modify parameters
3	Enable PPL login
4	Enable and Dial-out to PPL host
8	Return to Configure menu
9	Exit

Go to step 5.

Enabling and dialing out to PPL host

24 Enable PPL dial-out and initiate a dial-out session with the remote host by entering:

4 ↵

Note: Enable a dial-out session when you want to access a remote terminal to deliver PPL software.

You are prompted to select a dial-out host.

```
Dial-out to PPL host:

The following hosts have been defined for DIALOUT:

bmerha02

Dial-out to which host ():
```

—continued—

Procedure 2-5 (continued)

Configuring an OPC port to support electronic software delivery (PPL connection)

Step **Action**

25 Enter the name of the remote host you want to enable.

The SLIP connection is established with the specified host.

```
Processing...
Dialing...
Done. SLIP CONNECTION ESTABLISHED. ^G^G

Press Return to continue:

PPL configuration successful on port x.
```

26 Exit by entering:

9 ↵

The UNIX prompt, opc>, appears.

—end—

Procedure 2-6
Configuring a modem for electronic software delivery (PPL connection)

Use this procedure to configure and connect a Microcom QX communications modem to an operations controller (OPC) and Hewlett Packard (HP) workstation for electronic software delivery. In this document, electronic software delivery is referred to as PPL (point-to-point link).

Equipment

You need the following equipment for this procedure:

- 9600 baud modem
- telephone line for a modem
- modem-to-serial port cable for your workstation
- workstation

Action

Step **Action**

1 Remove the front faceplate of the modem and set the front DIP switches as listed in Table 2-5.

Table 2-5
Settings for front DIP switches

Switch	Position	Description
1	Up	DTR on, mode 2
2, 3	Down, Up	AT command mode
4	Up	Echo on
5	Up	Auto answer on
6, 7	Up,Up	CD, DTR on
8	Down	Smart mode
9	see note	n/c
10	Up	Asynchronous mode
Note: Switch 9 is not connected. A setting is not required.		

—continued—

Procedure 2-6 (continued)
Configuring a modem for electronic software delivery (PPL connection)

Step **Action**

2 Set the rear DIP switches of the modem as listed in Table 2-6.

Table 2-6
Settings for rear DIP switches

Switch	Position	Description
1, 2	Up,Up	No hardware flow control
3,4	Down,Up	Auto-reliable
5	Down	MNP result codes
6	Up	Use software configuration
7	Up	Don't read switch configuration
8	Down	BPS adjust off

3 Determine whether the modem will be used for PPL Dial-out or for PPL Dial-in.

If you are configuring for	Then go to
PPL Dial-out	step 4
PPL Dial-in	step 5

—continued—

Procedure 2-6 (continued)
Configuring a modem for electronic software delivery (PPL connection)

Step	Action
4	Connect a VT100 terminal to the modem and issue the following AT commands in the order listed in Table 2-7.

Table 2-7
AT commands for PPL dial-out

Command	Description
AT&F	Return to factory settings
AT\G1	Software flow control
AT\N3	Auto-reliable mode
AT\J0	BPS adjust off
AT\Q0	Hardware flow control off
AT&D2	DTR on, mode 2
AT&C1	CD on, mode 1
ATQ0	Quiet mode off
AT&W	Save configuration

Note: The dial-out modem should have the front panel switch set to originate mode.

If you are connecting to	Then go to
the OPC	step 6
HP400	step 7
HP700	step 8

—continued—

Procedure 2-6 (continued)
Configuring a modem for electronic software delivery (PPL connection)

Step	Action
5	Connect a VT100 terminal to the modem and issue the following AT commands in the order listed in Table 2-8.

Table 2-8
AT commands for PPL dial-in

Command	Description
AT&F	Return to factory settings
AT\G1	Software flow control
AT\N3	Auto-reliable mode
AT\J0	BPS adjust off
AT\Q0	Hardware flow control off
AT&D2	DTR on, mode 2
AT&C1	CD on, mode 1
ATS0=1	Answer mode on
ATQ1	Quiet mode on
AT&W	Save configuration

Note 1: The dial-in modem should have the front panel switch set to answer mode if used on leased lines.

Note 2: After the ATQ1 command is issued, the modem still accepts commands, but no longer responds with OK or other result codes.

If you are connecting to	Then go to
the OPC	step 6
HP400	step 7
HP700	step 8

—continued—

Procedure 2-6 (continued)
Configuring a modem for electronic software delivery (PPL connection)

Step	Action
6	Wire the modem-to-port B (OPC Port 1) cable as listed in Table 2-9. The cable should have a DB-9M connector for the OPC Port 1 (DTE) end, and a DB-25M connector for the modem (DCE) end.

Table 2-9
Wiring for modem-to-port B cable

OPC Port 1 Signal	OPC Port 1 pin assignment	Modem Pin Assignment
DCD	1	8
Rx	2	3
Tx	3	2
DTR	4	20
GND	5	7
DSR	6	6
RTS	7 (see note)	4
CTS	8 (see note)	5
n/c	9	
Note: Pins 7 and 8 on OPC Port 1 can be shorted together instead of wiring to modem pins 4 and 5 if hardware flow control is not absolutely required.		

If you are connecting to	Then go to
HP400	step 7
HP700	step 8

—continued—

Procedure 2-6 (continued)
Configuring a modem for electronic software delivery (PPL connection)

Step	Action
7	Wire the modem-to-HP400 cable as listed in Table 2-10. The cable should have a DB-25M connector for both the HP400 (DTE) and for the modem (DCE) end.

Table 2-10
Wiring for modem-to-HP400 cable

HP400 signal	HP400 pin assignment	Modem pin assignment
Rx	3	3
Tx	2	2
GND	7	7
DTR	20	20
DSR	6	6
RTS	4 (see note)	4
CTS	5 (see note)	5
DCD	8	8
RI	22	22
Note: Pins 4 and 5 on the HP400 can be shorted together instead of wiring to modem pins 4 and 5 if hardware flow control is not absolutely required.		

—continued—

Procedure 2-6 (continued)
Configuring a modem for electronic software delivery (PPL connection)

Step	**Action**
8	Wire the modem-to-HP700 cable as listed in Table 2-11. The cable should have a DB-9M connector for the HP700 (DTE) end and a DB-25M connector for the modem (DCE) end.

Table 2-11
Wiring for modem-to-HP700 cable

HP700 Signal	**HP700 Pin Assignment**	**Modem Pin Assignment**
DCD	1	8
Rx	2	3
Tx	3	2
GND	5	7
DTR	4	20
DSR	6	6
RTS	7 (see note)	4
CTS	8 (see note)	5
RI	9	22

Note: Pins 7 and 8 on the HP700 can be shorted together instead of wiring to modem pins 4 and 5 if hardware flow control is not absolutely required.

—end—

Procedure 2-7
Unconfiguring an OPC port

Use this procedure to unconfigure any operations controller (OPC) service.

For example, use this procedure in the following situations:

- to change X.3 PAD parameters (see the task table on page 2-8)
- to unconfigure X.3 PAD if the TL1 PID is set to zero (or null)
- to remove service from a port

Note 1: You cannot change the configuration of the port used to log in.

Note 2: Unconfiguring a port terminates without warning any user sessions currently logged in through X.3 PAD.

Requirements

To do this procedure, you must complete the following requirements:

- Obtain the root password or admin userID and password.

Action

Step **Action**

Display the OPC port configuration

1 Log in to the OPC.

If you do not know how to do this, see the procedures in *User Interfaces Description*, 323-3001-301, in this volume.

If you are logging in as	Then
root	*The UNIX prompt, opc>, appears. Enter the following command:* **config_port**
admin	*The User Session Manager appears. Move to the Port Configuration tool, then press **Ctrl_A** (or Keypad **0**).*

The Port Configuration main menu appears.

2 To display OPC port configuration, enter:

1 ↵

The port configurations appear. If ports 2 and 3 are available, these ports are listed.

3 Record the port configurations, then press **Enter** to return to the main menu.

—continued—

Procedure 2-7 (continued)
Unconfiguring an OPC port

Step **Action**

Unconfigure a service and X.25

4 Unconfigure a service by entering:

3 ↵

The Unconfigure a service menu appears.

This menu is customized for the services you have configured. In the following example, only X.25, PPL, and X.3 PAD are configured.

1	X.25 on Port 1
3	PPL
4	X.3 PAD
8	Return to Main menu
9	Exit

5 Enter the number that corresponds to the menu item you want to unconfigure, then press **Return**. X.3 PAD services must be unconfigured before X.25 can be unconfigured, and PPL services must be unconfigured before a terminal can be unconfigured.

If the service you are deconfiguring is X.3 PAD, the following warning appears.

```
Warning: Unconfiguring X.3 PAD will terminate any login
sessions currently logged in through X.3 PAD.
```

```
Do you wish to continue? (Yes/No): yes
```

6 Confirm by entering **y** and pressing **Return**.

The system confirms the removal of the service. Any user sessions logged in using X.3 PAD are terminated without warning.

If the service you are deconfiguring is X.25, the following warning appears.

```
Warning: X.25 operation is being removed from port ___.
```

```
Do you wish to continue? (Yes/No): yes
```

7 Confirm by entering **y** and pressing **Return**.

The system confirms the removal of the service. Any user sessions logged in using X.25 are terminated without warning.

The Unconfigure a service menu appears after a short period of time.

8 Repeat steps 5 through 7 for each service you want to unconfigure.

9 Exit by entering:

9 ↵

The UNIX prompt, opc>, appears.

—end—

Procedure 2-8
Managing virtual circuit profiles

Use this procedure to manage virtual circuit profiles. Virtual circuits must be defined to support the TL1 protocol. Profiles can be added, removed, or listed.

Requirements

To do this procedure, you must complete the following requirements:

- Obtain the root userID and password.
- Determine the remote address of the virtual circuit profile you are adding or removing.

Action

Step	Action
1	Log in to the operations controller (OPC) as the root user through a network element user interface (NE UI) or telnet. ***Note:*** The config_port application cannot be run on OPC Port 1. It has to be run remotely (NE or telnet). If you do not know how to do this, see the procedures in *Network Element User Interface Description*, 323-3001-300, in this volume. *The UNIX prompt, opc>, appears.*
2	Enter the following command: **cd /iws/vcp** ↵ *The UNIX prompt, opc>, appears.*

—continued—

Procedure 2-8 (continued)
Managing virtual circuit profiles

Step	Action
3	The vcpinfo command supports all of the virtual circuit profile management functions. Determine what you want to do from the left column in the following table. Then perform the actions in the right column.

If you want to	Then
list all existing virtual circuit profiles	Enter: **vcpinfo -l** *A list of virtual circuit profiles and the TL1 protocol identifier appears.*
add a new virtual circuit profile	Enter: **vcpinfo -a <Remote Address> <oss type>**↵ where: <Remote Address> is a decimal number from 1 to 16 digits. The form of the Remote Address can be seen by listing existing virtual circuit profiles. <loss type> **NMA** or **OPS** or **BTH** *A new virtual circuit profile is created.*
remove an existing virtual circuit profile	Enter: **vcpinfo -d <Remote Address> <oss type>**↵ where: <Remote Address> is a decimal number from 1 to 16 digits. The form of the Remote Address can be seen by listing existing virtual circuit profiles. <oss type> **NMA** or **OPS** or **BTH** *The specified virtual circuit profile is removed and no longer appears when the list appears.*
define a protocol ID for TL1 requests	Enter: **vcpinfo -p <protocol ID>** ↵ where: <protocol ID> is a hexadecimal number from 1 to 16 digits *A protocol identifier for TL1 requests is defined.* If an OPC port is configured to support X.3 PAD, set the protocol identifier for TL1 requests to other than null or 01.
view help information	Enter: **vcpinfo -h** ↵ *Help text appears.*

—continued—

Procedure 2-8 (continued)
Managing virtual circuit profiles

Step	Action
4	To exit the UNIX shell, enter: **exit** ↵ *The UNIX shell closes.*

—end—

Procedure 2-9
Connecting the cable

Use this procedure to connect the cable between port 1 (B), port 2, and port 3 and the communications modem, printer, or terminal.

The cable required depends on the device supported, as listed in the following tables:

If you are connecting port 1 (B) to	Then use part number
X.25 modem	NT7E44QA or QB
printer	NT7E44RA or RB
terminal	NT7E44RA or RB
modem for remote printer or terminal	NT7E44EA or EB

If you are connecting port 2 to	Then use a custom
X.25 modem	EIA-530, 25-pin cable

If you are connecting port 3 to	Then use part number
X.25 modem	NT7E44TA or TB
printer	NT7E44VA or VB
terminal	NT7E44VA or VB
modem for remote printer or terminal	NT7E44TA or TB

Requirements

Before starting this procedure, you must do the following:

- Complete the tasks listed in the chapter task list for the device you are connecting to operations controller (OPC) port 1 (B), port 2, or port 3.
- Obtain the correct cable.

Action

Step	Action
1	Connect the 9-pin end of the designated port 1 (B) cable to port 1 (B) (connector J07 on the network element frame), or the 25-pin end of the designated port 2 or 3 cable to port 2 or 3.
2	Connect the 25-pin end of the cable to the X.25 modem, printer, or terminal.
3	Make sure the connections are secure.

—end—

Procedure 2-10
Configuring the TL1 Interface Router Service over X.25

Use this procedure to configure and enable the TL1 Interface Router Service.

A TL1 Interface Router Service routes TL1 messages to up to four spans of control that are connected with

- optical tributaries
- Ethernet
- CNET

Use the primary router service to route TL1 messages to a remote primary operations controller (OPC) span of control. Use the backup router service to route TL1 messages to a remote backup OPC span of control.

Requirements

Before you start this procedure

- Obtain the root password or admin userID and password.
- Configure port 1 of the gateway OPC for X.25. Refer to Procedure 2-1 on page 2-16.
- Determine and provision the X.121 address of the operations system into the virtual circuit profile of both the gateway OPC containing the TL1 Interface Router Service configuration, and into the remote OPCs. Refer to Procedure 2-8 on page 2-61.
- Determine the X.121 address and protocol id (PID) used for the operations system connected to the OPC over an X.25 link.

—continued—

Procedure 2-10 (continued)
Configuring the TL1 Interface Router Service over X.25

Action

Step	Action

1 Log in to the OPC.

If you do not know how to do this, see the procedures in *User Interfaces Description*, 323-3001-301, in this volume.

If you are logging in as	Then
root	*The UNIX prompt, opc>, appears. Enter the following command:* **config_tl1**
admin	*The User Session Manager appears. Move to the TL1 Configuration tool, then press **Ctrl_A** (or Keypad **0**).*

The TL1 Configuration tool Main Menu appears.

2 Configure the TL1 Interface Router Service. Enter:

6 ↵

The TL1 Interface Router Services Configuration menu appears.

3 Configure TIRS over X.25 by entering:

1 ↵

The TL1 Interface Router Services over X.25 main menu appears.

4 Choose an action from the following table:

If you want to	Then enter
configure the primary router service	**1** ↵ and go to step 5
configure the backup router service	**2** ↵ and go to step 5
return to the main menu	**8** ↵
exit the TL1 Configuration tool	**9** ↵

—continued—

Procedure 2-10 (continued)
Configuring the TL1 Interface Router Service over X.25

Step **Action**

5 Choose an action from the following table:

If you want to	Then
configure the TL1 router protocol identifier (PID)	go to step 6
configure the TL1 router service	go to step 9
enable the TL1 router	enter **3** ↵
disable the TL1 router	enter **4** ↵
list the TL1 router service configuration	enter **5** ↵
list the TL1 router PID configuration	enter **6** ↵
add a span of control to an existing TL1 router configuration	enter **7** ↵ and go to step 15
add a target identifier (TID) to an existing TL1 router configuration	enter **7** ↵ and go to step 22
delete a SOC from an existing TL1 router configuration	enter **7** ↵ and go to step 26
delete a TID from an existing TL1 router configuration	enter **7** ↵ and go to step 31
edit the PID of an existing router configuration	enter **7** ↵ and go to step 36
return to the main menu	enter **8** ↵
exit	enter **9** ↵

Configure the TL1 router PID

6 Configure the TL1 router PID by entering:

1 ↵

A message similar to the following appears:

```
Enter the number of bytes for X.25 protocol id of TL1
Primary Router Service:
```

7 Type the number of bytes for the PID and press Enter:

↵

A message similar to the following appears:

```
Enter the X.25 protocol id for TL1 Primary Router:
```

—continued—

Procedure 2-10 (continued)
Configuring the TL1 Interface Router Service over X.25

Step **Action**

8 Type the X.25 protocol ID and press Enter:

↵

A message appears, indicating that the PID was configured. When it finishes, the TL1 Router Configuration menu appears again.

Go to step 5.

Configure the TL1 router service

9 Begin the TL1 router configuration. Enter:

2 ↵

A message similar to the following appears:

```
Enter the RemoteOPCName for TL1 Interface Primary Router
Service (END):
```

10 Type the remote OPC name in the form OPCxxxxP for primary router or OPCxxxxB for backup router and press Enter:

↵

A message similar to the following appears:

```
Enter the TID for TL1 Interface Primary Router Service
(END):
```

11 Type a TID for this OPC span of control and press Enter:

↵

12 Repeat step 11 until you have entered all the TIDs for this OPC, then enter:

end ↵

A message similar to the following appears again:

```
Enter the RemoteOPCName for TL1 Interface Primary Router
Service (END):
```

13 If you want to enter another remote OPC name and the TIDs in its span of control, then go to step 10. Otherwise, enter:

end ↵

A message similar to the following appears:

```
The TL1 Primary Router Configuration you have configured:

     The RemoteOPC:OPC4801P
          TheTargetIDentifier:4801
          TheTargetIDentifier:4802

Do you wish to Update the Configuration? (Yes/No):
```

—continued—

Procedure 2-10 (continued)
Configuring the TL1 Interface Router Service over X.25

Step **Action**

14 Update the configuration. Enter:

yes ↵

A message appears, indicating that the configuration is being updated. When it finishes, the TL1 Router Configuration menu appears again.

Go to step 5.

Add a SOC to an existing TL1 router configuration

15 Add a SOC to an existing router configuration. Enter:

1 ↵

A message similar to the following appears:

```
Enter the RemoteOPCName for TL1 Interface Primary Router
Service(END):
```

16 Type the RemoteOPCName for the router service and press Enter:

↵

A message similar to the following appears:

```
Enter the TID for TL1 Interface Primary Router Service
(END):
```

17 Type the TID and press Enter:

↵

A message similar to the following appears:

```
Enter the TID for TL1 Interface Primary Router Service
(END):
```

18 If you have other TIDS to enter for this remote OPC name, go to step 17. Otherwise, enter:

end ↵

The following message appears again:

```
Enter the RemoteOPCName for TL1 Interface Primary Router
Service (END):
```

—continued—

Procedure 2-10 (continued)
Configuring the TL1 Interface Router Service over X.25

Step **Action**

19 If you have other remote OPC names to enter, go to step 16. If you have no other remote OPC names to enter, enter:

end ↵

A message similar to the following appears:

```
The SOCs added are

The RemoteOPC : opc9257P
                The TIDs added : TIDNAME1

Do you wish to continue? (YES/NO):
```

20 Update the configuration by entering:

yes ↵

The Modify Router Configuration menu appears again.

21 Return to the TL1 Router Configuration over X.25 menu by entering:

8 ↵

The TL1 Router Configuration over X.25 menu appears again.

Go to step 5.

Add a TID to an existing TL1 router configuration

22 Add a TID to an existing router configuration. Enter:

2 ↵

A message similar to the following appears:

```
Enter the RemoteOPCName to which you want to add TID for
TL1 Interface Primary Router Service (END):
```

23 Type the remote OPC name where you want to add TIDs and press Enter:

↵

A message similar to the following appears:

```
Enter the TID for TL1 Interface Primary Router
Service(END):
```

24 Type the TID for the TL1 Interface Router Service and press Enter:

↵

A message appears, indicating that the configuration is being updated. When it finishes, the Modify Router Configuration menu appears again.

25 Return to the TL1 Router Configuration over X.25 menu by entering:

8 ↵

The TL1 Router Configuration menu appears again.

Go to step 5.

—continued—

Procedure 2-10 (continued)
Configuring the TL1 Interface Router Service over X.25

Step **Action**

Delete a SOC from an existing TL1 router configuration

26 To delete a SOC from an existing TL1 router configuration, enter:

3 ↵

A message similar to the following appears:

```
Enter the RemoteOPCName for TL1 Interface Primary Router
Service (END):
```

27 Type the remote OPC name and press Enter:

↵

A message similar to the following appears:

```
Enter the RemoteOPCName for TL1 Interface Primary Router
Service(END):
```

28 If you have other remote OPC names to delete, go to step 27. Otherwise, enter:

end ↵

A message similar to the following appears:

```
The Remote OPC : OPC4801P
                 The TIDs deleted : TIDNAME

Do you wish to continue? (YES/NO):
```

29 Update the configuration by entering:

yes ↵

The Modify Router Configuration menu appears again.

30 Return to the TL1 Router Configuration over X.25 menu by entering:

8 ↵

The TL1 Router Configuration over X.25 menu appears again.

Go to step 5.

Delete a TID from an existing TL1 router configuration

31 To delete a TID from an existing TL1 router configuration, enter:

4 ↵

A message similar to the following appears:

```
Enter the TID to be removed from the Primary Router
Service(End):
```

32 Type the TID you want to delete and press Enter:

↵

—continued—

Procedure 2-10 (continued)
Configuring the TL1 Interface Router Service over X.25

Step Action

Delete a TID from an existing TL1 Router Configuration

33 If you want to delete more TIDs, go to step 32. Otherwise, enter:

end ↵

A message similar to the following appears:

```
The Remote OPC : OPC4801P
                The TIDs deleted : TIDNAME

Do you wish to continue? (YES/NO)
```

34 Enter:

yes ↵

The Modify Router Configuration menu appears again.

35 Return to the TL1 Router Configuration over X.25 menu by entering:

8 ↵

Go to step 5.

Edit the PID of an existing router configuration

36 To edit the PID of an existing router configuration, begin the TL1 router configuration. Enter:

1 ↵

A message similar to the following appears:

```
Enter the number of bytes for X.25 protocol id of TL1
router:
```

37 Type the number of bytes (up to eight) and press Enter:

↵

A message similar to the following appears:

```
Enter the X.25 protocol id for TL1 Primary Router:
```

38 Type the X.25 protocol id for the router and press Enter:

↵

Note: The default X.25 PIDs are 0xC7 for primary routers and 0xC9 for backup routers. An error message appears if

—the PID of the current TL1 is NULL
—the protocol id has already been used
—the protocol id does not equal the number of bytes

A message similar to the following appears:

```
Enter the RemoteOPCName for TL1 Interface Primary Router
Service (END):
```

—continued—

Procedure 2-10 (continued)
Configuring the TL1 Interface Router Service over X.25

Step	Action
39	Enter: **end** ↵ *A message appears, indicating that the PID was configured for the TL1 Router Service, followed by the TL1 Router Configuration menu.* ***Note:*** The Router service must be re-enabled for the new protocol ID to take effect. Go to step 5.

—end—

Procedure 2-11
Configuring the TL1 Interface Router Service over TCP/IP

Use this procedure to configure the TL1 Interface Router Service (TIRS) over TCP/IP. TIRS routes TL1 messages to up to four spans of control that are connected with optical tributaries, Ethernet, or CNET.

The primary router service routes TL1 messages to the spans of control for remote primary operations controllers (OPC). The backup router service routes TL1 messages to the spans of control for remote backup OPCs.

Requirements

Before starting this procedure, you must do the following:

- Obtain the root password or admin userID and password.
- Determine the remote OPC names, TIDs, IP address of the operations system, operations system type, and port number for primary router service over TCP/IP.

Action

Step **Action**

1 Log in to the OPC.

If you do not know how to do this, see the procedures in *User Interfaces Description*, 323-3001-301, in this volume.

If you are logging in as	Then
root	*The UNIX prompt, opc>, appears. Enter the following command:* **config_tl1**
admin	*The User Session Manager appears. Move to the TL1 Configuration tool, then press* ***Ctrl_A*** *(or Keypad* ***0****).*

The TL1 Configuration tool Main Menu appears.

2 Configure the TL1 Interface Router Service. Enter:

6 ↵

The TL1 Interface Router Services Configuration menu appears.

3 Configure TIRS over TCP/IP by entering:

2 ↵

The TL1 Interface Router Services over TCP/IP main menu appears.

—continued—

Procedure 2-11 (continued)
Configuring the TL1 Interface Router Service over TCP/IP

Step	**Action**
4	Choose an action from the following table:

If you want to	**Then**
configure the primary router service	enter **1** ↵ and go to step 5
configure the backup router service	enter **2** ↵ and go to step 5
add an IP address for an operations system	go to step 43
delete an IP address from an operations system	go to step 48
list the IP addresses and interface types for each operations system	enter **5** ↵
return to the main menu	enter **8** ↵
exit	enter **9** ↵

Step	**Action**
5	Choose an action from the following table:

If you want to	**Then**
configure the TL1 router service port	go to step 6
configure the TL1 router service	go to step 9
enable the TL1 router service	enter **3** ↵
disable the TL1 router service	enter **4** ↵
list the TL1 router service configuration	enter **5** ↵
list the TL1 router service port configuration	enter **6** ↵
add a span of control to an existing TL1 router service configuration	enter **7** ↵ and go to step 15
add a target identifier (TID) to an existing TL1 router service configuration	enter **7** ↵ and go to step 22
delete a span of control from an existing TL1 router service configuration	enter **7** ↵ and go to step 29
delete a TID from an existing TL1 router service configuration	enter **7** ↵ and go to step 34
list the TIDs in a span of control	enter **7** ↵ and go to step 39
return to the main menu	enter **8** ↵
exit	enter **9** ↵

—continued—

Procedure 2-11 (continued)
Configuring the TL1 Interface Router Service over TCP/IP

Step Action

Configure the TL1 router service port

6 Configure the TL1 router service port by entering:

1 ↵

A message similar to the following appears:

```
Enter the port number for Primary Router Service over
TCPIP Operation:
```

7 Enter the port number that you want to configure and press:

↵

A message similar to the following appears:

```
Adding the Port Number 9007 for the TL1 Primary Router
Service

Do you wish to continue? (Yes/No):
```

8 Add the port number by entering:

yes ↵

The TL1 Router Configuration over TCP/IP menu appears again.

Go to step 5.

Configure the TL1 router service

9 Configure the TL1 router service by entering:

2 ↵

A message similar to the following appears:

```
Enter the RemoteOPCName for TL1 Interface Primary Router
Service (END):
```

The format is OPCxxxxP, where xxxx is an alphanumeric string, and P stands for primary OPC (or B for a backup OPC).

10 Enter the remote OPC name that you want to configure and press:

↵

A message similar to the following appears:

```
Enter the TID for TL1 Interface Primary Router
Service (END):
```

11 Enter the TID for this OPC span of control and press:

↵

A message similar to the following appears again:

```
Enter the TID for TL1 Interface Primary Router
Service (End):
```

—continued—

Procedure 2-11 (continued)
Configuring the TL1 Interface Router Service over TCP/IP

Step **Action**

12 If you have other TIDs to enter for this remote OPC name, go to step 11. Otherwise, enter:

end↵

A message similar to the following appears again:

```
Enter the RemoteOPCName for TL1 Interface Primary Router
Service (END):
```

13 If you have another remote OPC name to configure, go to step 10. Otherwise, enter:

end ↵

A message similar to the following appears:

```
The TL1 Primary Router over TCP/IP Configuration you have
Configured:

The RemoteOPC : OPC3801P
   The TID : OPC4801P
   The TID : 4801
   The TID : 4802

Do you wish to Update the Configuration? (Yes/No)
```

14 Update the configuration by entering:

yes ↵

The TL1 Router Configuration over TCP/IP menu appears again.

Go to step 5.

Add a span of control to an existing TL1 router service configuration

15 Add a span of control to an existing TL1 router service configuration by entering:

1 ↵

A message similar to the following appears:

```
Enter the RemoteOPCName for TL1 Interface Primary Router
Service (END):
```

16 Enter the remote OPC name and press:

↵

A message similar to the following appears:

```
Enter the TID for TL1 Interface Primary Router Service
(END):
```

—continued—

Procedure 2-11 (continued)
Configuring the TL1 Interface Router Service over TCP/IP

Step **Action**

17 Enter the TID and press:

↵

A message similar to the following appears again:

```
Enter the TID for TL1 Interface Primary Router Service
(END):
```

18 If you have other TIDs to enter for this remote OPC name, go to step 17. Otherwise, enter:

end ↵

A message similar to the following appears again:

```
Enter the RemoteOPCName for TL1 Interface Primary Router
Service (END):
```

19 If you have other remote OPC names to enter, go to step 16. If you have no other remote OPC names to enter, enter:

end ↵

A message similar to the following appears:

```
The SOCs added are

The RemoteOPC : OPC9275P
                The TIDs added : TIDNAME1

Do you wish to continue? (YES/NO):
```

20 Update the configuration by entering:

yes ↵

The following message appears:

```
Modifying the database.
```

The Modify Router Configuration menu appears again.

21 Return to TL1 Router Configuration over TCP/IP menu by entering:

8 ↵

The TL1 Router Configuration over TCP/IP menu appears again.

Go to step 5.

Add a TID to an existing TL1 router service configuration

22 Add a TID to an existing router service configuration by entering:

2 ↵

A message similar to the following appears:

```
Enter the RemoteOPCName to which you want to add TID for
TL1 Interface Primary Router Service (END):
```

—continued—

Procedure 2-11 (continued)
Configuring the TL1 Interface Router Service over TCP/IP

Step **Action**

23 Enter the remote OPC name and press:

↵

A message similar to the following appears:

```
Enter the TID for TL1 Interface Primary Router Service
(END):
```

24 Enter the TID and press:

↵

A message similar to the following appears again:

```
Enter the TID for TL1 Interface Primary Router Service
(END):
```

25 If you have other TIDs to enter for this remote OPC name, go to step 24. Otherwise, enter:

end ↵

A message similar to the following appears again:

```
Enter the RemoteOPCName to which you want to add TID for
TL1 Interface Primary Router Service (END):
```

26 If you want to add TIDs to another remote OPC name, go to step 23. Otherwise, enter:

end ↵

A message similar to the following appears:

```
The TIDs added are

The Remote OPC : OPC9275P

                The TIDs added : TIDNAME1

Do you wish to continue? (YES/NO):
```

27 Update the configuration by entering:

yes↵

The Modify Router Configuration menu appears again.

28 Return to TL1 Router Configuration over TCP/IP menu by entering:

8 ↵

The TL1 Router Configuration over TCP/IP menu appears again.

Go to step 5.

—continued—

Procedure 2-11 (continued)
Configuring the TL1 Interface Router Service over TCP/IP

Step **Action**

Delete a span of control from an existing TL1 router service configuration

29 Delete a span of control from an existing TL1 router service configuration by entering:

3 ↵

The following message appears:

```
Enter the RemoteOPCName for TL1 Interface Router Service
(END):
```

30 Enter the remote OPC name and press:

↵

The following message appears again:

```
Enter the RemoteOPCName for TL1 Interface Router Service
(END):
```

31 If you have other remote OPC names to delete, go to step 30. Otherwise, enter:

end ↵

A message similar to the following appears:

```
The SOC's deleted are

The Remote OPC : OPC4801P
                The TIDs deleted : OPC4801P

Do you wish to continue? (YES/NO):
```

32 Update the configuration by entering:

yes ↵

The Modify Router Configuration menu appears again.

33 Return to TL1 Router Configuration over TCP/IP menu by entering:

8 ↵

The TL1 Router Configuration over TCP/IP menu appears again.

Go to step 5.

Delete a TID from an existing TL1 router service configuration

34 Delete a TID from an existing TL1 router service configuration by entering:

4 ↵

A message similar to the following appears:

```
Enter the TID to be removed from Primary Router Service
(END):
```

—continued—

Procedure 2-11 (continued)

Configuring the TL1 Interface Router Service over TCP/IP

Step **Action**

35 Enter the TID that you want to delete and press:

↵

A message similar to the following appears again:

```
Enter the TID to be removed from Primary Router Service
(END):
```

36 If you have other TIDs to delete, go to step 35. Otherwise, enter:

end ↵

A message similar to the following appears:

```
The Remote OPC : OPC4801P
                The TIDs deleted : TIDNAME

Do you wish to continue? (YES/NO):
```

37 Update the configuration by entering:

yes ↵

The Modify Router Configuration menu appears again.

38 Return to TL1 Router Configuration over TCP/IP menu by entering:

8 ↵

The TL1 Router Configuration over TCP/IP menu appears again.

Go to step 5.

List the TIDs in a span of control

39 List the TIDs in a span of control by entering:

5 ↵

A message similar to the following appears:

```
Enter the RemoteOPCName for TL1 Interface Primary Router
Service (END):
```

40 Enter the remote OPC name and press:

↵

A message similar to the following appears:

```
The RemoteOPC : OPC9275P

       The TargetIDentifier : OPC9275P
       The TargetIDentifier : A1
       The TargetIDentifier : A2

Enter the RemoteOPCName for TL1 Interface Primary Router
Service (END):
```

—continued—

Procedure 2-11 (continued)
Configuring the TL1 Interface Router Service over TCP/IP

Step **Action**

41 If you have other TIDs to list, go to step 40. Otherwise, enter:

end ↵

The Modify Router Configuration menu appears again.

42 Return to TL1 Router Configuration over TCP/IP menu by entering:

8 ↵

The TL1 Router Configuration over TCP/IP menu appears again.

Go to step 5.

Add an IP address for an operations system

43 Add an IP address for an operations system by entering:

3 ↵

The following message appears:

```
Enter IP address of the OSS (END):
```

44 Enter the IP address and press:

↵

The following message appears:

```
Enter OSS Type [NMA or OPS or BTH] (End):
```

45 Enter the operations system type for this IP address (NMA or OPS or BTH) and press:

↵

The following message appears again:

```
Enter IP address of the OSS (END):
```

46 If you have more IP addresses to enter, go to step 44. Otherwise, enter:

end ↵

A message similar to the following appears:

```
The IP addresses added are

The IP Address : 192.219.223.73 - NMA

Do you wish to Update the configuration? (Yes/No):
```

47 Update the configuration by entering:

yes ↵

The TL1 Interface Router Services over TCP/IP main menu appears.

Go to step 4.

—continued—

Procedure 2-11 (continued)
Configuring the TL1 Interface Router Service over TCP/IP

Step **Action**

Delete an IP address for an operations system

48 Delete the IP address for an operations system by entering:

4 ↵

The following message appears:

```
Enter IP address of the OSS (END):
```

49 Enter the IP address and press:

↵

The following message appears again:

```
Enter IP address of the OSS (END):
```

50 If you have more IP addresses to delete, go to step 49. Otherwise, enter:

end ↵

A message similar to the following appears:

```
The IP addresses deleted are

The IP Address : 192.219.223.789 - NMA

Do you wish to Update the Configuration? (YES/NO):
```

51 Update the configuration by entering:

yes↵

The TL1 Interface Router Services over TCP/IP main menu appears.

Go to step 4.

—end—

Accessing TL1 by Ethernet

This chapter describes how to set up and access TL1 interfaces over an Ethernet network.

You can access the TL1 interface using a telnet session on an Ethernet network. This access allows you to use the following interfaces from a telnet session that you start from any workstation on the ethernet network:

- Operational processing system/intelligent network element provisioning operations system (OPS/INE)
- Network monitoring and analysis (NMA)
- Switched-access remote test system (SARTS)
- Digital analog remote test system (DARTS)

You set up TL1 access over Ethernet by creating a new userID specifically for that interface.

After you create and set up the user account for a specific TL1 interface, you can access that interface by opening a telnet session and logging in with the userID you created.

> ***Note:*** TL1 limits the number of OPS and NMA sessions that can run at one time. Before you set up and access TL1 interfaces, see *TL1 Interface Description*, 323-3001-190.

Chapter task list

This chapter includes the following tasks:

Procedure	Task	See
Procedure 3-1	Creating a user account for a TL1 interface	page 3-2
Procedure 3-2	Logging in and out of the TL1 interface using telnet	page 3-4

If you cannot complete these procedures, contact your next level of support.

Procedure 3-1
Creating a user account for a TL1 interface

Use this procedure to create a user account for a specific TL1 interface. Repeat this procedure for each TL1 interface you need to access.

CAUTION
Risk of deleting pwd file
Use extreme care when entering UNIX commands. UNIX commands are case sensitive. To quit anytime without saving changes press **esc** and enter **:q!**↵ .

Requirements

Before beginning this procedure, you must:

- be familiar with the vi editor. See the “Unix editor (vi) quick reference” in *User Interfaces Description*, 323-3001-301, in this volume
- have root access to the operations controller (OPC)

Action

Step **Action**

1 Log in to the OPC.

2 Determine the user information for the new user account. See Table 3-1.

Table 3-1
User accounts for accessing TL1 interfaces by ethernet

If you want to access this interface	Then add this user	To this group
OPS/INE	ops	prov
NMA	nma	slat
SARTS	sarts	test
DARTS	darts	test

3 Add the new user account using Procedure 4-1 of this document.

4 Open a UNIX terminal window.

—continued—

Procedure 3-1 (continued)
Creating a user account for a TL1 interface

Step	**Action**
5	Open the password file by entering: **vipw** ↵ *The password file appears.* ***Note:*** At any time in vi, you can press **<esc>** then type **:q!**↵ to exit the file without saving changes.
6	Scroll to the user account you just added using the up and down arrow keys.
7	Scroll to the beginning of the pathname shown below using the left and right arrow keys. Place the cursor on the first slash in the pathname. `/iws/usm/usmstart`
8	Enter x several times to delete the characters to the end of the line. *The vi editor deletes the pathname one character at a time.*
9	To add the new path name, enter: **a** *The vi editor goes into input mode.*
10	Enter the pathname for the user account you created. See Table 3-2.

Table 3-2
Pathnames for TL1 user accounts

If you created this user account	Then enter this pathname
ops	/iws/tl1/tl1ops.file
nma	/iws/tl1/tl1nma.file
sarts	/iws/tl1/tl1sarts.file
darts	/iws/tl1/tl1darts.file

11	To leave input mode, press **esc.**
12	To save the file and quit vi, enter: **wq**↵

—end—

Procedure 3-2
Logging in and out of the TL1 interface using telnet

Use this procedure to start your telnet session to the following interfaces:

- Operational processing system/intelligent network element provisioning operations system (OPS/INE)
- Network monitoring and analysis (NMA)
- Switched-access remote test system (SARTS)
- Digital analog remote test system (DARTS)

Requirements

You must have the userID and password for the account for the TL1 interface you want to use.

Action

Step	Action
1	Log in to the OPC using the userID and password for the TL1 interface. If you do not know how to do this, see the procedures in *User Interfaces Description*, 323-3001-301, in this volume.
2	Enter any of the TL1 interface commands for the TL1 interface you are using. (See *TL1 Interface Description*, 323-3001-190.)
3	To log out of the telnet session, enter: **canc-user;** ↵

—end—

Managing network security

This chapter contains procedures to create and manage user accounts and user groups, and user passwords for both the operations controller (OPC) and network elements. It also contains procedures to administer network element access privileges.

These procedures use the Centralized User Administration tool located in the operations controller (OPC) admin user group on the active OPC. The typical user of this tool is the OPC system administrator who manages overall security and command access for the system.

All user accounts have individual passwords, and belong to a user group. Password management consists of maintaining a single password for each user account.

Users must update their own passwords periodically, using the Password Update tool. The system notifies users that the time to update their password is approaching. The system administrator can provision the time period between notifications (see “Password aging” on page 4-13).

Occasionally, a user forgets a password. An OPC system administrator must then assign a new one.

> ***Note:*** After passwords expire, users (except the default admin user) will not be able to login to the network element. To login again, users with expired passwords must login to the OPC and change their passwords.

You define the network elements that are accessible by each user account and the user’s capabilities (access class) in each network element.

When adding new user accounts, the users with the same network element access requirements should be added to the same user group. You can create groups to accommodate various user requirements, but the number of groups should be substantially less than the number of user accounts.

A number of user groups, each with predefined user accounts, toolsets, and tools are defined as defaults when the OPC is delivered. These user accounts are defined in Table 4-1 on page 4-3. They represent different levels of security, and have access to different OPC tools. In each case, the user group identifier, user account name, and initial password are the same. Since these passwords are widely known, you should change them immediately.

When you update the network software with a new release, check the NTP for new predefined user accounts. If the release includes new accounts, you must enable the accounts before you can use them. See Procedure 4-6, “Enabling or disabling user accounts,” for directions.

CAUTION
After changing (including deleting user accounts and updating passwords) user accounts, it is recommended that you save the network element image so the changes are permanent on the network element.

If a network element reboot or restore occurs before you save the network element image, the changes are not saved on the network element. The next user profile audit (scheduled or on-demand) resolves any differences.

The following default user groups are delivered with the OPC. All of the default user groups, with the exception of the standby user group, are available on the active OPC. Only the standby and root default user groups can log into an inactive OPC.

> ***Note 1:*** The Password Update tool cannot be used on an inactive OPC. All password updating activity must be performed on an active OPC.
>
> ***Note 2:*** The system does not allow you to delete default groups, default toolsets, or default user accounts.

Table 4-1 summarizes the default user accounts delivered with the OPC.

Table 4-1
Default user accounts

Default user account types	Description
master	The default master user group is responsible for administration of the OPC. It contains several toolsets by default.
root	The default root user account is located in the root user group. This user account has special access privileges and cannot be viewed or modified in the Centralized User Administration tool. You can modify the password of the default root user by logging in as root and selecting the Password Update tool on an active OPC. This user account can open any tool and it has unlimited UNIX file privileges. As a security precaution, it should be used only when the required action is beyond the power of any other user account.
root1	The default root1 user account is located in the root user group. This user account can be enabled for use in special circumstances, such as upgrades or for troubleshooting when the User Session Manager is not operating. The root1 user must be explicitly enabled by the root user (see “Enabling or disabling the root1 user account” on page 4-36), but otherwise has all the access privileges of root. The root1 user accesses a UNIX shell on logging in to the OPC. By default, the root1 user is automatically disabled 24 hours after being enabled. The root user can override the default time period.
standby	The default standby user account is located in the root user group, and cannot be viewed or modified in the Centralized User Administration tool. This user account is responsible for operations on the inactive OPC. ***Note***: The Password Update tool cannot be used on an inactive OPC. All Password Update activity must be performed on an active OPC.
slat	The default slat user account is located in the slat user group. This user account is responsible for commissioning the network.
admin	The default admin user account is located in the admin user group. This user account is responsible for maintenance and administration of the network.
netsurv	The default netsurv user account is located in the netsurv user group. This user account is responsible for network surveillance.
prov	The default provisioning user account is located in the prov user group. This user account is responsible for provisioning of circuits which pass through the AccessNode.
test	The default test user account is located in the test user group. This user account is responsible for managing special test conditions on the circuits and line cards in the AccessNode System.

CAUTION
You cannot delete the default groups, default toolsets, or default user accounts.

Table 4-2 lists the toolsets and tools available to each default user group, and the user accounts within those groups.

An asterisk (*) beside a tool name indicates that the tool is automatically opened and displayed in the Open tools list in the User Session Manager window when the user account logs in. When a new user account is added to a default user group, the new account receives the tools, toolsets, and auto-start tools of the group to which it is being added.

A double asterisk (**) beside a tool name indicates that the tool appears only at the X terminal graphical user interface.

Table 4-2
Toolsets

Group (GID)	Users (UID)	Toolsets	Auto-Start Tools	NE Acc/Cls

admin(21)	admin(10)
	operator(13)
		Software Admin
		OPC Admin (admin)
		Network Admin
		Network Surveillance
		Utilities (DMS10)
				Yes/RWA

slat(17)	slat(8)	OPC Admin (others) Network Admin Network Surveillance SLAT Test Admin Utilities (DMS10)	Commissioning Mngr	No/R

—continued—

Table 4-2 (continued)
Toolsets

Group (GID)	Users (UID)	Toolsets	Auto-Start Tools	NE Acc/Cls
prov	prov	Network Surveillance Prov Admin Utilities		No/R
netsurv(18)	netsurv(18)	OPC Admin (others) Net Surv Test Admin Utilities	Alarm Monitor NE Login Manager Network Summary	Yes/R

root(0)	root(0)
	root1(0)
		Software Admin
		OPC Admin
		Network Admin
		Network Surveillance
		SLAT
		Prov Admin
		Test Admin
		Utilities (DMS10)
		Surveillance (View)
		Restricted Tools
			Unix Shell-2	No/R

standby(100+)	standby(15)	Standby		No/R
test		Network Surv (test) SLAT (test) Test Admin Utilities (test)		No/R

—continued—

Table 4-2 (continued)
Toolsets

Group (GID)	Users (UID)	Toolsets	Auto-Start Tools	NE Acc/Cls
techsupp	none	Software Admin OPC Admin Network Admin Network Surveillance SLAT Prov Admin Test Admin Training Utilities (DMS10) Surveillance (View) Restricted Tools	Unix Shell -2	Yes/RWA
viewsurv	viewsurv	Surveillance (View) Utilities	Alarm Monitor NE Login Manager Network Summary	Yes/R
demo	demo	Training		No/R
master	master	Network Surveillance Master Admin Utilities	Alarm Monitor Network Summary	No/R
—end—				

Table 4-3 lists the tools within each default toolset.

Table 4-3
Default toolsets

Toolset	**Tools**
Master Admin	OPC Shutdown OPC Save and Restore OPC Date Commissioning Mngr Unix Shell OPC Alarm Prov OPC PM Coll. Filter OPC TID/NE Mapping
Network Admin	Telemetry - TBOS E2A Alarm Manager Configuration Mngr Connection Mngr Cluster Inventory Host Prov Mngr Alarm Prov Manager
Network Surveillance	Alarm Monitor* Network Summary* Event Browser Network Browser Protection Manager
Network Surv (test)	Alarm Monitor Event Browser
Net Surv	Alarm Monitor Network Summary Event Browser Network Browser Protection Manager Connection Mngr (R)

—continued—

Table 4-3 (continued)
Default toolsets

Toolset	**Tools**
OPC Admin	Central User Admin Remote OPC SW Inst. OPC PM Collection Filter OPC Save and Restore OPC Shutdown OPC Date Unix Shell Port Configuration IP Routing Admin OPC Status OPC Clock** OPC Alarm Prov
OPC Admin (admin)	Central User Admin Remote OPC SW Inst. OPC PM Collection Filter OPC Save and Restore OPC Shutdown OPC Date Port Configuration IP Routing Admin OPC Status OPC Clock** OPC Alarm Prov
OPC Admin (others)	Remote OPC SW Inst. OPC Save and Restore OPC Shutdown OPC Date OPC Status OPC Clock** OPC PM Coll. Filter

—continued—

Table 4-3 (continued)
Default toolsets

Toolset	**Tools**
Prov Admin	Provisioning Manager Default Prov Mngr Host Prov Mngr Connection Mngr TR-08 Def Prov Mngr Alarm Prov Manager
Restricted tools	OPC Switch Enable Clear Com’g Ethernet Admin
SLAT	Commissioning Mngr* Configuration Mngr PGTC/MTA Prov Mngr Event Browser Reboot/Load Manager OPC Shutdown OPC Date OS Connection Mngr OPC Alarm Prov
SLAT (test)	PGTC/MTA Prov Mngr OS Connection Mngr
Software Admin	Reboot/Load Manager Backup/Restore Mngr Alarm Monitor Event Browser Network Upgrade Mngr Incremental SW Del.

—continued—

Table 4-3 (continued)
Default toolsets

Toolset	Tools
Standby	OPC Save and Restore OPC Shutdown OPC Date Event Browser Password Update Remote OPC Login** Logout
Surveillance (View)	Alarm Monitor Network Summary Event Browser Network Browser Protection Mngr (V) NE Login Manager
Test Admin	Specials Lineup Mngr Test Manager Provisioning Manager
Training	Message Alarm Demo Logout
Utilities	NE Login Manager* Password Update Remote OPC Login** Logout**

—continued—

Table 4-3 (continued)
Default toolsets

Toolset	Tools
Utilities (DMS)	NE Login Manager DMSTerm Password Update Remote OPC Login Logout
Utilities (test)	NE Login Manager Password Update Logout
—end—	

Intrusion attempt handling

The OPC validates the userID and password used for a log-in request to the OPC or to any network element within the OPC's span of control. The OPC or network element also monitors the number of failed log-in attempts. The security features of the OPC and AccessNode network element ensure that if a user enters either an invalid userID or password, the log-in attempt is rejected.

When the number of invalid log-in attempts reaches a provisioned number (from two to nine), the user interface port is locked out for a brief time. The period of time that the user interface port is locked out is also provisionable (from 0 to 180 seconds). If the lockout period is set to zero, the user interface is not locked out, regardless of the setting of the maximum number of invalid log-in attempts.

When the intrusion attempt handling feature is triggered, the user cannot enter anything at the terminal connected to that user interface port until the lockout period expires. If the intrusion attempt handling is triggered at a network element, the network element raises an alarm (if the provisioned lockout period is one or more seconds). If the intrusion attempt handling feature is triggered at an OPC, the OPC does not generate an alarm. However, the network element alarm is visible at the OPC (for example, through the Alarm Monitor and Event Browser tools).

The user interface port from which the log-in attempts are made is locked out, not the userID. For example, if a particular valid userID is entered with the wrong password more than the maximum allowed number of attempts, the port is locked out. However the user can still log in through another port (using the correct password).

The setting for the number of invalid log-in attempts and the lockout period can be different for the OPC and the network elements within OPC span of control. However, the network element settings apply to all the network elements and cannot be provisioned on network element basis.

Intrusion attempt handling applies to user interface ports 1, 2, 3, and 4 on the network element and to ports B and Esp 1 for the OPC. Port B is a physical RS-232 connector on the AccessNode. Both of these physical connectors map to port B in the OPC Port Configuration tool. Esp 1 is the label of the physical connector on the AccessNode that maps to port 3 in the OPC Port Configuration tool. The types of login are:

- login to an OPC or network element using the rlogin and nelogin commands
- rlogin access from the Network Manager
- login to an OPC using Telnet, including Telnet over Transmission Control Protocol/Internet Protocol (TCP/IP) or Telnet over Serial Line Internet Protocol (SLIP)
- login to an OPC using a terminal connected by way of an X.3 packet assembler/disassembler (PAD)
- login to an OPC using an X.11 Display Manager session
- access to an OPC using the TL1 or OSI/Q3 interfaces

The number of invalid log-in attempts is retained until one of the following events occurs:

- a successful log-in attempt is made from that user port
- a shelf processor restart or reboot occurs (which causes the invalid log-in attempt counters for that network element to be cleared)
- the OPC is rebooted (which causes the invalid log-in attempt counters for that OPC to be cleared)

The intrusion attempt handling feature supports connections through an asynchronous serial modem as follows:

- It is assumed that the data terminal ready (DTR) signal is passed through from the serial port to the modem.
- It is also assumed that the modem is configured to drop the connection if the DTR is lowered and to not answer an incoming call if the DTR is lowered.

If intrusion attempt handling is triggered, the DTR is lowered for the duration of the lockout period. For that period, the modem cannot answer incoming calls. When the lockout period expires, the DTR is raised, thereby allowing the modem to again answer incoming calls.

Password aging

Password aging is a security feature on the OPC and network elements that makes sure users change their passwords periodically. The longer a password remains in use, the greater the chance an intruder can discover that password. By changing their passwords frequently, users reduce the chances of an intruder breaking into the system.

Password aging is disabled by default. You can enable password aging by specifying a value in the password expiration period, the accreditation period, or both. You can disable password aging by emptying both fields.

The password expiration period and the accreditation period apply to all userIDs on both the primary and backup OPCs. These parameters also apply to all network elements in the span of control. To change these parameters, see "Managing system parameters" on page 4-56.

When you enable password aging, the OPC maintains the following parameters for each user:

Table 4-4
OPC password parameters

Parameter	Description
Password last changed date	date that the user or system administrator last changed the password.
Password expiration date	date the user must change the password before the OPC or network element permits login.
Account status	state of the user account. The status can be • valid • disabled • assigned • expired-AP (expired accreditation period) • expired-EP (expired expiration period)

You can use the Centralized User Administration tool to view these fields. Select a user, then select the **Show user account info...** command from the list item menu.

Password last changed date

The system resets the password last changed date whenever the user or the system administrator changes the password. The OPC tracks whether the user or the system administrator changed the password.

If the Centralized User Administration tool was used to change the password, the OPC assumes the system administrator changed the password. If the Password Update tool was used to make the change, the OPC assumes the user changed the password.

Password expiration date

The OPC calculates the password expiration date. The OPC adds either the accreditation period or the password expiration period to the password last changed date.

If the system administrator last changed the user password, the OPC uses the accreditation period. If the user last changed the password, the OPC uses the password expiration period.

The system administrator typically assigns a password to a user for one of the following reasons:

- initial creation of the user account
- the user has forgotten the password

The system administrator might assign a well known password. The user account is then vulnerable to an intruder break-in. A short accreditation period minimizes the period of vulnerability before the user must change the password.

If the accreditation period is undefined, the OPC uses the password expiration period to calculate the password expiration date. It does not matter if the user or system administrator last changed the password.

If the system administrator last changed the password and the password expiration period is undefined, the OPC uses the accreditation period to calculate the password expiration date. If the user last changed the password and the password expiration period is undefined, the password never expires.

If both the password expiration and the accreditation period are undefined, password aging is disabled.

The password expiration occurs at midnight on the expiration date. At any time after password expiration, the following happens:

- The user’s login attempt to a network element results in a warning message indicating that the password has expired. The network element denies login access. The user must log in to the OPC to change the password. The admin user gets the same message when the admin password expires, but the network element allows the admin user to log in.
- The user’s login attempt to the OPC automatically accesses the Password Update tool. A message indicates that the password has expired. The user must change the password before logging in to the OPC.

Account status

When the system administrator changes the user’s password, the account status becomes “assigned.” When the user changes the password, the Account status becomes “valid.”

If the system administrator last changed the user’s password and the user's password expires, the Account status becomes “expired_AP” (expired accreditation period). If the user last changed the password and the password expires, the Account status becomes “expired_EP” (expired expiration period).

If the system administrator disables the user, the account status becomes “disabled.”

Password change notification period

The password change notification period ends on the day before the password expires. The following happens during the password change notification period:

- When the user logs in to the network element, a warning message indicates the number of days left before the password expires.
- When the user logs in to the OPC, the Password Update tool appears. A message indicates the number of days remaining before the password expires. The user can postpone entering a new password by exiting the Password Update tool.

You can provision the password change notification period from 0 to 14 days. The parameter applies to all userIDs on both the primary and backup OPCs and to all network elements in the span of control.

A value of 1 to 14 means a warning message appears when the user logs in on any of the specified number of days before the password expires. A value of zero means no message appears to indicate the password is about to expire.

Chapter task list

Look up the task, as it relates to your job, in the left column in the following task list. Then refer to the page in the right column.

A security-related task that you must complete during system installation is the creation of user groups and user accounts and their privileges to access network elements. To perform this task, you must create user accounts for all users authorized to use the network. These users should be formed into user groups that have the same requirements.

Task	Procedure	See
User accounts	Creating a new user account (including setting the password) Creating a new user account by duplicating the current attributes of an existing user, including setting the password Changing an existing user account Deleting a user account Changing user account passwords Enabling or disabling user accounts Enabling or disabling the root1 user account	page 4-17 page 4-21 page 4-25 page 4-28 page 4-31 page 4-33 page 4-36
User groups	Creating a new user group Deleting a user group Changing user group attributes Moving users between user groups	page 4-38 page 4-41 page 4-43 page 4-60
Toolsets	Creating a new toolset Changing an existing toolset Deleting a toolset	page 4-46 page 4-49 page 4-52
Auto-start tools	Creating auto-start tools for user groups	page 4-54
Passwords	Managing system parameters Changing user account passwords	page 4-56 page 4-31
Sort and filter user list	Sorting the users list Filtering the users list	page 4-62 page 4-63
Audits and backups	Auditing user profile data Scheduling a user profile audit Transferring user profile data to the backup OPC	page 4-65 page 4-67 page 4-69
UserIDs (for NEs)	Listing all authorized userIDs on the NE Listing all users logged in to the NE Listing all users logged in to the NE and the device Displaying the userID logged in at a terminal Logging out another userID	page 4-70 page 4-71 page 4-72 page 4-73 page 4-74

If you cannot complete these procedures, contact your next level of support.

Procedure 4-1
Creating a new user account

Use this procedure to create a new user account. It includes adding the user account to an existing user group, defining the account accessibility and access class to a network element (NE) in the operations controller (OPC) span of control, and assigning a password to the account.

You must assign a password to the new user account before the user can log in to the OPC or NEs.

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the OPC with permission to use the OPC Centralized User Administration tool (default user groups root, admin)
- read the command conventions for the interface (CMT or graphical) you are using in *OPC User Interface Description*, 323-3001-301, in this volume

CAUTION
If communications between the OPC and the NEs where the user account has access are not in operation, you can attempt to enable or disable the user account, or change the access class. However, the changes are not applied until the next user profile audit.

Action

Step **Action**

1 Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool.

The Centralized User Administration tool main window appears.

2 Tab to the Create a new user button, then press **Ctrl_A** (or Keypad **0**).

The Create User Profile screen appears.

3 Enter a unique user account name in the User Id field. This field is required. The name can have 1 to 8 characters. The following characters can be used in the login name: a-z (lowercase only), and 0 to 9. The first character must be alphabetic.

Note: Do not use the word “abort” for the userID.

—continued—

Procedure 4-1 (continued)
Creating a new user account

Step	Action
4	Tab to the Group field, and enter the name of an existing user group where you want to assign the user account.
5	Tab to the User Name field, and enter the full name of the owner of the account, up to 20 characters.
6	Tab to the Detail field, and enter any text you want (for example, the site or location of the user).
7	Tab to the Network View list.
8	If you want to change the NE configuration, select the NE you want to modify for this user account access, then press **Ctrl_A** (or Keypad **0**). Otherwise, go to step 13.
9	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).

If you want to	Then
enable user access to the NE	In the list item menu, select the Enable Access command by pressing **Space** (or Keypad **0**). The user's access to the network element is created and the Accessibility column in the Network View list displays Yes for the specified network element. Go to step 7.
disable user access to the NE	In the list item menu, move to the Disable Access command, then press **Space** (or Keypad **0**). The user's access to the network element is removed and the Accessibility column in the Network View list displays No for the specified network element. Go to step 7.
change user access class for the NE	Go to step 10.

Note: If a "?" appears beside an NE, that NE is not communicating with the OPC. If you make changes that affect this NE, then an error dialog appears. You can continue or stop the operation.

10 In the list item menu, move to the Set Access Class command.

A cascade menu appears.

11 Move to the cascade menu by pressing the right arrow key.

—continued—

Procedure 4-1 (continued)
Creating a new user account

Step **Action**

12 Move to the access class option that you want, then press **Space** (or Keypad **0**). The access class assigned to a user can be greater than the default value assigned to the user group.

The access class for the network element changes to the selected option.

Go to step 7.

13 Verify the data you entered. Decide whether you want to save the data and continue with the procedure and define a password for the user, or exit the procedure without saving the data.

14 If you want to exit without saving the data, tab to the Cancel button, then press **Ctrl_A** (or Keypad **0**). Otherwise, go to step 15.

All changes are lost. The Create User Profile dialog closes.

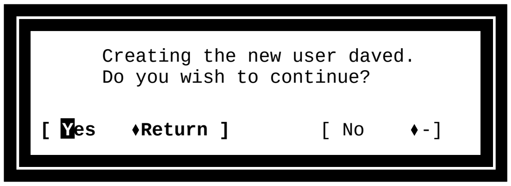
Go to step 19.

15 Tab to the OK button, then press **Ctrl_A** (or Keypad **0**).

The information is verified. If an error is detected in the user account information fields, an X appears at the beginning of the field with the error and the cursor returns to the field. Make the correction and re-execute this step. Error messages also appear while you are entering the information in the user account field.

When no errors exist, the following confirmation dialog appears:

PC-21603



```
      Creating the new user daved.
      Do you wish to continue?

[ Yes   ♦Return ]        [ No    ♦-]
```

16 To create this new user account, select the Yes button by pressing **Ctrl_A** (or Keypad **0**).

The Assign Password dialog appears.

—continued—

Procedure 4-1 (continued)
Creating a new user account

Step	Action
17	Enter a password for this user in the password field, then press **Return**. *The password must be 5 to 8 characters. The first character must be alphabetic (a to z, A to Z). The remaining characters can be a to z, A to Z, 0 to 9, _ (underscore), or a $. Passwords must have at least one numeric character or one character from the set [_$]. The characters are not displayed as you enter them, but the cursor moves.* *When you press Return, the password field is checked. If the password is accepted, the password field label changes to “Retype new password”. Otherwise, an X appears next to the password field, and an error dialog indicates why the password was not accepted.*
18	Reenter the password, then press **Return**. *If this second password does not match the first password, then an error message appears.* Select the OK button to remove the message, and redo the same sequence. *When the passwords match, the Assign Password dialog closes, and the Centralized User Administration main window appears.*
19	To close the tool, press **Esc**), or do the following: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 4-2
Creating a new user account by duplicating the current attributes of an existing user

Use this procedure to create a new user account by duplicating the current attributes of an existing user. This procedure includes adding the user account to an existing user group, defining the account accessibility and access class to a network element (NE) in the operations controller (OPC) span of control, and assigning a password to the account.

You must assign a password to the new user account before the user can log in to the OPC or NEs.

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the OPC with permission to use the OPC Centralized User Administration tool (default user groups root, admin)
- read the command conventions for the interface (character-mode terminal or graphical) you are using in *OPC User Interface Description*, 323-3001-301, in this volume

> **CAUTION**
> If communications between the OPC and the NEs where the user account has access are not in operation, you can attempt to enable or disable the user account, or change the access class. However, the changes are not applied until the next user profile audit.

Action

Step	Action
1	Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool. *The Centralized User Administration tool main window appears.*
2	Move to the user account with the attributes you want to apply to the new user account. Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**). *The list item menu appears.*

—continued—

Procedure 4-2 (continued)
Creating a new user account by duplicating the current attributes of an existing user

Step	Action
3	Move to the Duplicate command, then press **Space** (or Keypad **0**). *The Create User Profile screen appears The new user account inherits the information in the Group, User Name, Detail, and list (including the NEs, accessibility and access class).*
4	Enter a unique user account name in the User Id field. This field is required. The name can have 1 to 8 characters. The following characters can be used in the login name: a to z (lowercase only), and 0 to 9. The first character must be alphabetic. ***Note:*** Do not use the word “abort” for the userID.
5	Tab to the Group field.
6	If you want to change the displayed group, enter the name of an existing user group where you want the user account assigned. Otherwise, go to step 7.
7	Tab to the User Name field.
8	If you want to change the user name, enter the full name of the owner of the account, up to 20 alphanumeric characters. Otherwise, go to step 9.
9	Tab to the Detail field.
10	If you want to change the detail, enter any text you want (for example, the site or location of the user). Otherwise, go to step 11.
11	Tab to the Network View list.
12	If you want to change the NE configuration, select the NE you want to modify for this user account access, then press **Ctrl_A** (or Keypad **0**). Otherwise, go to step 17.
13	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).

—continued—

Procedure 4-2 (continued)
Creating a new user account by duplicating the current attributes of an existing user

Step **Action**

If you want to	**Then**
enable user access to the NE	In the list item menu, select the Enable Access command by pressing **Space** (or Keypad **0**). The user’s access to the network element is created and the Accessibility column in the Network View list displays Yes for the specified network element. Go to step 11.
disable user access to the NE	In the list item menu, move to the Disable Access command, then press **Space** (or Keypad **0**). The user’s access to the network element is removed and the Accessibility column in the Network View list displays “No” for the specified network element. Go to step 11.
change user access class for the NE	Go to step 14.

Note: If a “?” appears beside an NE, that NE is not communicating with the OPC. if you make changes that affect this NE, then an error dialog appears. You can continue or stop the operation.

14 In the list item menu, move to the Set Access Class command.

A cascade menu appears.

15 Move to the cascade menu by pressing the right arrow key.

16 Move to the desired access class option, then press **Space** (or Keypad **0**). The access class assigned to a user can be greater than the default value assigned to the user group.

The access class for the NE changes to the selected option.

Go to step 11.

—continued—

Procedure 4-2 (continued)
Creating a new user account by duplicating the current attributes of an existing user

Step	Action
17	Verify the data you entered. Decide whether you want to save the data and continue with the procedure and define a password for the user, or exit the procedure without saving the data.
18	If you want to exit without saving the data, tab to the Cancel button, then press **Ctrl_A** (or Keypad **0**). Otherwise, go to step 19. *All changes are lost. The Create User Profile dialog closes.* Go to step 23.
19	Tab to the OK button, then press **Ctrl_A** (or Keypad **0**). *The information is verified. If an error is detected in the user account information fields, an X appears at the beginning of the field with the error, and the cursor returns to the field. Make the correction and re-execute this step. Error messages also appear while you are entering the information in the user account field.* *When no errors exist, a confirmation dialog appears.*
20	To create this new user account, tab to the **Yes** button, then press **Ctrl_A** (or Keypad **0**). *The Assign Password dialog appears.*
21	Enter a password for this user in the password field, then press **Return**. *The password must be 5 to 8 characters. The first character must be alphabetic (a to z, A to Z). The remaining characters can be a to z, A to Z, 0 to 9, _ (underscore), or a $. Passwords must have at least one numeric character or one character from the set [_$]. The characters are not displayed as you enter them, but the cursor moves.* *When you press Return, the password field is checked. If the password is accepted, the password field label changes to “Retype new password”. Otherwise, an X appears next to the password field, and an error dialog indicates why the password was not accepted.*
22	Reenter the password, then press **Return**. *If this second password does not match the first password, then an error message appears.* Select the OK button to remove the message, and redo the same sequence. *When the passwords match, the Assign Password dialog closes, and the Centralized User Administration main window appears.*
23	To close the tool, press **Esc**), or do the following: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 4-3
Changing an existing user account

Use this procedure to change an existing user account. This procedure includes changing groups, and redefining the account accessibility and access class to a network element (NE) in the operations controller (OPC) span of control.

Disabling NE access when user account is in-use

When you disable a user's access to a 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
- the current NE session is not disturbed
- the user's password automatically expires upon logout
- 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.

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the OPC with permission to use the OPC Centralized User Administration tool (default user groups root, admin)
- read the command conventions for the interface (character-mode terminal or graphical) you are using in *OPC User Interface Description*, 323-3001-301, in this volume

CAUTION
If communications between the OPC and the NEs where the user account has access are not in operation, you can attempt to enable or disable the user account, or change the access class. However, the changes are not applied until the next user profile audit.

Action

Step	Action
1	Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool. *The Centralized User Administration tool main window appears.*

—continued—

Procedure 4-3 (continued)
Changing an existing user account

Step	Action
2	Move to the user account that you want to change. Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**). *The list item menu appears.*
3	Select the Open command by pressing **Space** (or Keypad **0**). *The Edit User Profile dialog appears.* You cannot change the User Id field when editing an existing user account.
4	Tab to the Group field.
5	If you want to change the displayed group, enter the name of an existing user group where you want the user account assigned. Otherwise, go to step 6.
6	Tab to the User Name field.
7	If you want to change the user name, enter the full name of the owner of the account, up to 20 alphanumeric characters. Otherwise, go to step 8.
8	Tab to the Detail field.
9	If you want to change the detail, enter any text you want (for example, the site or location of the user). Otherwise, go to step 10.
10	Tab to the Network View list.
11	If you want to change the NE configuration, select the NE you want to modify for this user account access, then press **Ctrl_A** (or Keypad **0**). Otherwise, go to step 16.
12	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).

If you want to	**Then**
enable user access to the NE	In the list item menu, select the Enable Access command by pressing **Space** (or Keypad **0**). The user's access to the network element is created and the Accessibility column in the Network View list displays Yes for the specified network element. Go to step 10.
disable user access to the NE	In the list item menu, move to the Disable Access command, then press **Space** (or Keypad **0**). The user's access to the network element is removed and the Accessibility column in the Network View list displays “No” for the specified network element. Go to step 10.
change user access class for the NE	Go to step 13.

—continued—

Procedure 4-3 (continued)
Changing an existing user account

Step	Action
	Note: If a “?” appears beside an NE, that NE is not communicating with the OPC. If you make changes that affect this NE, then an error dialog appears. You can continue or stop the operation.
13	In the list item menu, move to the Set Access Class command. *A cascade menu appears.*
14	Move to the cascade menu by pressing the right arrow key.
15	Select the access class option by pressing **Space** (or Keypad **0**). The access class assigned to a user can be greater than the default value assigned to the user group. *The access class for the NE changes to the option you selected.* Go to step 10.
16	Verify the data you entered. Decide whether you want to save the data and continue with the procedure, or exit the procedure without saving the data.
17	If you want to exit without saving the data, tab to the Cancel button, then press **Ctrl_A** (or Keypad **0**). Otherwise, go to step 18. *All changes are lost.* *If you select the Yes button, the Edit User Profile dialog closes, and you are returned to the Centralized User Administration main window. Go to step* 20. *If you select the No button, you remain in the Edit User Profile dialog. You then go to step* 3 *and make the changes.*
18	Tab to the OK button, then press **Ctrl_A** (or Keypad **0**). *The information is verified. If an error is detected in the user account information fields, an X appears at the beginning of the field with the error and the cursor returns to the field.* Make the correction and re-execute this step. *Error messages also appear while you are entering the information in the user account field. When no errors exist, a confirmation dialog appears.*
19	To apply the changes, tab to the Yes button, then press **Ctrl_A** (or Keypad **0**). Otherwise, select **No** to stay in the Edit User Profile dialog. *The Centralized User Administration main window appears.*
20	To close the tool, press **Esc**), or do the following: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the **Exit** command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 4-4
Deleting a user account

Use this procedure to delete a user account.

Deleting in-use user accounts

OPC users

When you delete a user account being used for an 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 an NE session, be aware of the following consequences:

- the current NE session is not disturbed
- the user’s password automatically expires upon logout
- 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

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the OPC with permission to use the OPC Centralized User Administration tool
- read the command conventions for the interface you are using (CMT or graphical) in *OPC User Interface Description*, 323-3001-301, in this volume
- check to see if the user account is logged in to any of the NEs where the user account has access

  Note: If you do not know how to do this, see Procedure 4-23 on page 4-71.

—continued—

Procedure 4-4 (continued)
Deleting a user account

CAUTION
If communications between the OPC and the NEs where the user account has access are not in operation, you can attempt to delete the user account. However, the changes are not applied until the next user profile audit.

CAUTION
You cannot change the default user accounts.

Action

Step **Action**

1 Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool.

The Centralized User Administration tool main window appears.

2 In the users list, move to the user account you want to delete, then press **Ctrl_A** (or Keypad **0**).

The selected user account is highlighted.

3 Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).

4 Select the Open command by pressing **Space** (or Keypad **0**).

The Edit User Profile dialog appears.

5 Check the Network View list to make sure all communication links with the NEs are in operation.

Note: A “?” beside an NE listed in the Network View indicates that communications between the OPC and that NE are not in operation. If you make changes that affect this NE, then an error dialog appears. You can continue or stop the operation.

6 After you review the Network View list, tab to the Cancel button, then press **Ctrl_A** (or Keypad **0**).

The users list of the Centralized User Administration main window appears.

7 To continue with this deletion, display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**). Otherwise, go to step 10.

8 Move to the Delete command, then press **Space** (or Keypad **0**).

A confirmation dialog appears.

—continued—

Procedure 4-4 (continued)
Deleting a user account

Step	Action

9 Tab to the Yes button to delete the user account, or to the No button to stop the deletion. Press **Ctrl_A** (or Keypad **0**).

Note 1: If a user account is logged in to any NE, or if the communication link to an NE is not in operation when you select the OK button, an error message appears indicating that the operation cannot be successfully completed. You can continue or stop the operation.

Note 2: When the deleted user logs out of the NE, the user is not able to log in again.

If you want to	Then go to
exit the Centralized User Administration tool	step 10
delete another user account	step 2

10 To close the tool, press **Esc**), or do the following:

a. Display the window menu by pressing **Ctrl_L W** (or Keypad **6**).

The window menu appears.

b. Select the Exit command by pressing **Space** (or Keypad **0**).

The tool closes.

—end—

Procedure 4-5
Changing user account passwords

Use this procedure to assign a password to a user who has forgotten his or her password. This password is propagated to all network elements (NE) where the user has been given access.

This procedure does not affect the current session if a user is logged in to the OPC when the user account password is changed. However, the new password must be used for the next login.

> **CAUTION**
> **Risk of security vulnerability**
> Root and root1 users have access to the UNIX passwd command. Do not use the passwd command to change an OPC password. The passwd command updates the password only on the OPC, not on the network elements.
>
> In addition, the new password is not subject to any security validation checks. For example, the passwd command allows you to enter a null password, which allows anyone to log in to that userID without a password. To change the root or root1 password, log in as root or root1 and use the Password Update tool as described in the procedure for changing your password in *OPC User Interface Description*, 323-3001-301, in this volume.

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the OPC with permission to use the OPC Centralized User Administration tool
- read the command conventions for the interface you are using (CMT or graphical) in *OPC User Interface Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool. *The Centralized User Administration tool main window appears.*

—continued—

Procedure 4-5 (continued)
Changing user account passwords

Step	Action
2	In the users list, move to the user account with the password you want to change, then press **Ctrl_A** (or Keypad **0**).
3	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).
4	Move to the Show user account info command, then press **Space** (or Keypad **0**). *The User Account Information dialog appears, showing the current status of the user account.*
5	Check to see if the password has expired or is still in effect, then select the **Done** button. *The User Account Information dialog closes.*
6	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).
7	Move to the Assign user password command, then press **Space** (or Keypad **0**). *The Password Update dialog appears.*
8	Enter a password for this user in the password field, then press **Return**. *The password must have from 5 to 8 characters. The first character must be alphabetic (a to z, A to Z). The remaining characters can be a to z, A to Z, 0 to 9, _ (underscore), or a $. Passwords must have at least one numeric character or one character from the set [_$]. The characters are not displayed as you enter them, but the cursor moves.* *When you press Return, the password field is checked. If the password is accepted, the password field label changes to “Retype new password”. Otherwise, an X appears next to the password field, and an error dialog indicates why the password was not accepted.*
9	Reenter the password, then press **Return**. *If this second password does not match the first password, then an error message appears.* Select the **OK** button to remove the message and redo the operation. *When the passwords match, the Assign Password dialog closes and the Centralized User Administration main window appears.*
10	To close the tool, press **Esc**), or do the following: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 4-6 **Enabling or disabling user accounts**

Use this procedure to enable or disable a user account. This procedure includes:

- disabling a user password to deny access to all network elements (NEs) and to the operations controller (OPC)
- enabling a user password after it has been disabled

Disabling in-use user accounts

OPC users

When you disable a user account being used for an 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 disable a user account being used for a NE session, be aware of the following consequences:

- the current NE session is not disturbed
- the user's password automatically expires upon logout
- the user account is disabled in 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

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the OPC with permission to use the OPC Centralized User Administration tool
- read the command conventions for the interface you are using (CMT or graphical) in *OPC User Interface Description*, 323-3001-301, in this volume
- check to see if the user account is logged in to any of its associated NEs. (If you do not know how to do this see Procedure 4-23 on page 4-71.)

—continued—

Procedure 4-6 (continued)
Enabling or disabling user accounts

CAUTION
If communications between the OPC and the NEs where the user account has access are not in operation, you can attempt to enable or disable the user account. However, the changes are not applied until the next user profile audit.

Action

Step **Action**

1 Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool.

The Centralized User Administration tool main window appears.

2 In the users list, move to the user account you want to disable, then press **Ctrl_A** (or Keypad **0**).

The selected user account is highlighted.

3 Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).

4 Select the Open command by pressing **Space** (or Keypad **0**).

The Edit User Profile dialog appears.

5 Check the Network View list to make sure all communication links with the NEs are in operation.

Note: A "?" beside an NE listed in the Network View indicates that communications between the OPC and that NE are not in operation. If you make changes that affect this NE, then an error dialog appears. You can continue or stop the operation.

6 After you review the Network View list, tab to the Cancel button, then press **Ctrl_A** (or Keypad **0**).

The Central User Administration main window appears.

7 To continue with this procedure, display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**). Otherwise, go to step 13.

8 To disable the user's password, move to the Disable command, then press **Space** (or Keypad **0**). Otherwise, go to step 10.

A confirmation dialog appears stating that you are disabling the selected user.

—continued—

Procedure 4-6 (continued)
Enabling or disabling user accounts

Step	**Action**
9	Tab to the Yes button, then press **Ctrl_A** (or Keypad **0**). *The main window appears with the user account shown as “Disabled.”* *If a user is logged in to any NEs using this account, an error message appears, indicating that the password could not be disabled for those NEs.* You can select Continue (if you want the disable operation to take affect at the next user profile audit) or Abort (to cancel the disable operation). Go to step 13.
10	To enable the user’s password, select the Enable command by pressing **Space** (or Keypad **0**). *The Assign Password dialog appears.*
11	Enter a password for this user in the password field, then press **Return**. *The password must have from 5 to 8 characters. The first character must be alphabetic (a to z, A to Z). The remaining characters can be a to z, A to Z, 0 to 9, _ (underscore), or a $. Passwords must have at least one numeric character or one character from the set [_$]. The characters are not displayed as you enter them, but the cursor moves.* *When you press Return, the password field is checked. If the password is accepted, the password field label changes to “Retype new password”. Otherwise, an X appears next to the password field, and an error dialog indicates why the password was not accepted.*
12	Reenter the password, then press Return. *If this second password does not match the first password, then an error message appears.* Select the **OK** button to remove the message and redo the operation. *When the passwords match, the Assign Password dialog closes and the Centralized User Administration main window appears.*
13	To close the tool, press **Esc**), or do the following: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 4-7
Enabling or disabling the root1 user account

Use this procedure to enable or disable the root1 user account for an operations controller (OPC). Root1 is a temporary user account used in situations such as the following:

- when a user requires root access privileges, but you do not want to give out the root password
- when the OPC User Session Manager is not available (for example, during upgrades or a failure of the OPC software load)

The root1 user is not intended to remain enabled for long periods of time. Therefore, you can disable the user account immediately, specify a set number of hours after which the root1 user is disabled, or accept the default that the account is disabled after 24 hours. If the root1 user is still logged in to the OPC when it is disabled, the user is not logged out.

The state of the root1 user on the primary OPC at the time of the most recent data synchronization from primary to backup determines the state of the root1 user on the backup OPC. For example, if the root1 user is disabled on the backup OPC and enabled on the primary OPC, a data synchronization causes the root1 user to be enabled on the backup OPC. Unless the state is manually changed, the state of the root1 user on the backup OPC remains as set by the most recent data synchronization until the next data synchronization occurs.

To enable the root1 user immediately on the backup OPC, enable the root1 user on the primary OPC, and then immediately perform a data synchronization to the backup OPC. The root1 user is enabled on the backup OPC.

When restoring an OPC database from tape, the state of the root1 user in the database determines its state on tape. For example, if the root1 user is enabled in the tape database, but disabled in the OPC database, the root1 user is enabled when the restore-from-tape operation is performed.

The OPC tracks the amount of time after which the root1 user is to be disabled independently of the tape restore operation. When the provisioned amount of time has passed since the root1 user was enabled, the root1 user is disabled, regardless of when the tape restore occurred. If the OPC is tracking the time period set for disabling the root1 user and the root1 user is disabled as the result of a tape restore before the time period expires, the time period expires in due course with no effect.

Procedure 4-7 (continued)
Enabling or disabling the root1 user account

Requirements

Before starting this procedure, you must log in to the OPC with root access privileges. For log-in instructions and an overview of the OPC user interface, see *OPC User Interface Description*, 323-3001-301.

Action

Step	Action
1	To enable the root1 user, enter the following command at the UNIX shell prompt: **enable_rlu -e** ↵ *A prompt appears for you to enter a password for the root1 user.*
2	Enter a password of your choice for the root1 user, then press the **Return** key. The password must comply with UNIX standards for passwords. *The root1 user is enabled. The root1 user is automatically scheduled to be disabled in 24 hours or as specified with the -t option (see step 3).* ***Note:*** The root1 user is not enabled on the backup OPC until a primary-to-backup OPC data synchronization has been performed.
3	To specify a set number of hours after which the root1 user is automatically disabled, enter the following command with any desired options at the UNIX shell prompt: **enable_rlu -t <hours>** ↵ *A prompt appears for you to enter a password for the root1 user.*
4	Enter a password of your choice for the root1 user, then press the **Return** key. The password must comply with UNIX standards for passwords. *The root1 user is scheduled to be disabled automatically in the number of hours specified with the -t option. The default, if the -t option is not used, is 24 hours.*
5	To disable the root1 user immediately, enter the following command at the UNIX shell prompt: **enable_rlu -d** ↵ *The root1 user is disabled.* ***Note:*** The root1 user is not disabled on the backup OPC until a primary-to-backup OPC data synchronization has been performed.
6	To display help for the enable_rlu command, enter the following command at the UNIX shell prompt: **enable_rlu -h** ↵

—end—

Procedure 4-8
Creating a new user group

Use this procedure to create additional user groups.

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the OPC with permission to use the OPC Centralized User Administration tool
- read the command conventions for the interface you are using (CMT or graphical) in *OPC User Interface Description*, 323-3001-301, in this volume

If you do not know which toolsets and tools are in the default groups, see the table at the beginning of this chapter.

Action

Step	Action
1	Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool. *The Centralized User Administration tool main window appears.*
2	Display the Configure menu by pressing **Ctrl_L T** (or Keypad **,**).
3	Select the Groups command by pressing **Space** (or Keypad **0**). *The Configure Groups dialog appears.*
4	If you want to display the list menu of the Groups list, press **Ctrl_L /** (or Keypad **3**). Otherwise, go to step 6.
5	Select the Create a new group command by pressing **Space** (or Keypad **0**). *The Create Group Profile dialog appears.* Go to step 8.
6	Move to the group you want to duplicate (using your arrow keys). Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).
7	Select the Duplicate command by pressing **Space** (or Keypad **0**). *The Create Group Profile dialog appears. The Description, Default NE Accessibility, and Default NE Access Class fields as well as the Current Toolsets list display information from the duplicated toolset profile.*
8	In the Group field, enter a unique name for the new user group. This field is required and can be up to 8 alphanumeric characters.
9	Tab to the Description field.

—continued—

Procedure 4-8 (continued)
Creating a new user group

Step	**Action**
10	To change the description, enter any text in the comment field (up to 40 characters) for example, the physical location of the user group. Otherwise, go to step 11.
11	Tab to the Default NE Accessibility field.
12	To select the default NE accessibility from the chooser, press **Ctrl_L** / (or Keypad **3**). Otherwise, go to step 14. ***Note:*** Changes made in this field do not affect the default user group that you copied.
13	Move to Yes or No, then press **Space** (or Keypad **0**). *The Accessibility column shows the change in accessibility.*
14	Tab to the Default NE Access Class field. You can select an Access Class value from the chooser menu, or leave the default value of "read". ***Note 1:*** Changes made in this field do not affect the user group that you copied. ***Note 2:*** All users created in this new group are given the default access class selected in this step.
15	To select an access from the chooser, display the chooser menu by pressing **Ctrl_L /** (or Keypad **3**). Otherwise, go to step 17.
16	Move to an option in the chooser, then press **Space** (or Keypad **0**). ***Note:*** Changes made in this field do not affect the default user group that you copied.
17	Tab to the Available Toolsets list and move to the toolsets that you want for your group.
18	Select the toolsets. For a single toolset selection, press **Ctrl_A** (or Keypad **0**). For multi-tool set selection, press **Ctrl_A** (or Keypad **0**) for the first item, then **Ctrl_Y** (or Keypad**.**) for subsequent items. *The toolsets are highlighted.*
19	Tab to the left Move button, then press **Ctrl_A** (or Keypad **0**). *The selected toolsets are removed from the Available Toolsets list and appear in the Current Toolsets list.*

—continued—

Procedure 4-8 (continued)
Creating a new user group

Step	Action

20 Verify the data you entered. Decide whether you want to save the data, exit the procedure without saving the data, or reenter the data.

If you want to	Then
save the data you entered	Go to step 21.
exit without saving the data	Tab to the Cancel button, then press **Ctrl_A** (or Keypad **0**). *No data is saved. The Create Group Profile dialog closes.* Go to step 24.
reenter the data	Go to step 2.

21 Tab to the OK button, then press **Ctrl_A** (or Keypad **0**).

The system checks all fields for errors, and, if none are found, a new user group is created. If an error is detected, an error dialog appears, indicating the reason for the error. An X appears at the beginning of the field that has the error and the cursor is returned to the field. Make the correction indicated, and re-execute this step.

If no errors are found, a confirmation dialog appears.

22 Tab to the Yes button, then press **Ctrl_A** (or Keypad **0**).

The Configure Groups dialog appears.

23 To return to the main window, tab to the Done button, then press **Ctrl_A** (or Keypad **0**).

Note: New groups are not displayed in the Centralized User Administration main window until a new user has been created within the new group.

24 To close the tool, press **Esc**), or do the following:

a. Display the window menu by pressing **Ctrl_L W** (or Keypad **6**).

The window menu appears.

b. Select the Exit command by pressing **Space** (or Keypad **0**).

The tool closes.

—end—

Procedure 4-9
Deleting a user group

Use this procedure to remove a user group.

Deleting a user group deletes all accounts in the group.

Deleting in-use user accounts

OPC users

When you delete a user account being used for an 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 NE session, be aware of the following consequences:

- the current NE session is not disturbed
- the user’s password automatically expires upon logout
- 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

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the operations controller (OPC) with permission to use the OPC Centralized User Administration tool
- read the command conventions for the interface you are using (CMT or graphical) in *OPC User Interface Description*, 323-3001-301, in this volume

CAUTION
You cannot delete the default groups. These groups are defined in Table 4-1 on page 4-3.

—continued—

Procedure 4-9 (continued)
Deleting a user group

Action

Step	Action
1	Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool. *The Centralized User Administration tool main window appears.*
2	Display the Configure menu by pressing **Ctrl_L T** (or Keypad **,**).
3	Select the Groups command by pressing **Space** (or Keypad **0**). *The Configure Groups dialog appears.*
4	Move to the user group that you want to delete, then press **Ctrl_A** (or Keypad **0**). *The user group is highlighted.*
5	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).
6	Move to the Delete command, then press **Space** (or Keypad **0**). *A confirmation dialog appears.*
7	Select the Yes button to delete the user group by pressing **Ctrl_A** (or Keypad **0**). *The user group and users of the group are deleted. The Configure Groups dialog appears.*
8	To return to the main window, tab to the Done button, then press **Ctrl_A** (or Keypad **0**). *The main window appears.*
9	To close the tool, press **Esc**), or do the following: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 4-10
Changing user group attributes

Use this procedure to change user group attributes. You can change group attributes such as the comments assigned to a user group and the group's default access class.

> **CAUTION**
> You cannot change the current Toolsets list of the default groups. These groups are defined in Table 4-2 on page 4-4.

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the operations controller (OPC) with permission to use the OPC Centralized User Administration tool
- read the command conventions for the interface you are using in *OPC User Interface Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool. *The Centralized User Administration tool main window appears.*
2	Display the Configure menu by pressing **Ctrl_L T** (or Keypad **,**).
3	Select the Groups command by pressing **Space** (or Keypad **0**). *The Configure Groups dialog appears.*
4	Move to the group you want to modify, then display the list item menu of the Groups list by pressing **Ctrl_L** (or Keypad **Enter**).
5	Select the Open command by pressing **Space** (or Keypad **0**). *The Edit Group Profile dialog appears.* ***Note:*** You cannot change the Group Name when changing a user group's attributes.
6	Tab to the Description field.
7	To change the Description field, display the field menu by pressing **Ctrl_L** (or Keypad **Enter**). Otherwise, go to step 10.
8	Select the Select all command by pressing **Space** (or Keypad **0**). *The Description field appears in reverse video.*

—continued—

Procedure 4-10 (continued)
Changing user group attributes

Step	Action
9	Enter any text in the Description field (up to 40 characters); for example, the physical location of the user group. *The original text is replaced by the new text.*
10	Tab to the Default NE Accessibility field.
11	To select the default NE accessibility, from the chooser, press **Ctrl_L** / (or Keypad **3**). Otherwise, go to step 13. ***Note:*** Changes made in this field do not affect the default user group that you copied.
12	Move to Yes or No, then press **Space** (or Keypad **0**). *The Accessibility column shows the change in accessibility.*
13	Tab to the Default NE Access Class field. You can select an Access Class value from the chooser menu, or leave the current value. ***Note:*** All users created in this new group are given the default access class selected in this step.
14	To select an access from the chooser, display the chooser menu by pressing **Ctrl_L /** (or Keypad **3**). Otherwise, go to step 16.
15	Move to an option in the chooser, then press **Space** (or Keypad **0**). *The Default NE Access Class will change to the selected value.* ***Note:*** Changes made in this field do not affect the default user group that you copied.
16	Tab to the Available Toolsets list (or Current Toolsets list) and move to the toolsets that you want to add to (or remove from) your group.
17	Select the toolsets. For a single toolset selection, press **Ctrl_A** (or Keypad **0**). For multi-tool set selection, press **Ctrl_A** (or Keypad **0**) for the first item, and then **Ctrl_Y** (or Keypad **.**) for subsequent items. *The toolsets are highlighted.*
18	Tab to the left or right Move button, then press **Ctrl_A** (or Keypad **0**). *The selected toolsets are removed from the Available Toolsets list (or Current Toolsets list) and appears in the Current Toolsets list (or Available Toolsets list).*

—continued—

Procedure 4-10 (continued)
Changing user group attributes

Step **Action**

19 Verify the data you entered. Decide whether you want to save the data, exit the procedure without saving the data, or reenter the data.

If you want to	Then
save the data you entered	Go to step 20.
exit without saving the data	Tab to the Cancel button, then press **Ctrl_A** (or Keypad **0**). *No data is saved. The Edit Group Profile dialog closes.* Go to step 22.
reenter the data	Go to step 6.

20 Tab to the OK button, then press **Ctrl_A** (or Keypad **0**).

All fields are checked for errors.

If no errors are found, then a confirmation dialog appears.

21 Tab to the Yes button, then press **Ctrl_A** (or Keypad **0**).

The Configure Groups dialog appears.

22 To return to the main window, select the Done button by pressing **Ctrl_A** (or Keypad **0**).

23 To close the tool, press **Esc**), or do the following:

a. Display the window menu by pressing **Ctrl_L W** (or Keypad **6**).

The window menu appears.

b. Select the Exit command by pressing **Space** (or Keypad **0**).

The tool closes.

—end—

Procedure 4-11
Creating a new toolset

Use this procedure to create a new toolset.

Requirements

This procedure requires a user account and password that permit access to the operations controller (OPC) with permission to use the OPC Centralized User Administration (CUA tool).

> ***Note 1:*** For command conventions for the interface you are using, see *OPC User Interface Description*, 323-3001-301, in this volume.
>
> ***Note 2:*** If you do not know which toolsets and tools are in the default groups, see Table 4-1 on page 4-3.

Action

Step **Action**

1 Log in to the OPC, display the User Session Manager, and open the CUA tool.

The Centralized User Administration tool main window appears.

2 To display the Configure menu, press **Ctrl_L T** (or Keypad **,**).

The Configure Utilities menu appears.

3 Move to the Toolsets command, then press **Space** (or Keypad **0**).

The Configure Toolsets dialog appears.

4 To create a completely new toolset, display the Toolsets list menu by pressing **Ctrl_L /** (or Keypad **3**). Otherwise, go to step 6 to create a new toolset by duplicating an existing one.

The list menu appears.

5 To select the Create a new toolset command, press **Space** (or Keypad **0**).

The Create Toolset Profile dialog appears.

Go to step 8.

6 To create a new toolset by duplicating an existing one, use the arrow keys to move to the Toolset you want to duplicate, then press **Ctrl_L** (or Keypad **Enter**) to display the list item menu.

7 To select the Duplicate command, press **Space** (or Keypad **0**).

The Create Toolset Profile dialog appears. The Toolset Title and Detail fields as well as the Current Tools list display information from the duplicated toolset profile.

8 In the Toolset name field (up to 20 alphanumeric characters), enter a unique name for the new toolset. This is required.

—continued—

Procedure 4-11 (continued)
Creating a new toolset

Step	**Action**

9 Tab to the Toolset Title field.

10 Enter the text (up to 20 characters) that you want displayed in the User Session Manager tool (specifically, in the Available Tools list).

Note: The toolset has to be assigned to a group to appear in the Available Tools list.

11 Tab to the Detail field.

12 Enter text that describes the function of the toolset.

13 Tab to the Available Tools list and move to the tools you want to include in the toolset.

Note: The Connection Manager tool has read/write access. The Connection Manager (R) tool has read-only access.

14 Complete the following substeps to select the tools:

a. To select a single tool, press **Ctrl_ A** (or Keypad **0**).

b. To select multiple tools, press **Ctrl_A** (or Keypad 0) for the first tool, then press **Ctrl_Y** (Keypad **.**) for subsequent tools.

The tools are highlighted.

15 Tab to the left Move button, then press **Ctrl_A** (or Keypad **0**).

The selected tools are removed from the Available Tools list and appear in the Current Tools list.

16 Complete the instructions in the following table:

If you want to	**Then**
save the data you entered	go to step 17.
exit without saving the data	Tab to the Cancel button and press **Ctrl_A** (or Keypad **0**). *No data is saved. The Create Toolset Profile dialog closes.* Go to step 20.
reenter the data	go to step 6.

17 Tab to the OK button and press **Ctrl_A** (or Keypad **0**).

The system checks all fields for errors and, if none are found, a new user group is created. If an error is detected, an error dialog appears, indicating the reason for the error. An X appears at the beginning of the field that has the error and the cursor is returned to the field. Make the correction indicated, and re-execute this step.

If no errors are found, then a confirmation dialog appears.

—continued—

Procedure 4-11 (continued)
Creating a new toolset

Step	Action
18	Tab to the Yes button, then press **Ctrl_A** (or Keypad **0**). *The Configure Toolsets dialog appears with the new toolset displayed in the list of available toolsets.*
19	To return to the main window, tab to the Done button, then press **Ctrl_A** (or Keypad **0**). *The main window appears.*
20	To close the tool, select one of the following substeps: **a.** Press **Esc)** to close the tool. **b.** Press **Ctrl_L W** (or Keypad **6**) to display the window menu. **c.** Press **Space** (or Keypad **0**) to select the Exit command.

—end—

Procedure 4-12
Changing an existing toolset

Use this procedure to change the attributes of an existing toolset.

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the OPC with permission to use the OPC Centralized User Administration tool
- read the command conventions for the interface you are using in *OPC User Interface Description*, 323-3001-301, in this volume

If you do not know which toolsets and tools are in the default groups, see the table at the beginning of this chapter.

Action

Step	Action
1	Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool. *The Centralized User Administration tool main window appears.*
2	Display the Configure menu by pressing **Ctrl_L T** (or Keypad **,**).
3	Move to the Toolsets command, then press **Space** (or Keypad **0**). *The Configure Toolsets dialog appears.*
4	Move to the toolset you want to modify, then display the list item menu of the Toolsets list by pressing **Ctrl_L** (or Keypad **Enter**).
5	Select the Open command by pressing **Space** (or Keypad **0**). *The Edit Toolset Profile dialog appears.* ***Note:*** The Toolset Name cannot be changed when changing a toolset’s attributes.
6	In the Toolset Title field, enter the text (up to 20 characters) that you want displayed in the User Session Manager tool (specifically, in the Available Tools list). *The original text is replaced by the new text.*
7	Tab to the Detail field.
8	Enter any text you want to describe the function of the toolset.
9	Tab to the Current Tools list or Available Tools list, and go to the tools that you want to move. ***Note:*** The Connection Manager tool has read/write access. The Connection Manager (R) tool has read-only access.

—continued—

Procedure 4-12 (continued)
Changing an existing toolset

Step	Action
10	Select the tools.
	For a single tool selection, press **Ctrl_A** (or Keypad **0**). For multi-tool selection, press **Ctrl_A** (or Keypad **0**) for the first item, then press **Ctrl_Y** (or Keypad **.**) for subsequent items.
	The tools are highlighted.
11	Tab to the left or right Move button (depending on the tools you want in your Current Tools list), then press **Ctrl_A** (or Keypad **0**).
	The selected tools are removed from the Available Tools list and appears in the Current Tools list, or vice versa.
12	Verify the data you entered. Decide whether you want to save the data, exit the procedure without saving the data, or reenter the data.

If you want to	Then go to
save the data you entered	step 15
exit without saving the data	step 13
reenter data	step 6

Step	Action
13	Tab to the Cancel button, then press **Ctrl_A** (or Keypad **0**).
	A confirmation dialog appears.
14	Tab to the Yes button, then press **Ctrl_A** (or Keypad **0**).
	No data is saved. The Edit Toolset Profile dialog closes. The Configure Toolsets dialog appears.
	Go to step 17.
15	Tab to the OK button, then press **Ctrl_A** (or Keypad **0**).
	The system checks all fields for errors. If none are found, the toolset changes are saved. If an error is detected, an error dialog appears, indicating the reason for the error. Make the correction indicated, and re-execute this step.
	If no errors are found, then a confirmation dialog appears.
16	Tab to the Yes button, then press **Ctrl_A** (or Keypad **0**).
	The Edit Toolset Profile dialog appears.
17	To return to the main window, tab to the Done button, then press **Ctrl_A** (or Keypad **0**).
	The Configure Toolsets dialog is removed, and the main window appears.

—continued—

Procedure 4-12 (continued)
Changing an existing toolset

Step	Action
18	To close the tool, press **Esc**), or do the following: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 4-13
Deleting a toolset

Use this procedure to delete an existing toolset. You cannot delete default toolsets.

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the operations controller (OPC) with permission to use the OPC Centralized User Administration tool
- read the command conventions for the interface you are using in *OPC User Interface Description*, 323-3001-301, in this volume

If you do not know which toolsets and tools are in the default groups, see Table 4-2 on page 4-4 and Table 4-3 on page 4-7.

Action

Step	Action
1	Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool. *The Centralized User Administration tool main window appears.*
2	Display the Configure menu by pressing **Ctrl_L T** (or Keypad **,**).
3	Move to the Toolsets command, then press **Space** (or Keypad **0**). *The Configure Toolsets dialog appears.*
4	Select the toolset that you want to delete.
5	Display the list item menu of the Toolsets list by pressing **Ctrl_L** (or Keypad **Enter**).
6	Select the Delete command by pressing **Space** (or Keypad **0**). *A confirmation dialog appears.*
7	Select the Yes button to delete the toolset by pressing **Ctrl_A** (or Keypad **0**). *The toolset is deleted. All references to this toolset from all groups profiles are removed. The confirmation dialog is removed, and the Configure Toolsets dialog appears.*
8	To return to the main window, tab to the Done button, then press **Ctrl_A** (or Keypad **0**). *The main window appears.*

—continued—

Procedure 4-13 (continued)
Deleting a toolset

Step	**Action**
9	To close the tool, press **Esc**), or do the following: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 4-14
Creating auto-start tools for user groups

Use this procedure to create auto-start tools.

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the operations controller (OPC) with permission to use the OPC Centralized User Administration tool
- read the command conventions for the interface you are using in *OPC User Interface Description*, 323-3001-301, in this volume

If you do not know which toolsets and tools are in the default groups, see the table at the beginning of this chapter.

Action

Step	Action
1	Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool. *The Centralized User Administration tool main window appears.*
2	Display the Configure menu by pressing **Ctrl_L T** (or Keypad **,**).
3	Select the Groups command by pressing **Space** (or Keypad **0**). *The Configure Groups dialog appears.*
4	Move to the group for which you want to configure the auto-start tools.
5	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**). *The list item menu appears.*
6	Move to the Configure auto-start tools command, then press **Space** (or Keypad **0**). *The Configure Auto-Start Tools dialog appears.*
7	Tab to the Auto-Start Tools list or the Available Tools list and, using the down arrow key, move to the tool that you want to place in the other list.
8	Select the tool by pressing **Ctrl_A** (or Keypad **0**). *The tool is highlighted.*

—continued—

Procedure 4-14 (continued)
Creating auto-start tools for user groups

Step	Action
9	Tab to the left or right Move button (depending on the tools you want in your Auto-Start Tools list), then press **Ctrl_A** (or Keypad **0**). *The selected tools appear in the Auto-Start Tools list. The tool name that has been added to the Auto-Start Tools list is shown in the Tool Name field, and the number of instances currently operating for that tool is shown in the Instance field.*
10	Verify the data you entered. Decide whether you want to save the data, exit the procedure without saving the data, or reenter the data.

If you want to	Then
save the data you entered	Go to step 11.
exit without saving the data	Tab to the Cancel button, then press **Ctrl_A** (or Keypad **0**). *If you have not made any changes, the Configure Auto-Start Tools dialog closes, and the Configure Groups dialog appears. If you have made changes, a confirmation dialog appears asking you whether you want to save the changes you made.* Select **Yes** (to complete the cancel operation) or **No** (to discontinue the operation). The Configure Auto-Start Tools dialog closes, and you are returned to the Configure Groups dialog. Go to step 13.
reenter the data	Go to step 7.

11 Tab to the OK button, then press **Ctrl_A** (or Keypad **0**).

A confirmation dialog appears.

12 Tab to the Yes button, then press **Ctrl_A** (or Keypad **0**).

The Configure Groups dialog appears.

13 Tab to the Done button, then press **Ctrl_A** (or Keypad **0**).

The main window appears.

14 To close the tool, press **Esc**), or do the following:

a. Display the window menu by pressing **Ctrl_L W** (or Keypad **6**).

The window menu appears.

b. Select the Exit command by pressing **Space** (or Keypad **0**).

The tool closes.

—end—

Procedure 4-15 **Managing system parameters**

Use this procedure to change system security parameters for all user accounts and user groups (both default and non-default). These system parameters include

- accreditation period (Passwords that are assigned by the system administrator can have an accreditation period associated with them. This period defines the maximum number of days the assigned password can be used before the user must assign a new password.)
- password expiration period (Passwords that are assigned by the user owner can have an expiration period associated with them. This period defines the maximum number of days the user can use the specified password.)
- password obsolescence interval (the number of days before a previously used password can be reused)
- passwords that are unacceptable

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the operations controller (OPC) with permission to use the OPC Centralized User Administration tool
- read the command conventions for the interface you are using in *OPC User Interface Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool. *The Centralized User Administration tool main window appears.*
2	Display the Configure menu by pressing **Ctrl_L T** (or Keypad **,**). *The Configure menu appears.*
3	Move to the Security Parameters command, then press **Space** (or Keypad **0**). *The Configure System Parameters dialog appears.*
4	Enter the number of days (from 0 to 30 inclusive) that an “assigned” password can be used before the user must change it. ***Note:*** Leaving this field blank disables this feature.

—continued—

Procedure 4-15 (continued)
Managing system parameters

Step	Action
5	Tab to the Password expiration period field and enter the number of days (from 30 to 365 inclusive) that the user can use the new password that they have specified. ***Note:*** Leaving this field blank disables this feature.
6	Tab to the Password obsolescence interval field.
7	Enter the number of days (a value from 30 through 360) the user cannot reuse a password. ***Note:*** Leaving this field blank disables this feature.
8	Tab to the Password change notify period field and enter the number of days of notification users receive before their passwords expire. You can enter a value of 0 to 14. A value of 0 means no notification occurs before the password expires. A value of 1 to 14 means the user receives a notification on logging in that the password is going to expire in that number of days. The default period is 14 days. ***Note:*** To disable the password change notification feature, you can enter either 0 or delete any characters in the field (such as the number 14 displayed by default).
9	If you want to change the value from the default, tab to the OPC field under the heading Maximum invalid login attempts. There is a default of three invalid log-in attempts that can be made from an OPC user interface port (port B or Esp 1) before the port is locked out. Port B is a physical RS-232 connector on the AccessNode. They both map to port B in the OPC Port Configuration tool. Esp 1 is the label of the physical connector on the AccessNode that maps to port 3 in the OPC Port Configuration tool. ***Note:*** If you do not want the OPC ports to be locked out if suspected intrusion attempts occur, set the duration of alert condition to 0, as described in steps 11 through 13.
10	If you want to change the value from the default, tab to the NE field under the heading Maximum invalid login attempts. You can enter a value of 2 to 9. There is a default of 3 invalid log-in attempts that can be made from a network element user interface port (1, 2, 3, or 4) before the port is locked out. ***Note:*** If you do not want the network element ports to be locked out in the event of suspected intrusion attempts, set the duration of alert condition to 0, as described in steps 14 through 16.
11	Tab to the OPC field under the heading Duration of alert condition (sec).
12	Enter a value of 0 to 180 to specify the length of time in seconds that a user interface port on the OPC is locked out after a suspected intrusion attempt.

—continued—

Procedure 4-15 (continued)
Managing system parameters

Step	Action
13	At the end of this period of time, the port is free to be used. If you enter 0, the port is not locked out if a suspected intrusion attempt occurs.
	Note: Leaving this field blank disables this feature.
14	Tab to the NE field under the heading Duration of alert condition (sec).
15	Enter a value of 0 to 180 to specify the length of time in seconds that a user interface port on the NE is locked out after a suspected intrusion attempt.
16	At the end of this period of time, the port is free to be used. If you enter 0, the port is not locked out if a suspected intrusion attempt occurs.
	Note: Leaving this field blank disables this feature.
17	Tab to the Unacceptable Passwords list, which contains the passwords that cannot be used.
18	To delete passwords, select the passwords that you want deleted. Otherwise, go to step 21.
	For a single selection, press **Ctrl_A** (or Keypad **0**). For multi-tool selection, press **Ctrl_A** (or Keypad **0**) for the first item, and then press **Ctrl_Y** (or Keypad **.**) for subsequent items.
	The passwords are highlighted.
19	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).
20	Select the Delete command by pressing **Space** (or Keypad **0**).
	The selected passwords are deleted from the list.
21	To enter a new unacceptable password, tab to the Enter new unacceptable password field. Otherwise, go to step 23.
22	Enter the unacceptable password into this field, then press **Return**.
	The unacceptable password is added to the Unacceptable Passwords list.
	Repeat steps 21 and 22 to enter additional unacceptable passwords.

—continued—

Procedure 4-15 (continued)
Managing system parameters

Step	**Action**
23	Verify all the data you entered. Decide whether you want to save the data, exit the procedure without saving the data, or reenter the data.

If you want to	**Then**
save the data you entered	Tab to the OK button, then press **Ctrl_A** (or Keypad **0**). A confirmation dialog appears, asking you whether you want to save. Select yes to save. *The dialog closes, and the Centralized User Administration main window appears.* Go to step 24.
exit without saving the data	Tab to the Cancel button, then press **Ctrl_A** (or Keypad **0**). *If you have not made any changes, the dialog closes, and you are returned to the main window.* *If you have made changes, a confirmation dialog appears asking you whether you want to save the changes you made.* Select Yes (to complete the cancel operation) or No (to discontinue the cancel operation). *The main window appears.* Go to step 24.
add another unacceptable password	Go to step 21.
reenter the data	Go to step 4.

24 To close the tool, press **Esc**), or do the following:

a. Display the window menu by pressing **Ctrl_L W** (or Keypad **6**).

The window menu appears.

b. Select the Exit command by pressing **Space** (or Keypad **0**).

The tool closes.

—end—

Procedure 4-16
Moving users between user groups

Use this procedure to move a user account from one user group to another.

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the operations controller (OPC) with permission to use the OPC Centralized User Administration tool
- read the command conventions for the interface you are using in *OPC User Interface Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool. *The Centralized User Administration tool main window appears.*
2	Move to the user account that you want to move, then press **Ctrl_A** (or Keypad **0**). *The selected user account is highlighted.*
3	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).
4	Select the Open command by pressing **Space** (or Keypad **0**). *The Edit User Profile dialog appears.*
5	Tab to the Group field. *The entire field is highlighted in reverse video.*
6	Enter the name of the group where you want to copy the selected user account. *The information is replaced by the new information as soon as you begin entering it.*
7	Tab to the OK button, then press **Ctrl_A** (or Keypad **0**). *The information you provided is verified. A confirmation dialog appears.*
8	To commit the user account move, tab to the Yes button, then press **Ctrl_A** (or Keypad **0**). *The confirmation dialog and Edit User Profile dialog disappear.*

—continued—

Procedure 4-16 (continued)
Moving users between user groups

Step	**Action**
9	To close the tool, press **Esc**), or do the following: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 4-17
Sorting the users list

Use this procedure to sort the list of user accounts, displayed in the main window of the Centralized User Administration tool.

The users list can be sorted alphabetically according to the information in the User Id, Group, Status, User Name, or Detail columns.

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the operations controller (OPC) with permission to use the OPC Centralized User Administration tool
- read the command conventions for the interface you are using in *OPC User Interface Description*, 323-3001-301, in this volume

Action

Step **Action**

1 Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool.

The Centralized User Administration tool main window appears.

2 Display the users list menu by pressing **Ctrl_L /** (or Keypad **3**).

3 Move to the Sort command.

A cascade menu appears, showing the attributes you can use to sort the list.

4 Move to the cascade menu by pressing the right arrow key.

5 Move to the desired sorting attribute, then press **Space** (or Keypad **0**).

The list is redisplayed sorted by the order of the selected attribute. The Users sorted by field displays the selected attribute.

Note: If the list is empty, the Sort command is disabled.

6 To close the tool, press **Esc**), or do the following:

a. Display the window menu by pressing **Ctrl_L W** (or Keypad **6**).

The window menu appears.

b. Select the Exit command by pressing **Space** (or Keypad **0**).

The tool closes.

—end—

Procedure 4-18
Filtering the users list

Use this procedure to filter the list of user accounts, displayed in the main window of the Centralized User Administration tool.

The users list can be filtered to show all user groups or only selected user groups.

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the operations controller (OPC) with permission to use the OPC Centralized User Administration tool
- read the command conventions for the interface you are using in *OPC User Interface Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool. *The Centralized User Administration tool main window appears.*
2	Display the users list menu by pressing **Ctrl_L /** (or Keypad **3**).
3	Move to the Filter command, then press **Space** (or Keypad **0**). *The Filter Users List dialog appears. The dialog shows the current settings.*
4	To show all groups, select the Show all Groups radio button by pressing **Ctrl_A** (or Keypad **0**). Otherwise, go to step 5. *A diamond shape (showing that the button has been selected) appears beside the Show all Groups radio button.* Go to step 10.
5	Move to the Show Included Groups radio button using the arrow keys, then press **Ctrl_A** (or Keypad **0**). *A diamond shape (showing that the button has been selected) appears beside the Show Included Groups radio button.*
6	Tab to the Group List, then select the group that you want included in the users list display. For a single selection, press **Ctrl_A** (or Keypad **0**). For multi-Group selection, press **Ctrl_A** (or Keypad **0**) for the first item, and then press **Ctrl_Y** (or Keypad **.**) for subsequent items.

—continued—

Procedure 4-18 (continued)
Filtering the users list

Step	Action
7	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).
8	To add or remove a group, press **Space** (or Keypad **0**) at the Add or Remove command as appropriate. *If you selected Add, then the word “Included” appears next to the group in the Group list. If you selected Remove, then the words “Not Included” appear next to the group.*
9	Verify all the data you entered. Decide whether you want to apply the data, exit the procedure and save the data, or cancel it.

If you want to	**Then**
apply the data you entered (and stay in dialog and make other changes)	Go to step 10.
exit and save the data	Go to step 11.
exit without saving the data (or cancel)	Tab to the Cancel button, then press **Ctrl_A** (or Keypad **0**). The dialog closes, and the main window appears. No changes are saved. Go to step 12.

Step	Action
10	Tab to the Apply button, then press **Ctrl_A** (or Keypad **0**). *The changes are applied to the list, and you remain in the dialog.* Go to step 4 and continue with changes.
11	Tab to the OK button, then press **Ctrl_A** (or Keypad **0**). *The changes are made and the dialog is removed. You are returned to the Centralized User Administration main window.*
12	To close the tool, press **Esc**), or do the following: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 4-19
Auditing user profile data

Use this procedure to audit the user profile data.

The user profile data audit is used to resolve any inconsistencies between the operations controller (OPC) and the network element (NE) in its span of control. (Note that the data maintained on the OPC is viewed as the master data.)

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the OPC with permission to use the OPC Centralized User Administration tool
- read the command conventions for the interface you are using in *OPC User Interface Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool. *The Centralized User Administration tool main window appears.*
2	Display the Utilities menu by pressing **Ctrl_L T** followed by a **+** (or Keypad **2** for global menu, then use the arrow key to move down to Utilities).
3	Select the Audit user profile data command by pressing **Space** (or Keypad **0**). *A dialog appears that indicates user profile data is being transferred to the network elements.*
4	To stop the transfer, tab to the No button, then press **Ctrl_A** (or Keypad **0**). Otherwise, go to step 5. *The dialog is removed and the Centralized Security Administration main window appears.* Go to step 7.
5	Tab to the Yes button, then press **Ctrl_A** (or Keypad **0**). *If the audit was successfully completed at all network elements, the Centralized User Administration main window appears.* Go to step 7. *If the audit was not successfully completed at all network elements, a warning appears.*

—continued—

Procedure 4-19 (continued)
Auditing user profile data

Step	Action
6	Press the **OK** button to remove the warning. *The Centralized User Administration main window appears.*
7	To close the tool, press **Esc**), or do the following: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 4-20
Scheduling a user profile audit

Use this procedure to schedule automatic user profile audits.

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the operations controller (OPC) with permission to use the OPC Centralized User Administration tool
- read the command conventions for the interface you are using in *OPC User Interface Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool.
	The Centralized User Administration tool main window appears.
2	Display the Utilities menu by pressing **Ctrl_L T** followed by a **+** (or Keypad **2** for the global menu, then use an arrow key to move down to Utilities).
3	Move to the Schedule audit command, then press **Space** (or Keypad **0**).
	A Schedule User Profile Audit dialog appears.
4	To change this field, enter a number from **1** to **23** (for hours) or **1** to **7** (for days). Otherwise, go to step 5.
5	Tab to the options (minute(s), hour(s), day(s)).
6	To select an option, move to the desired button using the arrow keys, then press **Ctrl_A** (or Keypad **0**). Otherwise, go to step 7.
	A diamond shape appears in the button, signifying that the option has been chosen.
7	Tab to the Next run fields (hh:mm).
8	To change these fields, enter the hours (01 to 23) and the months (00 to 59). Otherwise, go to step 9.
9	Tab to the Next run fields (mm/dd/yyyy).
10	To change these fields, enter the month (mm) (0 to 12), the day (dd) (01 to 31), and the year (199x).Otherwise, go to step 11.
	If you want today’s or tomorrow’s date, use the chooser by pressing **Ctrl_L /** (or Keypad **3**) and choosing today or tomorrow as required. (The date is restricted to either today’s or tomorrow’s date.)
11	Tab to the Default button.

—continued—

Procedure 4-20 (continued)
Scheduling a user profile audit

Step	Action
12	To apply the default, select the Default button by pressing **Ctrl_A** (or Keypad **0**). Otherwise, go to step 13. *All the entries in the fields are set to the default values.*
13	Verify the data you entered. Decide whether you want to save the data or exit the procedure without saving the data.

If you want to	Then
save the data you entered	Go to step 14.
exit without saving the data	Tab to the Cancel button, then press **Ctrl_A** (or Keypad **0**). *The Centralized Security Administration main window appears.* Go to step 15.

Step	Action
14	Tab to the Yes button, then press **Ctrl_A** (or Keypad **0**). *The dialog is removed and the Centralized Security Administration main window appears.*
15	To close the tool, press **Esc**), or do the following: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 4-21
Transferring user profile data to the backup OPC

Use this procedure to transfer user profile data to the backup operations controller (OPC) so the backup OPC has the identical user profile data as the primary OPC.

Requirements

Before starting this procedure, you must:

- obtain a user account and password that permit access to the OPC with permission to use the OPC Centralized User Administration tool
- read the command conventions for the interface you are using in *OPC User Interface Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC, display the User Session Manager, and open the Centralized User Administration tool.
	The Centralized User Administration tool main window appears.
2	Display the Utilities menu by pressing **Ctrl_L T** followed by a **+** (or Keypad **2** for the global menu, then use an arrow key to move down to Utilities).
	The Utilities menu appears.
3	Move to the Transfer data to backup OPC command, then press **Space** (or Keypad **0**).
	A confirmation dialog appears after the transfer operation is confirmed, stating that you should refer to the Event Browser tool.
4	To remove the message, select the OK button by pressing **Ctrl_A** (or Keypad **0**).
5	To close the tool, press **Esc**), or do the following:
	a. Display the window menu by pressing **Ctrl_L W** (or Keypad **6**).
	The window menu appears.
	b. Select the Exit command by pressing **Space** (or Keypad **0**).
	The tool closes.

—end—

Procedure 4-22
Listing all authorized userIDs on the NE

Use this procedure to list all users who have access to the network element (NE) in context.

Requirements

Before starting this procedure, you must:

- read the command conventions for the NE user interface in *Network Element User Interface Description*, 323-3001-300, in this volume
- be logged in to the NE user interface

  Note: This command is available only to users with access class Read/Write/Admin.

Action

Step	Action
1	You can list all users from any NE user interface menu by entering: **show users** ↵ *A screen that lists users who have access to the NE under the "show users" title at the bottom of the screen appears.*

—end—

Procedure 4-23
Listing all users logged in to the NE

Use this procedure to list all users who are logged in to the network element (NE) in context.

Requirements

Before starting this procedure, you must:

- read the command conventions for the network element user interface (NEUI) in *Network Element User Interface Description*, 323-3001-300, in this volume
- be logged in to the NEUI

Note: This command is available to users with access class Read, Read/Write, or Read/Write/Admin.

Action

Step	Action
1	From any NE user interface menu, you can list all users logged in to the NE in context by entering: **print users** ↵ *A screen that lists users who are logged in to the NE under the “print users” title at the bottom of the screen appears.*

—end—

Procedure 4-24
Listing all users logged in to the NE and the device

Use this procedure to list all users who are logged in to the network element (NE) in context and the device to which they are attached.

Requirements

Before starting this procedure, you must:

- read the command conventions for the network element user interface (NEUI) in *Network Element User Interface Description*, 323-3001-300, in this volume
- be logged in to the NEUI

  Note: This command is available to users with access class Read, Read/Write, or Read/Write/Admin.

Action

Step	Action
1	You can list all users logged in to the NE in context, and the device to which they are attached, from any NE user interface menu by entering: **quser** ↵ *A screen appears when this procedure has been completed.*

—end—

Procedure 4-25
Displaying the userID logged in at a terminal

Use this procedure to determine who is logged in to a terminal.

Requirements

Before starting this procedure, you must:

- read the command conventions for the network element user interface (NEUI) in *Network Element User Interface Description*, 323-3001-300, in this volume
- be logged in to the NEUI

Note: This command is available to users with access class Read, Read/Write, or Read/Write/Admin.

Action

Step	Action
1	From any NE user interface menu, you can determine who is logged in to a terminal by entering: **quit all; mapci** ↵ *A screen appears when this procedure has been completed. The user account currently logged in is listed below the MAPCI menu.*
2	To return to the NE user interface main menu, enter: **fwpui** ↵

—end—

Procedure 4-26
Logging out another userID

Use this procedure to log in to a network element (NE), either locally or remotely (by the rlogin command), and log out another user who is already logged in to the same NE.

Requirements

Before starting this procedure, you must:

- read the command conventions for the network element user interface (NEUI) in *Network Element User Interface Description*, 323-3001-300, in this volume
- be logged in to the NEUI

  Note: This command is only available to users with access class Read/Write/Admin.

Action

Step	Action
1	Move the cursor to the first column in the command input area.
2	To log out a user, enter:

forceout <userid> ↵

where:

<userid> is a string of 1 to 8 characters.

Note: To prevent an unauthorized user from accessing the system, use the Centralized User Administration tool on the operations controller (OPC) to change the password of the account. Therefore, the unauthorized user cannot log on to the same NE, a different NE, or the OPC at a later time.

—end—

Cluster inventory

This chapter describes the Cluster Inventory tool and explains how to perform procedures that use the Cluster Inventory tool.

Chapter task list

This chapter includes the following tasks:

Procedure	Task	See
5-1	Generating inventory reports	page 5-11
5-2	Generating summary reports	page 5-14
5-3	Managing reports	page 5-17
5-4	Updating the database	page 5-20
5-5	Searching through inventory reports	page 5-22
5-6	Sorting an inventory report	page 5-24

If you cannot complete these procedures, contact your next level of support.

Definitions

Table 5-1 defines terms that are commonly used in this chapter.

Table 5-1
Commonly used terms

Term	Description
Cluster	Refers to the operations controller (OPC) span of control.
Cluster Inventory tool	Permits generation of a variety of reports on the hardware components in the cluster. The tool uses the network element (NE) data in the OPC database as its information source. Seven search criteria are available that can be used individually or combined in any way.
Domain	Refer to one of the four tiers where the Cluster Inventory tool groups the hardware components. A report at the NE domain level supplies overview information for the NEs. A report at the slot domain level offers more details on every slot.
Reports	Display as on-screen tables and are generated using the OPC screen. The two types of reports are inventory reports and summary reports.

Domain structure

The following figure shows the four domains for the Cluster Inventory tool. Table 5-2 explains each domain.

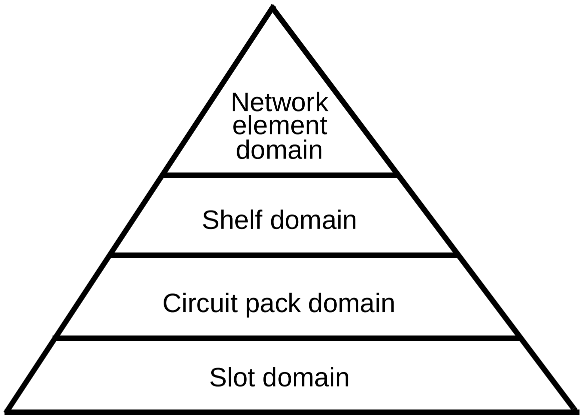


Table 5-2
Explanation of the domains for the Cluster Inventory Tool

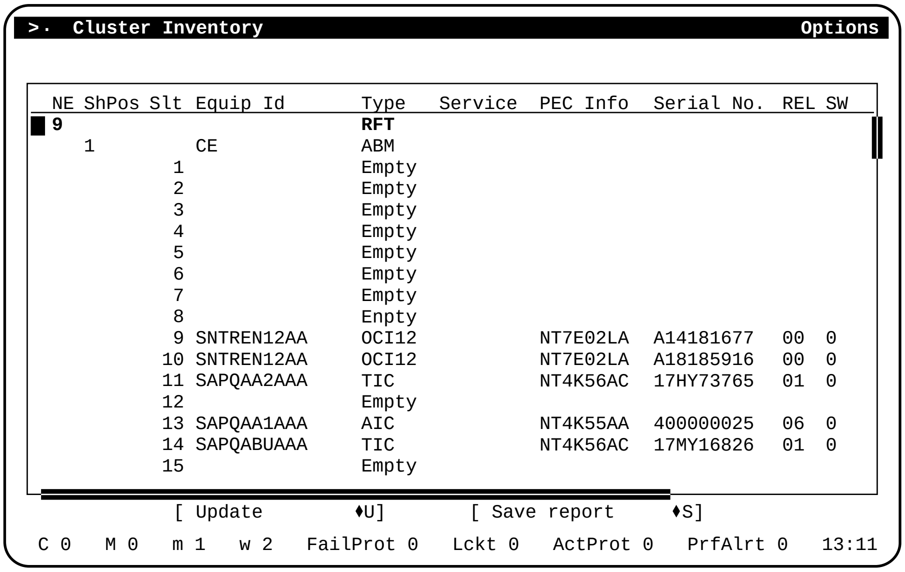
Cluster Inventory tool domains	Description of the four domains
Network element (NE) domain	The NE domain represents the NE level in the cluster hardware hierarchy. A cluster can have up to 16 NEs arranged in FCOT/RFT pairs.
Shelf domain	The second tier in the hierarchy is the shelf domain. Shelves can be one of these types: • an access bandwidth manager (ABM) shelf • a transport bandwidth manager (TBM) shelf • an AccessNode Express (ANX) shelf • a copper distribution (CDS) shelf, or • a universal edge 9000 (UE9000) shelf
Circuit pack domain	The next tier in the hierarchy is the circuit pack domain. Circuit packs are the smallest hardware component in the hierarchy.
Slot domain	The slot domain includes all empty slots, in addition to all circuit packs in a shelf.

Structure of inventory reports

Inventory reports list inventories of the equipment you specify. You can generate inventory reports for each of the four domains. Figure 5-1 shows a slot domain report that is typical of all inventory reports.

Figure 5-1
Slot domain report

SC-10415



```
>·  Cluster Inventory                                                Options


 NE ShPos Slt Equip Id       Type   Service  PEC Info  Serial No.  REL SW
 9                           RFT
    1         CE             ABM
            1                Empty
            2                Empty
            3                Empty
            4                Empty
            5                Empty
            6                Empty
            7                Empty
            8                Enpty
            9 SNTREN12AA     OCI12           NT7E02LA  A14181677   00  0
           10 SNTREN12AA     OCI12           NT7E02LA  A18185916   00  0
           11 SAPQAA2AAA     TIC             NT4K56AC  17HY73765   01  0
           12                Empty
           13 SAPQAA1AAA     AIC             NT4K55AA  400000025   06  0
           14 SAPQABUAAA     TIC             NT4K56AC  17MY16826   01  0
           15                Empty

            [ Update        ♦U]        [ Save report     ♦S]

C 0   M 0   m 1   w 2   FailProt 0   Lckt 0   ActProt 0   PrfAlrt 0   13:11
```

The heading of the inventory report is the same for all four domains although the body of the report changes. Table 5-3 lists and describes the headings.

Table 5-3
Column headings for Inventory reports

Column	Description
NE	NE ID of the network element
ShPos	Shelf position
Slt	Slot number
Equip Id	Equipment identification
Type	Type
Service	Service (applicable to line card slots)
PEC Info	Product engineering code and vintage
Serial No.	Serial number
REL	Release
SW	Software release
Cpk State	Circuit pack state
Card Id	Card identification

Table 5-4 lists the contents of the Inventory report for each domain.

Table 5-4
Structure of inventory reports for each domain

This inventory report	Has this information	For this equipment
NE	• NE • type • card identification	each network element in the cluster
Shelf	• NE information • shelf number • equipment identification • type (does not report DLE shelves) • card identification	the selected shelf or shelves
Circuit pack	• NE and shelf information • slot number • equipment identification • type • service (when available) • PEC information • serial number • release • software release (when available) • circuit pack state (See note) • card identification	NE and shelf where the circuit pack is located
Slot	• all information that is listed in the Circuit Pack inventory report • empty slots	NE and shelf where the slot is located
Note: A number of codes are associated with each circuit pack state. These codes are listed later in this chapter.		

Structure of summary reports

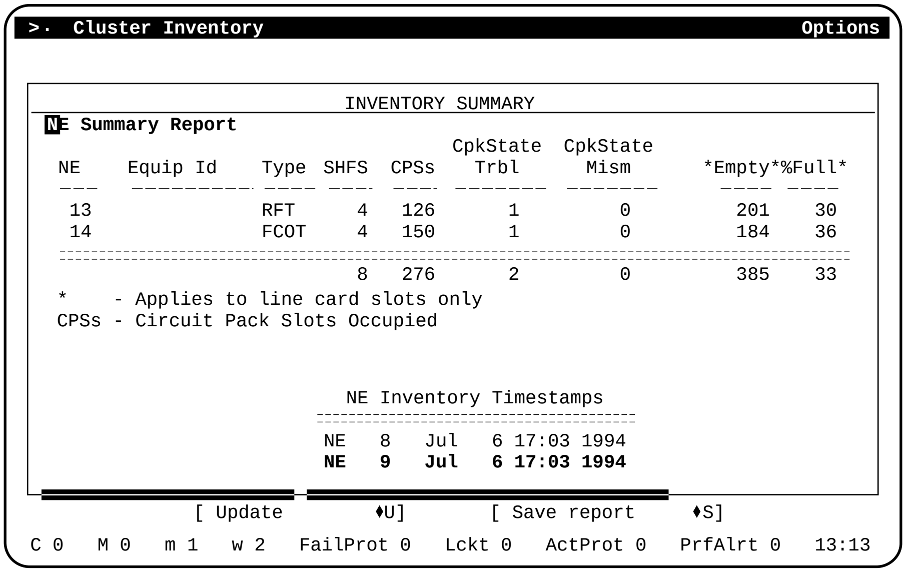
Summary reports provide an overview of the components in the selected domain for the entire cluster. The three types of summary reports are NE, shelf, and PEC Info (for circuit packs).

NE summary report

Figure 5-2 shows a sample of an NE summary report:

Figure 5-2
NE summary report

SC-10416



```
>.  Cluster Inventory                                                        Options


                                INVENTORY SUMMARY
 NE Summary Report
                                          CpkState  CpkState
   NE    Equip Id    Type  SHFS  CPSs    Trbl      Mism       *Empty*%Full*
   ---   ----------  ----  ----  ----  --------  --------      ----  ----
    13               RFT      4   126       1         0          201    30
    14               FCOT     4   150       1         0          184    36
   ========================================================================
                              8   276       2         0          385    33
   *    - Applies to line card slots only
   CPSs - Circuit Pack Slots Occupied



                              NE Inventory Timestamps
                             =============================
                              NE   8   Jul   6 17:03 1994
                              NE   9   Jul   6 17:03 1994

              [ Update        ♦U]       [ Save report     ♦S]
 C 0   M 0   m 1   w 2   FailProt 0   Lckt 0   ActProt 0   PrfAlrt 0   13:13
```

The report has nine columns, with each column specifying a particular item. Table 5-5 lists and describes the abbreviated column headings.

Table 5-5
Column headings for NE summary reports

Column	Description
NE	NE ID of the network element
Equip Id	Equivalent to equipment identification
Type	Type of NE (FCOT or RFT)
SHFS	Number of physical shelves in the NE
CPSs	Circuit pack slots occupied
CpkState Trbl	Number of circuit packs that are in trouble circuit pack state
CpkState Mism	Number of circuit packs that are mismatched circuit pack state
Empty	Number of empty line card slots
% Full	Percent of line card slots filled with circuit packs

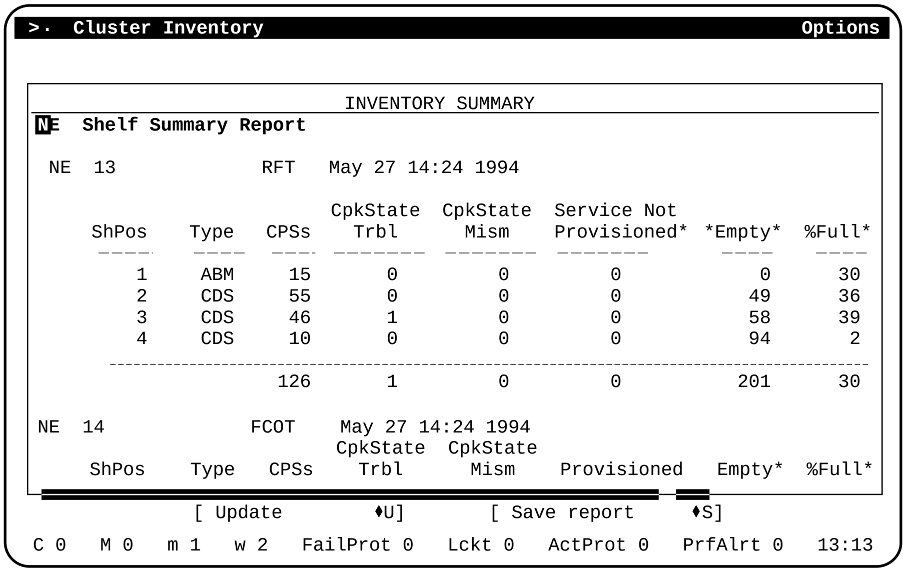
Note: Also shown at the bottom of the screen are the NE Inventory Timestamps, displaying the NE #, date, and time.

Shelf summary report

Figure 5-3 shows a sample of a shelf summary report.

Figure 5-3
Shelf summary report

SC-10417



```
>·  Cluster Inventory                                                   Options


                               INVENTORY SUMMARY
NE  Shelf Summary Report

 NE  13            RFT   May 27 14:24 1994

                               CpkState  CpkState  Service Not
     ShPos    Type   CPSs    Trbl      Mism    Provisioned* *Empty*  %Full*
     -----    ----   ----  --------  --------  --------       ----    ----
         1     ABM     15      0         0         0             0      30
         2     CDS     55      0         0         0            49      36
         3     CDS     46      1         0         0            58      39
         4     CDS     10      0         0         0            94       2
       ---------------------------------------------------------------------
                      126      1         0         0           201      30

NE  14            FCOT    May 27 14:24 1994
                            CpkState  CpkState
    ShPos    Type   CPSs    Trbl      Mism     Provisioned   Empty*  %Full*

             [ Update        ♦U]       [ Save report     ♦S]

C 0   M 0   m 1   w 2   FailProt 0   Lckt 0   ActProt 0   PrfAlrt 0   13:13
```

For each NE in the cluster, the shelf summary provides a title line, a header line, and a line for each shelf. The title line shows the NEID, equipment identification, and type for the NE. The header line has eight columns, with each column specifying a particular item. Table 5-6 lists and describes the abbreviated column headings.

Table 5-6
Column headings for shelf summary reports

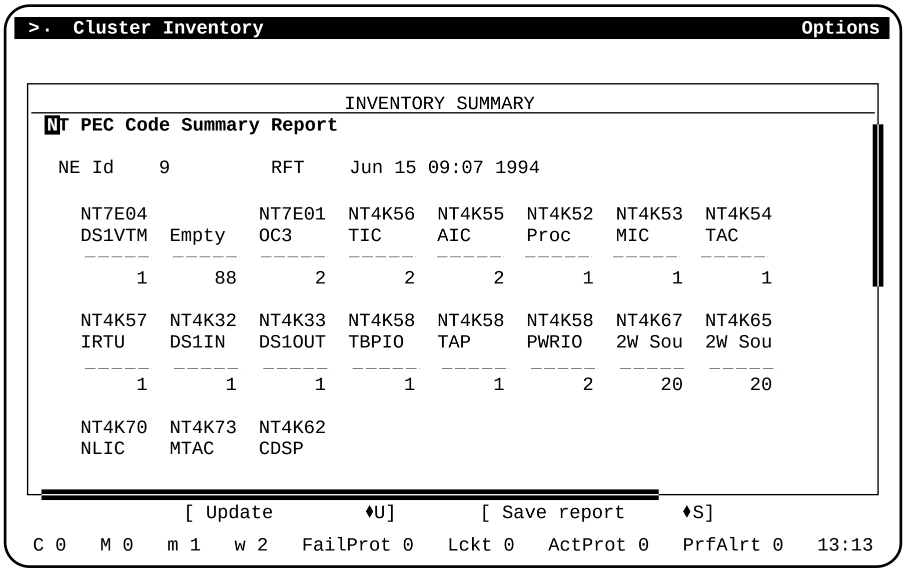
Column	Description
ShPos	Number of the shelf
Type	Type of shelf
CPSs	Circuit pack slots occupied
CpkState Trbl	Number of circuit packs in trouble circuit pack state
CpkState Mism	Number of circuit packs that are mismatched circuit pack state
Service Not Provisioned	Number of circuit packs not provisioned with a service
Empty	Number of empty slots
% Full	Percent of slots filled with circuit packs

PEC Info summary report

Figure 5-4 shows a sample of a PEC Info summary.

Figure 5-4
PEC info summary

SC-10418



```
>.  Cluster Inventory                                                 Options

                                INVENTORY SUMMARY
 NT PEC Code Summary Report

  NE Id    9         RFT    Jun 15 09:07 1994

    NT7E04          NT7E01  NT4K56  NT4K55  NT4K52  NT4K53  NT4K54
    DS1VTM  Empty   OC3     TIC     AIC     Proc    MIC     TAC
    ------  ------  ------  ------  ------  ------  ------  ------
         1      88       2       2       2       1       1       1

    NT4K57  NT4K32  NT4K33  NT4K58  NT4K58  NT4K58  NT4K67  NT4K65
    IRTU    DS1IN   DS1OUT  TBPIO   TAP     PWRIO   2W Sou  2W Sou
    ------  ------  ------  ------  ------  ------  ------  ------
         1       1       1       1       1       2      20      20

    NT4K70  NT4K73  NT4K62
    NLIC    MTAC    CDSP

              [ Update       ♦U]       [ Save report     ♦S]
C 0   M 0   m 1   w 2   FailProt 0   Lckt 0   ActProt 0   PrfAlrt 0   13:13
```

For each NE in the cluster, the PEC Info summary has a title line that lists the NEID, equipment identification, and type for the NE. A summary of the circuit packs according to their PEC and type follows the title line. The report shows the number of circuit packs provisioned for each PEC/type combination.

Searching inventory reports

Searching allows you to edit an inventory report to include only the information that you want. Table 5-7 lists the search criteria for the inventory tool.

Table 5-7
Search criteria for inventory reports

This search criteria	Searches for this information by
Type	using the component’s descriptive name These names are 3 to 9 alphanumeric characters. For example: 2W SINK, 2W SOURCE, OC3, IRTU.
Service	choosing a service which allows you to search for components by the service provided by the software load. These names refer to the actual service function (for example, COIN, POTSCT, COINRT).
PEC	choosing a PEC which allows you to search for components according to their manufacturing number (product equipment code).
PEC vintage	choosing a vintage which allows you to search for components according to their vintage. The vintage is a 2-character, alphabetic code that follows the PEC (for example, AA, AB). Usually, you search for a particular PEC, then do another search for the desired vintage.
Release	choosing a release which allows you to search for components according to their NT Release. NT Release is a numeric value between 01 and 99.
Software version	choosing a software version which allows you to search for components according to their software version (up to 45 different circuit pack software release codes)
Circuit pack state	choosing a circuit pack state which allows you to search for components according to their circuit pack state. These states include the following: unequipped (Ueq), mismatch (Mism), initializing (Init), testing (Test), loading (Load), trouble (Trbl), partial fail (PF), diagnostics (Diag), active (Act), standby (Stby), part of line card (Polc).

Smart lists

When you start the Cluster Inventory tool, it automatically edits all lists to reflect the actual components actually available in the cluster. For this reason, the lists provided by the Cluster Inventory tool are called smart lists.

Choosing multiple search criteria

After you a search on a report, you can focus the report on a smaller set of information by searching for a second criteria. Then only those components that meet both search criteria remain. No limit exists for the number of criteria that can be searched.

Sorting inventory reports

When first generated, inventory reports are sorted according to their NEID (for NEs), shelf number (for shelves), and slot number (for circuit packs and slots). The report can be resorted using other sort criteria. Table 5-8 lists the sort criteria for inventory reports.

Table 5-8
Sort criteria for inventory reports

This sort criteria	**Sorts the equipment in this order**
Shelf	shelves in descending shelf order
Slot	circuit packs numerically by their physical slot number (in descending slot order)
Equipment identification	components alphabetically by the customer defined identification
Type	components alphabetically by their descriptive names. For example, FCOT or RFT for NEs; ABM or CDS for shelves; O2W or O2WS for circuit packs.
Service	components alphabetically by the service provided by the software load. For example, COIN, POTSCT, COINRT.
PEC information	components numerically by manufacturing number (PEC)
Serial number	components numerically by serial numbers
PEC vintage	components alphabetically by the 2-letter code that follows the PEC. (For example, AA or AB.)
Release	components numerically by NT Release. NT Release is a numeric value between 01 and 99.
Software Version	components numerically by software version
Circuit pack state	components alphabetically by circuit pack state These states include the following: unequipped (Ueq), mismatch (Mism), initializing (Init), testing (Test), loading (Load), trouble (Trbl), partial fail (PF), diagnostics (Diag), active (Act), standby (Stby), part of line card (Polc).
Card identification	components numerically by card identification • For NEs, the card identification is the NEID of the NE. • For shelves, the card identification is the combination of the NEID of the NE and the shelf number. For example, a shelf in position 1 of NE with NEID 003 would have a card identification of 0031. • For circuit packs, the circuit pack slot number is combined with the NEID and shelf number. For example, a circuit pack in slot 10 of shelf 1 in NE 003 would have a card identification of 0031010. ***Note:*** Circuit packs are always represented by a 3-digit number with leading zeros used as required.

Procedure 5-1
Generating inventory reports

Use this procedure to generate inventory reports. You can also use this procedure to save an inventory report to view or print later.

An inventory report can provide a listing:

- by network element (NE)
- by shelf
- by circuit pack
- by slot

Note: In this procedure, inventory reports are generated using the list command, Inventory Mode. The Inventory Mode command allows you to choose the type of inventory report you want and generate it directly. The displayed data is current as of the time of the last database backup from the NEs to the operations controller (OPC).

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the Network Admin toolset of the OPC
- read the command conventions for the interface you are using (CMT or graphical) in *User Interfaces Description*, 323-3001-301, in this volume.

Action

Step	Action
1	Log in to the OPC and open the Cluster Level Inventory tool (in the Network Admin toolset). *The Cluster Level Inventory tool main window appears. The tool opens with the inventory report for the NE domain displayed. The first NE in the NE inventory report is selected.* ***Note:*** Wait for the window to display as the tool updates its local data tables with the data in the OPC database.
2	Display the list menu by pressing **Ctrl_L *l*** (or Keypad **3**). *The list menu appears.*

—continued—

Procedure 5-1 (continued)
Generating inventory reports

Step **Action**

3 Move to the Inventory Mode command (if you are not there already) by using your arrow keys.

If you want to generate	Then go to
the NEs inventory report	step 4
a shelves inventory report	step 5
a circuit pack inventory report	step 6
a slots inventory report	step 7

4 Move to the NEs option (in the Inventory Mode submenu) by using your arrow keys, then press **space** (or Keypad **0**).

The tool searches the NE domain information and generates a NE inventory report for all NEs.

Note: To view more fields (not all fields can be displayed on the screen), press **Ctrl_F** (for scroll mode), and use the left and right arrow keys.

If you want to	Then go to
generate another inventory report	step 2
save the report	step 8
leave the tool	step 9

5 Move to the shelves option (in the Inventory Mode submenu) by using your arrow keys, then press **Space** (or Keypad **0**).

The tool searches the shelf domain information and generates a shelf inventory report for all NEs.

If you want to	Then go to
generate another inventory report	step 2
save the report	step 8
leave the tool	step 9

6 Move to the circuit packs option (in the Inventory Mode submenu) by using your arrow keys, then press **Space** (or Keypad **0**).

The tool searches the circuit pack domain information and generates a circuit pack inventory report for all NE shelves.

If you want to	Then go to
generate another inventory report	step 2
save the report	step 8
leave the tool	step 9

—continued—

Procedure 5-1 (continued)
Generating inventory reports

Step	**Action**

7 Move to the slots option (in the Inventory Mode submenu) by using your arrow keys, then press **Space** (or Keypad **0**).

The tool searches the slot domain information and generates a slot inventory report for all NE shelves.

If you want to	Then go to
generate another inventory report	step 2
save the report	step 8
leave the tool	step 9

8 To save the report:

a. Tab to the Save report button, then press **Ctrl_A** (or Keypad **0**).

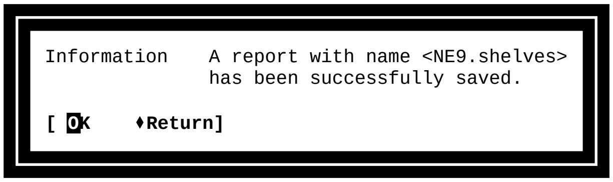
A dialog prompting you for a report name appears.

b. Enter the name of the report.

c. Tab to the OK button, then press **Ctrl_A** (or Keypad **0**).

The following information dialog appears.

PC-21854



```
Information    A report with name <NE9.shelves>
               has been successfully saved.

[ OK    ♦Return]
```

d. Select the OK button to remove the information dialog.

The dialog is removed, and the main window appears.

If you want to generate more inventory reports, return to step 2.

9 To close the tool:

a. Display the window menu by pressing **Ctrl_L W** (or Keypad **6**).

The window menu appears.

b. Select the Exit command by pressing **Space** (or Keypad **0**).

The tool closes.

—end—

Procedure 5-2
Generating summary reports

Use this procedure to generate summary reports (by network elements (NE), shelf, or by product engineering code (PEC) information). You can also use this procedure to save a summary report for later viewing or printing.

In this procedure, summary reports are generated using the list command, Summarize. The Summarize command allows you to choose and directly generate the type of report you want. The data displayed is data current as of the time of the last database backup from the NEs to the operations controller (OPC).

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the Network Admin toolset of the OPC
- read the command conventions for the interface you are using (character-mode terminal (CMT) or graphical) in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC and open the Cluster Level Inventory tool (in the Network Admin toolset). *The Cluster Level Inventory tool main window appears. The tool opens with the inventory report for the NE domain displayed. The first NE in the NE inventory report is selected.* ***Note:*** Wait for the window to display as the tool updates its local data tables with the data in the OPC database.
2	Display the list menu by pressing **Ctrl_L /** (or Keypad **3**).
3	Move to the Summarize command by using your arrow keys. *The Summarize submenu appears.*

If you want to generate	**Then go to**
an NE summary report	step 4
a shelves summary report	step 5
a PEC Info summary report	step 6

—continued—

Procedure 5-2 (continued)
Generating summary reports

Step **Action**

4 Move to the NEs option (in the Summarize submenu) using your arrow keys, then press **Space** (or Keypad **0**).

The NE Summary report appears.

If you want to	Then go to
generate another summary report	step 2
save the report	step 7
leave the tool	step 8

5 Move to the Shelves option (in the Summarize submenu) using your arrow keys, then press **Space** (or Keypad **0**).

The Shelves Summary report appears.

If you want to	Then go to
generate another summary report	step 2
save the report	step 7
leave the tool	step 8

6 Move to the PEC Info option (in the Summarize submenu) using your arrow keys, then press **Space** (or Keypad **0**).

The PEC Info Summary report appears.

If you want to	Then go to
generate another summary report	step 2
save the report	step 7
leave the tool	step 8

7 To save the report:

a. Tab to the Save report button, then press **Ctrl_A** (or Keypad **0**).

A dialog prompting you to enter the name of the report appears.

b. Enter the name of the report.

c. Tab to the OK button, then press **Ctrl_A** (or Keypad **0**).

An information dialog appears.

d. Select the **OK** button to remove the information dialog.

The dialog is removed, and the main window appears.

—continued—

Procedure 5-2 (continued)
Generating summary reports

Step	Action
8	To close the tool: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 5-3 **Managing reports**

Use this procedure for managing the reports by

- listing the reports that are already generated
- viewing the reports
- printing a hard copy
- deleting the reports

Note: All reports are automatically deleted after a system reboot/restart.

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the Network Admin toolset of the operations controller (OPC)
- read the command conventions for the interface you are using *User Interfaces Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC and open the Cluster Level Inventory tool (in the Network Admin toolset). *The Cluster Level Inventory tool main window appears. The tool opens with the inventory report for the NE domain displayed. The first NE in the NE inventory report is selected.* ***Note:*** Wait for the window to display as the tool updates its local data tables with the data in the OPC database.
2	Display the Options menu by pressing **Ctrl_L T** (or Keypad **,**). *The Options menu appears.*
3	Move to the Show Reports command, then press **Space** (or Keypad **0**). *The Inventory Reports dialog displays all the Report files:*

—continued—

Procedure 5-3 (continued)
Managing reports

Step	Action

4 Determine what you want to do based on the following information:

If you want to	Then go to
delete a report	step 5
print the report	step 6
view the report	step 7
return to the main window	step 8

5 To delete a report:

a. Move (using the arrow keys) to the report you want to delete.

b. Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).

The list menu appears.

c. Move to the Delete report command, then press **Space** (or Keypad **0**).

The report is removed from the list.

d. Return to step 4.

6 To print a report:

Note: If a printer is not configured at one of the appropriate OPC ports, you cannot print a report (and the Print report command is shown as disabled).

a. Move (using the arrow keys) to the report you want to print.

b. Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).

The list menu appears.

c. Move to the Print report command, then press **Space** (or Keypad **0**).

The report is printed.

d. Return to step 4.

—continued—

Procedure 5-3 (continued)
Managing reports

Step	Action
7	To view a report:
	a. Move (using the arrow keys) to the report you want to view.
	b. Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).
	The list item menu appears.
	c. Move to the Details... command, then press **Space** (or Keypad **0**).
	The report appears. You can view a maximum of two reports at one time.
	d. Tab to the Done button.
	The report is removed, and the report list appears.
	e. Return to step 4.
8	To return to the main window:
	a. Tab to the Done button.
	b. Select it by pressing **Ctrl_A** (or Keypad **0**).
	The dialog is removed, and the main window appears.
9	To close the tool:
	a. Display the window menu by pressing **Ctrl_L W** (or Keypad **6**).
	The window menu appears.
	b. Select the Exit command by pressing **Space** (or Keypad **0**).
	The tool closes.

—end—

Procedure 5-4
Updating the database

Use this procedure to retrieve the latest inventory data from the network elements (NEs), as well as to update the information currently displayed in your session.

Normally, an automated update process occurs every 24 hours. This procedure allows you to retrieve the inventory data and initiate an update immediately.

The operations controller (OPC) retrieves the latest inventory data by accessing each NE in the cluster and updating the database information with the current NE data.

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the Network Admin toolset of the OPC
- read the command conventions for the interface you are using (character-mode terminal (CMT) or graphical) in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC and open the Cluster Inventory tool (in the Network Admin toolset).
	The Cluster Inventory tool main window appears. The tool opens with the inventory report for the NE domain displayed. The first NE in the NE inventory report is selected.
	Note: Wait for the window to display as the tool updates its local data tables with the data in the OPC database.
2	Tab to the Update button, then press **Ctrl_A** (or Keypad **0**).
	The Backup Requested dialog appears.
3	Select the OK button by pressing **Ctrl_A** (or Keypad **0**).
	The Backup Initiated dialog appears.
4	Select the OK button by pressing **Ctrl_A** (or Keypad **0**).
	The OPC begins to retrieve the data. This process can last a few minutes.

—continued—

Procedure 5-4 (continued)
Updating the database

Step	Action
5	If the OPC can communicate with each NE, the Retrieve Successful or the Retrieve Failure dialog box appears. Select the Continue button by pressing **Ctrl_A** (or Keypad **0**). *The Please Standby dialog box appears to warn you that the parsing process can take several minutes.*
6	Select the Continue button by pressing **Ctrl_A** (or Keypad **0**). *The data parsing process begins. When the process is complete, the Access Completed dialog box appears.* ***Note:*** It can take several minutes to complete the data parsing. While waiting, you can perform any of the functions in the Options menu.
7	Select the OK button by pressing **Ctrl_A** (or Keypad **0**). *The Cluster Inventory tool is ready.*
8	To close the Cluster Level Inventory tool: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 5-5
Searching through inventory reports

Use this procedure to search through an inventory report.

An inventory report can provide a listing by network element (NE), shelf, by circuit pack, and slot. However, when you first generate a report, the amount of data can make it difficult to focus on the information that is needed.

Searching allows you to edit a report so that it includes only the information you need. Seven search criteria are available:

- type
- service
- PEC
- vintage
- release
- software
- circuit pack state

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the Network Admin toolset of the operations controller (OPC)
- read the command conventions for the interface you are using (character-mode terminal (CMT) or graphical) in *User Interfaces Description*, 323-3001-301, in this volume
- have the Cluster Level Inventory tool main window open and an NE inventory report at the circuit pack or slot level generated and displayed

—continued—

Procedure 5-5 (continued)
Searching through inventory reports

Action

Step	Action
1	Display the list menu by pressing **Ctrl_L /** (or Keypad **3**).
2	Using your arrow keys, move to the option you want, then press **Space** (or Keypad **0**). *Selecting a particular option edits the currently displayed inventory report so that only those components that meet the search criterion remain.*
3	To close the tool: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 5-6
Sorting an inventory report

Use this procedure to sort an inventory report.

An inventory report can provide a listing by network element (NE), shelf, circuit pack, and by slot. However, a report can be resorted using other sort criteria, such as the following:

- NE
- shelf
- slot
- equip ID
- type
- service
- PEC info
- vintage
- serial number
- release
- SW version
- circuit pack state
- card ID

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the Network Admin toolset of the operations controller (OPC)
- read the command conventions for the interface you are using (CMT or graphical) in *User Interfaces Description*, 323-3001-301 in this volume
- have the Cluster Level Inventory tool main window open, and an NE inventory report generated and displayed

—continued—

Procedure 5-6 (continued)
Sorting an inventory report

Action

Step	Action
1	Display the list menu by pressing **Ctrl_L /** (or Keypad **3**).
2	Using your arrow keys, move to the Sort by command. *A cascade menu with all the sort options appears.*
3	Move to the cascade menu (using the right arrow key), then move (with the up and down keys) to the option you want to sort by. *Selecting a particular option sorts the currently displayed inventory report. See “Sorting inventory reports” on page 5-10 for information on the sorting characteristics.*
4	To close the tool: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Changing the OPC date and time

The active operations controller (OPC) provides a single time-of-day clock source for the network elements (NE) it controls. NE clocks are synchronized with the active OPC every two hours. If primary OPC failure occurs, the backup OPC clock becomes the time-of-day clock source, although clock synchronization between the two OPCs must be maintained manually.

Offset time

Since local time on the NEs is derived from the OPC, local time is not defined at the NE during commissioning. Instead, an offset time is defined in each NE. Offset time is the difference in time between a reference time zone (Greenwich Mean Time or GMT) and the time zone where the NE is located. Offset times are specified in minutes. See *Commissioning and Testing*, Volume 3, to specify the shelf time offset in NEs.

OPC and time zone codes

In the OPC, the offset time is specified by selecting a time zone code. Each time zone code is associated with the offset time and performs the same function as the offset time that is specified in NEs.

The local date and time and the time zone code for an OPC is initially set during commissioning. Changes to the time zone should not be necessary unless the OPC is moved to a new time zone or replaced. However, if the clock drifts the time can require adjustment.

OPC and local time

Local time is also specified on an OPC. Using the time offsets specified in the NEs, and the local time and time zone specified on the active OPC, the correct time is derived on all NEs.

OPC time of day clock synchronization example

As an example of how time-of-day clock synchronization works, consider a network that has an NE in Tokyo and an NE in Los Angeles. The controlling OPC is in Chicago.

After commissioning, the following information is specified and derived.

Network element	Time zone or offset time in hours (and equivalent)	Set time	Derived time
Chicago (OPC)	Central Standard Time (+6)	10:00	-
Tokyo (NE)	– 9 (Japan Standard Time)	-	01:00
Los Angeles (NE)	+8 (Pacific Standard Time)	-	08:00

Both NEs request the reference time from the OPC. The OPC determines this time (GMT) by adding the time zone offset (+6 hours) to its local time. In the example, a time of 16:00 on the current date would be provided by the OPC to the NEs.

The NEs then subtract the offset time from the GMT value provided. For the NE in Los Angeles, this provides a derived local time of 08:00 on the same day. Since the NE in Japan has a negative offset time, it is added to GMT, producing a value of 25:00. Since this value is greater than 24, the date is incremented and the time is reduced by 24 hours, giving a time of 01:00 the following day.

OPC and daylight saving time

Unlike NEs, the OPC automatically adjusts for daylight saving time, at the proper time, according to the selected time zone code. Since different countries adjust for daylight saving time on different days, more time zone codes exist than time zones. You must select the correct code to make sure the OPC correctly initiates daylight saving time.

In the NEs, the offset time must be manually changed for daylight saving time. See *Commissioning and Testing,* Volume 3, for further information.

Powered down OPC

If an OPC is powered down, its battery backup maintains the OPC time-of-day clock for at least two weeks, if the backup was fully charged when the OPC was powered down.

OPC and changing time or date

To change the time or date of an operational OPC by more than 30 minutes, you must shut down the OPC. The procedure to change the time automatically initiates the shutdown procedure. Adjusting the OPC time within 30 minutes does not require a shutdown. Time adjustments are made slowly, so that performance measurements and other system activities that depend on the clock are not significantly affected.

The time-of-day clocks on the primary and backup OPCs must be set as closely to the same time as possible, since no automatic synchronization exists.

For further information on the OPC Date tool, see the description in *OPC User Interface Description*, 323-3001-301, in this volume.

Chapter task list

This chapter includes the following tasks.

Procedure		**See**
6-1	Changing the OPC date and time	page 6-4
6-2	Querying current time adjustment	page 6-8
6-3	Querying the OPC clock source	page 6-9
6-4	Selecting the OPC clock source	page 6-10

If you cannot complete these procedures, contact your next level of support.

Procedure 6-1
Changing the OPC date and time

Use this procedure to change the date, time, or time zone code in an operations controller (OPC). To change the time by more than 30 minutes, you must shut down the OPC.

Requirements

Before starting this procedure, you must:

- obtain the password of a user account with permission to change the OPC time. (These accounts include root, slat, and admin for the active OPC, and standby for the inactive OPC.)
- obtain the time zone code and local time for the location of the OPC
- read the command conventions for the interface you are using (CMT or graphical) in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step **Action**

1 Log in to the OPC and open the OPC Date tool.

The OPC Date tool opens and the main window appears.

2 Decide whether you are changing the time by more than 30 minutes.

If you are changing the time by	Then go to
less than 30 minutes	step 3
more than 30 minutes	step 7

3 Select the Adjust Time button by pressing **Ctrl_A** (or Keypad **0**).

The time and date change dialog appears.

—continued—

Procedure 6-1 (continued)
Changing the OPC date and time

Step **Action**

4 To change the date, enter:

dd/mm/yyyy↵

where:

<dd > the day of the month (range **01** to **28**, **29**, **30**, or **31**, depending on the month)

<mm> the month (range **01** to **12**)

<yyyy> the year (range **1976** to **2036**)

The new date appears in the Date entry field.

Note 1: Make sure all inaccurate data is removed. Use the right arrow key to position the cursor ahead of the inaccurate data and press the backspace key.

Note 2: When using the adjust time capability, you can only change the date to the immediately preceding or following day, and only if the current time is within 30 minutes of that day. Modifications to the date field at this point is required to support a 30-minute time advance near the end of a day.

5 To change the time, tab to the Time field and enter:

hh:mm↵

where:

<hh > the hour (range **00** to **23**)

<mm> the minute (range **00** to **59**)

The new time appears in the Date entry field.

Note 1: When using the adjust time capability, you can only change the time to within 30 minutes of the current value.

Note 2: It is recommended that the current time on the active OPC clock be used as the source of the correct time when setting the inactive OPC clock.

6 Tab to the Update button, then press **Ctrl_A** (Keypad **0**).

The system validates the data you entered. If incorrect, an error dialog appears. If correct, the time and date dialog closes, and the main window appears. The clock rate is slightly modified to begin the adjustment.

If you select Cancel, the system ignores the changes.

The procedure is complete.

7 Tab to the Reset Time button, then press **Ctrl_A** (Keypad **0**).

A confirmation dialog appears, indicating the amount of time required for the shutdown and giving you a final chance to stop the shutdown.

—continued—

Procedure 6-1 (continued)
Changing the OPC date and time

Step	Action
8	Tab to the Proceed button, then press **Ctrl_A** (Keypad **0**).
	The confirmation dialog closes and OPC shutdown process starts. A console message appears.
	Note: Selection of the Proceed button commits the shutdown of the OPC. If you decide later to stop changes to the time and date, you can select the Cancel button to stop the OPC shutdown procedure.
9	Select the OK button by pressing **Ctrl_A** (Keypad **0**).
	A shutdown progress message appears. As the shutdown progresses, the dots on the dialog are replaced with Xs.
	The progress message indicates that the OPC is shutting down normally. Since the shutdown continues while the above console message appears, the shutdown can complete before you select the OK button in this step. Therefore, you would not see the progress message below.
	This shutdown progress message is replaced by a dialog that states the OPC is out of service when the shutdown is complete. The new dialog appears to all users who are currently logged in to the OPC.
10	Select the Done button by pressing **Ctrl_A** (Keypad **0**).
	The Time and Date Change dialog appears.
11	To change the date, enter:
	dd/mm/yyyy↵
	where:
	<dd > the day of the month (range **01** to **28**, **29**, **30**, or **31**, depending on the month)
	<mm> the month (range **01** to **12**)
	<yyyy> the year (range **1976** to **2036**)
	The new date appears in the Date entry field.
	Note: Make sure incorrect data is removed. Use the right arrow key to position the cursor ahead of the incorrect data and press the backspace key.

—continued—

Procedure 6-1 (continued)
Changing the OPC date and time

Step	Action
12	To change the time, tab to the Time field and enter: **hh:mm**↵ where: <hh > the hour (range **00** to **23**) <mm> the minute (range **00** to **59**) *The new time appears in the Date entry field.* ***Note:*** It is recommended that the current time on the active OPC clock be used when setting the inactive OPC clock.
13	To change the time zone, tab to the Time Zone list, use the arrow keys to move to the time zone code you want, then press **Ctrl_A** (Keypad **0**). *The selected entry appears in the Time Zone field.* ***Note:*** A table of valid time zone codes is located at the end of this chapter.
14	Tab to the Update button, then press **Ctrl_A** (Keypad **0**). If you select Cancel, the changes you have made are ignored, but the OPC continues to shutdown. *A confirmation message appears, indicating that an error in selecting the new time and date requires a second OPC shutdown to correct.*
15	Select the OK button, by pressing **Ctrl_A** (Keypad **0**). If you select the Cancel button, the time and date change dialog appears. *The system validates the data you entered. If incorrect, an error dialog appears telling you what to do. If correct, the time and date information is saved, and the OPC begins its reboot sequence. The Session Manager screen appears briefly.* *The reboot process takes about 5-10 minutes. When it completes, the OPC login prompt (login:) appears.* *The shutdown of the OPC terminates all user login sessions. You have to log in again, after the OPC returns to service.*

—end—

Procedure 6-2
Querying current time adjustment

Use this procedure to determine whether a time adjustment is in progress and how much time remains to be adjusted.

Requirements

Before starting this procedure, you must:

- obtain the password of a user account with permission to change the operations controller (OPC) time. (These accounts include root, slat, and admin for the active OPC, and standby for the inactive OPC.)
- obtain the time zone code and local time for the location of the OPC. If you do not know how to do this, see *User Interfaces Description*, 323-3001-301, in this volume.

Action

Step	Action
1	Log in to the OPC and open the OPC Date tool. *The OPC Date tool is opened and the main window appears.*
2	Display the Options menu by pressing **Ctrl_L T** (or Keypad **,**). *The tool menu appears.*
3	Select the Query Time Adjust command, by pressing **Space** (or Keypad **0**). *The query time dialog appears.*
4	When finished, select the Done button by pressing **Ctrl_A** (or Keypad **0**). *The query time dialog closes, and the main window appears.*

—end—

Procedure 6-3
Querying the OPC clock source

Use this procedure to determine whether the 1 Hz pulse is being used as the clock source.

Requirements

Before starting this procedure, you must:

- obtain the password of a user account with permission to change the operations controller (OPC) time. These accounts include root, slat, and admin for the active OPC, and standby for the inactive OPC.
- obtain the time zone code and local time for the location of the OPC
- read the command conventions for the interface you are using (CMT or graphical) in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC and open the OPC Date tool. *The OPC Date tool opens and the main window appears.*
2	Display the Options menu by pressing **Ctrl_L T** (or Keypad **,**). *The tool menu appears.*
3	Select the Query 1HZ Pulse command by pressing **Space** (or Keypad **0**). *The clock pulse query dialog appears.*
4	When finished, select the Done button by pressing **Ctrl_A** (or Keypad **0**). *The clock pulse query dialog closes, and the main window appears.*

—end—

Procedure 6-4
Selecting the OPC clock source

Use this procedure to select the source for the operations controller (OPC) system clock. When the 1 Hz pulse is enabled, the clock source is the 1 Hz pulse. When it is disabled, the clock is driven by its own internal crystal. The local crystal is subject to drift and is therefore less accurate.

Requirements

Before starting this procedure, you must:

- obtain the password of a user account with permission to change the OPC time. (These accounts include root, slat, and admin for the active OPC, and standby for the inactive OPC.)
- obtain the time zone code and local time for the location of the OPC
- read the command conventions for the interface you are using (CMT or graphical) in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step **Action**

1 Log in to the OPC and open the OPC Date tool.

The OPC Date tool opens and the main window appears.

2 Display the Options menu by pressing **Ctrl_L T** (or Keypad **,**).

The tool menu appears.

3 Decide whether you are enabling the 1 Hertz pulse as the clock source.

If you are	Then go to
enabling the 1 Hz pulse	step 4
disabling the 1 Hz pulse	step 5

4 Select the Enable 1 HZ Pulse command, by pressing **Space** (or Keypad **0**).

The 1 Hz pulse becomes the source of the OPC clock. The new enable state of the 1 Hz pulse appears.

Go to step 6.

5 Select the Disable 1 HZ Pulse command, by pressing **Space** (or Keypad **0**).

The internal crystal of the clock becomes the source of the OPC clock. A dialog showing the new enable state of the 1 Hz pulse appears.

6 To remove the dialog, select the Done button by pressing **Ctrl_A** (or Keypad **0**).

The dialog closes, and the main window appears.

—end—

Time zone codes

Table 6-1 lists time zones, their associated time zone codes, and their offsets from Greenwich Mean Time (GMT).

Table 6-1
Time zone codes and GMT offsets

Time zone	Country: region	Time zone code	GMT offset in minutes
Hawaiian Standard Time Hawaiian Daylight Time	United States: Hawaii	HST10	–600 –540*
Aleutian Standard Time Aleutian Daylight Time	United States: Alaska (parts)	AST10ADT	–600 –540*
Yukon Standard Time Yukon Daylight Time	United States: Alaska (parts)	YST9YDT	–540 –480*
Pacific Standard Time Pacific Daylight Time	Canada: British Columbia	PST8PDT#Canada	–480 –420*
Pacific Standard Time Pacific Daylight Time	United States: California, Idaho (parts), Nevada, Oregon (parts), Washington	PST8PDT	–480 –420*
Mountain Standard Time Mountain Daylight Time	Canada: Alberta, Saskatchewan (parts)	MST7MDT#Canada	–480 –360*
Mountain Standard Time Mountain Daylight Time	United States: Colorado, Idaho (parts), Kansas (parts), Montana, Nebraska (parts), New Mexico, North Dakota (parts), Oregon (parts), South Dakota (parts), Texas (parts), Utah, Wyoming	MST7MDT	–480 –360*
Mountain Standard Time Mountain Daylight Time	United States: Arizona	MST7	–420 –360*
Central Standard Time Central Daylight Time	Canada: Manitoba, Ontario (parts), Saskatchewan (parts)	CST6CDT#Canada	–360 –300*

—continued—

Table 6-1 (continued)
Time zone codes and GMT offsets

Time zone	Country: region	Time zone code	GMT offset in minutes
Central Standard Time Central Daylight Time	United States: Alabama, Arkansas, Florida (parts), Illinois, Iowa, Kansas, Kentucky (parts), Louisiana, Michigan (parts), Minnesota, Mississippi, Missouri, Nebraska, North Dakota, Oklahoma, South Dakota, Tennessee (parts), Texas, Wisconsin	CST6CDT	–360 –300*
Central Standard Time Central Daylight Time	United States: Indiana (most)	EST5CDT	–300 –240*
Eastern Standard Time Eastern Daylight Time	Canada: Ontario (parts), Quebec (parts)	EST5EDT#Canada	–300 –240*
Eastern Standard Time Eastern Daylight Time	United States: Connecticut, Delaware, District of Columbia, Florida, Georgia, Kentucky, Maine, Maryland, Massachusetts, Michigan, New Hampshire, New Jersey, New York, North Carolina, Ohio, Pennsylvania, Rhode Island, South Carolina, Tennessee (parts), Vermont, Virginia, West Virginia	EST5EDT	–300 –240*
Atlantic Standard Time Atlantic Daylight Time	Canada: Newfoundland (parts), Nova Scotia, Prince Edward Island, Quebec (parts)	AST4ADT	–240 –180*
Newfoundland Standard Time Newfoundland Daylight Time	Canada: Newfoundland (parts)	NST3:30NDT	–210 –150*
Western European Time Western European Daylight Time	Great Britain, Ireland	WETOWETDST	0 60*

—continued—

Table 6-1 (continued)
Time zone codes and GMT offsets

Time zone	Country: region	Time zone code	GMT offset in minutes
Portuguese Winter Time Portuguese Summer Time	Portugal	PWTOPST	0 60*
Middle European Time Middle European Daylight Time	Austria, Belgium, Bosnia-Herzegovina, Denmark, Croatia, Czech Republic, France, Germany, Hungary, Italy, Luxembourg, Poland, Slovakia, Slovenia, Spain, Sweden, Switzerland, Yugoslavia	MET-1METDST	60 120*
South Africa Standard Time South Africa Daylight Time	South Africa	SAST-2SADT	120 180*
Japan Standard Time	Japan	JST-9	540
Australian Western Standard Time	Australia: Western Australia	WST-8:00	480
Australian Central Standard Time	Australia: Northern Territory	CST-9:30	570
Australian Eastern Standard Time	Australia: Queensland	EST-10	600
Australian Central Standard Time Australian Central Daylight Time	Australia: South Australia	CST-9:30CDT	570 630*
Australian Eastern Standard Time Australian Eastern Daylight Time	Australia: New South Wales, Victoria	EDT-10EDT	600 660*

Note: Offsets marked with an asterisk denote the network element offset that should be used when the Daylight Saving Time is observed in the corresponding region. Daylight Saving Time change is automatically updated by the software.

—end—

Setting parameters of the NE user interface ports

This chapter has the procedures to change the parameters of the user interface ports at a network element (NE). Parameters include:

- the baud rate
- the usage of parity correction
- the stop bits
- the character size setting

Perform these procedures at the network element user interface (NEUI).

Chapter task list

This chapter includes the following tasks:

If you cannot complete these procedures, contact your next level of support.

Procedure 7-1
Displaying all the interface ports

Use this procedure to display a general overview of the provisioned telemetry ports, user interface ports, and TBOS ports.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see the quick reference summary in *Network Element User Interface Description*, 323-3001-300, in this volume.

Step	**Action**
1	Access the system administration screen, and display the NE profile parameters and all the user interface ports. Enter: **admin ip** ↵ *A screen that shows provisioned telemetry ports, user interface ports, and TBOS ports appears.*

—end—

Procedure 7-2
Displaying the user interface port parameters

Use this procedure to display the selected user interface port and the parameters associated with it. Two user interface ports are available: 1 and 2.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see the quick reference summary in *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step	Action
1	Access the system administration screen and display all the user interface ports. Enter: **admin ip** ↵ *The system administration screen appears.*
2	Display the port parameters. Enter: **dtlport <port #>** ↵ where <port #> **1** or **2** *A screen that shows the selected user interface port and its parameters appears.*

—end—

Procedure 7-3
Changing the user interface port parameters

Use this procedure to change or set the parameters of a user interface port.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level.
- deactivate the user interface port (1 or 2) before changing its parameters. A user interface port cannot be deactivated if a user is already logged in to this port.
- be familiar with the VT100-type NE user interface. For a reminder of how to use the interface, see the quick reference summary in *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step **Action**

1 Access the system administration screen and display all the user interface ports. Enter:

admin ip ↵

The system administration screen appears.

2 Display the port parameters. Enter:

dtlport <port #> ↵

where

<port #> **1** or **2**

If port state reads	Then go to
IS (in service)	step 3
OOS (out of service)	step 4

—continued—

Procedure 7-3 (continued)
Changing the user interface port parameters

Step **Action**

3 Deactivate user interface port (1 or 2). Enter:

chgstate OOS ↵

Confirm the action. Enter:

yes ↵

4 Edit the port parameter. Enter:

edit ↵

The edit user interface screen appears.

5 Set or change any or all of the user interface port parameters listed in the table below. If you are provisioning for the first time, set all of the parameters. Set or change any parameter as often as required.

If the parameter is	Then
baudrate	Set the baud rate: **baudrate <value>** ↵ where <value> **300**, **1200**, **2400**, **4800**, or **9600**
parity	Set the parity error type: **parity <type>** ↵ where <type> **none**, **even** or **odd**
charsize	Set the number of bits in a character: **charsize <value>** ↵ where <value> **7** or **8**
stopbit	Set the number of stopbits: **stopbits <value>** ↵ where <value> **1** or **2**

The parameter settings appear on screen as they are set or changed.

6 Activate the user interface port (1 or 2). Enter:

quit ↵
chgstate IS ↵

—end—

Procedure 7-4
Querying another user interface port

Use this procedure to display the interface parameters for the selected port. Perform this procedure from the current interface port menu when another interface port's parameters are required.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see the quick reference summary in *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step **Action**

1 Access the system administration screen and display all the user interface ports. Enter:

admin ip ↵

The system administration screen appears.

2 Display the port parameters. Enter:

dtlport <port #> ↵

where:

<port #> is **1** or **2**

3 Query another user interface port. Enter:

query <ui port #> ↵

where

<ui port #> is **1, 2** or **all**

A screen that shows the interface parameters for the selected port appears.

A screen that shows the interface parameters for all the ports appears.

—end—

Procedure 7-5
Activating or deactivating a user interface port

Use this procedure to activate or deactivate a user interface port on a selected shelf. You must deactivate a user interface port before you can change any of its parameters.

Requirements

- You must be logged on the network element user interface (NEUI) and be at the main menu level.
- You must be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see the quick reference summary in *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step	Action
1	Access the system administration screen and display all the user interface ports. Enter: **admin ip** ↵ *The system administration screen appears.*
2	Display the port parameters. Enter: **dtlport <port #>** ↵ where <port #> **1** or **2**
3	Change the state. Enter: **chgstate <target state>** ↵ where <target state> **oos,** (out of service), or **is** (in service) Confirmation of the action (for oos only). Enter: **yes** ↵ *A screen that shows the port state appears.*

—end—

Setting serial telemetry ports and displays with the NE user interface

Telemetry byte-oriented serial (TBOS) mapping is a protocol for transmitting alarm surveillance and control data between monitoring and monitored equipment.

The data is transmitted in the form of displays. A display is a group of 64 bits. Two types of displays exist:

- Monitor displays are predefined to represent alarm and status information by mapping the bits in a display to alarm and status points.
- Control displays are predefined to represent commands that the monitoring equipment wants the monitored network element (NE) to execute.

Displays are mapped from monitored NEs to TBOS interface ports that reside on designated NEs. Up to two TBOS ports can exist on one of these designated NEs. You can map up to eight displays to the mapping positions on a single TBOS port. An E2A alarm processing remote (APR) does the actual monitoring of TBOS displays and transmission of command displays.

For NEs without a serial link to an E2A APR, the operations controller (OPC) passes monitoring data to NEs, that in turn pass it to the APR. (This feature is not available in this release.)

> ***Note:*** To add a new TBOS port, you must have the correct software feature. To remove a TBOS port, you must first place it out of service, then deactivate the correct software feature.

Chapter task list

This chapter includes the following tasks:

Procedure		**See**
8-1	Displaying the E2A TBOS port parameters	page 8-3
8-2	Querying another E2A TBOS port	page 8-4
8-3	Activating or deactivating an E2A TBOS port	page 8-5
8-4	Adding or changing an E2A TBOS port display	page 8-6
8-5	Deleting a display from an E2A TBOS port	page 8-8
8-6	Enabling or disabling a TBOS port display	page 8-9

If you cannot complete these procedures, contact your next level of support.

Procedure 8-1
Displaying the E2A TBOS port parameters

Use this procedure to display an E2A TBOS port and the parameters associated with it. Two TBOS ports are available: 3 and 4. See *Alarms and Surveillance Description*, 323-3001-104, in *Description*, Volume 2A, for a complete description of TBOS surveillance.

Requirements

- You must be logged on the network element user interface (NEUI) and be at the main menu level.
- You must be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see the quick reference summary in *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step	Action
1	Access the system administration screen and display all the user interface ports. Enter: **admin ip** ↵ *The system administration screen appears.*
2	Display the port parameters. Enter: **dtlport <port #>** ↵ where <port #> **3** or **4** *A screen that shows the port parameters appears.*

—end—

Procedure 8-2
Querying another E2A TBOS port

Use this procedure to display the parameters for another TBOS port. Perform this procedure from the current TBOS port menu when other TBOS port parameters are required.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see the quick reference summary in *Network Element User Interface Description*, 323-3001-300, in this document.

Action

Step	Action
1	Access the system administration screen and display all the user interface ports. Enter: **admin ip** ↵ *The system administration screen appears.*
2	Display the port parameters. Enter: **dtlport <port #>** ↵ where: <port #> **3** or **4**
3	Query another user interface port. Enter: **query <tbos port # >** ↵ where <tbos port #> **3**, **4**, or **all** *A screen that shows the parameters of a TBOS port appears.* *A screen that shows the parameters of all the TBOS ports appears.*

—end—

Procedure 8-3
Activating or deactivating an E2A TBOS port

Use this procedure to activate or deactivate the selected E2A TBOS port. See *Alarms and Surveillance Description*, 323-3001-104, in *Description,* Volume 2A, for a complete description of TBOS surveillance.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see the quick reference summary in *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step **Action**

1 Access the system administration screen and display all the user interface ports. Enter:

admin ip ↵

The system administration screen appears.

2 Display the port parameters. Enter:

dtlport <port #>↵

where:

<port #> **3** or **4**

3 Change the state. Enter:

chgstate <target state> ↵

where

<target state> **oos,** (out of service), or **is** (in service)

Confirm your action (for oos only). Enter:

yes ↵

A screen that shows the status of the E2A TBOS port appears.

—end—

Procedure 8-4
Adding or changing an E2A TBOS port display

Use this procedure to assign a display to a telemetry (E2A TBOS) port. Up to eight displays can be assigned to each port. See *Alarms and Surveillance Description*, 323-3001-104, in *Description*, Volume 2A, for a complete description of TBOS surveillance.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see the quick reference summary in *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step	Action
1	Access the system administration screen and display all the user interface ports. Enter: **admin ip** ↵ *The system administration screen appears.*
2	Display the port parameters. Enter: dtlport **<port #>** ↵ where <port #> **3** or **4**
3	Edit the TBOS screen. Enter: **edit** ↵ *The edit TBOS screen appears.*

—continued—

Procedure 8-4 (continued)
Adding or changing an E2A TBOS port display

Step	**Action**
4	Add a display to the port. Enter:

display <mapping position #><display type><display id>↵

where

<mapping position>	**1** to **8**
<display type>	**monitor, control** or **remote**
<display id>	**1** to **32**

A screen that shows the new display for the port appears.

—end—

Procedure 8-5
Deleting a display from an E2A TBOS port

Use this procedure to delete a display from a telemetry (E2A TBOS) port. See *Alarms and Surveillance Description*, 323-3001-104, in *Description*, Volume 2A, for a complete description of TBOS surveillance.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see the quick reference summary in *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step **Action**

1 Access the system administration screen and display all the user interface ports. Enter:

admin ip ↵

The system administration screen appears.

2 Display the port parameters. Enter:

dtlport <port #> ↵

where

<port #>	**3** or **4**

3 Edit the TBOS screen. Enter:

edit ↵

The edit TBOS screen appears.

4 Delete a display from the port. Enter:

deldisp <mapping position>↵

where

<mapping position>	**1** to **8**

To confirm the action, enter:

yes ↵

A screen that shows the display has been deleted appears.

—end—

Procedure 8-6
Enabling or disabling a TBOS port display

Use this procedure to enable or disable a telemetry (E2A TBOS) port display.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level.
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see the quick reference summary in *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step	Action
1	Access the system administration screen and display all the user interface ports. Enter: **admin ip** ↵ *The system administration screen appears.*
2	Display the port parameters. Enter: **dtlport <port #>** ↵ where <port #> **3** or **4**
3	Edit the TBOS screen. Enter: **edit** ↵ *The edit TBOS screen appears.*
4	Display the status from the port. Enter: **status <mapping position> <target status>**↵ where <mapping position> **1** to **8** <target status> **on** or **off** To confirm the action, enter: **yes** ↵ *A screen that shows the status of the telemetry port display appears.*

—end—

Setting parallel telemetry parameters

The AccessNode can have an input parallel telemetry port to permit scanning 11 status points and an output parallel telemetry port distributing 18 status points. Each of the status points can be set so its active state is either a normally-closed or normally-open relay contact.

An E2A alarm processing remote (APR) performs parallel telemetry monitoring. The input points are scanned every 500 ms to establish their status. The output points can feed status information to external systems through the APR.

Perform these procedures at the network element user interface.

Chapter task list

This chapter includes the following tasks:

Procedure		See
9-1	Displaying telemetry input port parameters	page 9-2
9-2	Querying another telemetry input	page 9-3
9-3	Enabling or disabling a telemetry input point	page 9-5
9-4	Provisioning the alarm severity of the telemetry inputs	page 9-7
9-5	Provisioning the telemetry input service impact (SA or NSA)	page 9-9
9-6	Changing the telemetry input description	page 9-11
9-7	Displaying the telemetry output port parameters	page 9-13
9-8	Querying another telemetry output port	page 9-14
9-9	Changing the telemetry output port settings	page 9-15
9-10	Manually operating or releasing a telemetry output relay	page 9-19

If you cannot complete these procedures, contact your next level of support.

Procedure 9-1
Displaying telemetry input port parameters

Use this procedure to display the currently selected external parallel input port and the parameters associated with it.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step	Action
1	Access the system administration screen and display the user profile parameters. Enter: **admin ip** ↵ *The system administration screen with the user profile parameters appears.*
2	Display the input telemetry port parameters. Enter: **dtlport <port #> <point #>** ↵ where <port #> **5** <point #> **1** to **11** *A screen that shows the input port parameters appears.*

—end—

Procedure 9-2
Querying another telemetry input

Use this procedure to

- display the parameters for the selected external input port
- execute from the current external input port's menu when another external input port's parameters are required

See *Alarms and Surveillance Description*, 323-3001-104, in *Description,* Volume 2A, for a complete description of telemetry input surveillance.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step	Action
1	Access the system administration screen and display the user profile parameters. Enter: **admin ip** ↵ *The system administration screen with the user profile parameters appears.*
2	Display the input telemetry port parameters. Enter: **dtlport <port #> <point #>** ↵ where <port #> **5** <point #> **1** to **11** *The telemetry port parameter screen appears.*

—continued—

Procedure 9-2 (continued)
Querying another telemetry input

Step	Action
3	Query another input port. Enter:

query <point #> ↵

where

<point #> **1** to **11**

A screen that shows the parameters for the selected external input port appears.

A screen that shows the parameters for all the external input ports appears.

—end—

Procedure 9-3
Enabling or disabling a telemetry input point

Use this procedure to enable or disable the reporting of a telemetry input point. See *Alarms and Surveillance Description*, 323-3001-104, in *Description*, Volume 2A, for a complete description of telemetry surveillance.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step **Action**

1 Access the system administration screen and display the user profile parameters. Enter:

admin ip ↵

The system administration screen with the user profile parameters appears.

2 Display the input telemetry port parameters. Enter:

dtlport <port #> <point #> ↵

where

<port #>	**5**
<point #>	**1** to **11**

The telemetry port parameter screen appears.

3 To edit the input telemetry point, enter:

edit ↵

The telemetry input point screen appears.

—continued—

Procedure 9-3 (continued)
Enabling or disabling a telemetry input point

Step	Action
4	Change the status of the telemetry input. Enter:

status <target state>↵

where

<target state>   **on** or **off**

Confirm your action (for off only). Enter:

yes ↵

A screen that shows the status of the telemetry input port appears.

—end—

Procedure 9-4
Provisioning the alarm severity of the telemetry inputs

Use this procedure to provision the alarm severity of the telemetry input. The severity can be critical, major, minor, or warning. See *Alarms and Surveillance Description*, 323-3001-104, in *Description*, Volume 2A, for a complete description of telemetry surveillance.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step	Action
1	Access the system administration screen and display the user profile parameters. Enter: **admin ip** ↵ *The system administration screen with the user profile parameters appears.*
2	Display the input telemetry port parameters. Enter: **dtlport <port #> <point #>** ↵ where <port #> **5** <point #> **1** to **11** *The telemetry port parameter screen appears.*
3	To edit the input telemetry point, enter: **edit** ↵ *The telemetry input point screen appears.*

—continued—

Procedure 9-4 (continued)
Provisioning the alarm severity of the telemetry inputs

Step	**Action**
4	To provision the severity level, enter:

severity <severity>↵

where

<severity> **critical, major, minor,** or **warning**

A that shows the alarm severity of the telemetry input appears.

—end—

Procedure 9-5
Provisioning the telemetry input service impact (SA or NSA)

Use this procedure to provision the impact of a telemetry input event. The impact can be provisioned as either service-affecting (SA) or non-service-affecting (NSA). See *Alarms and Surveillance Description*, 323-3001-104, in *Description*, Volume 2A, for a complete description of telemetry surveillance.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step **Action**

1 Access the system administration screen and display the user profile parameters. Enter:

admin ip ↵

The system administration screen with the user profile parameters appears.

2 Display the input telemetry port parameters. Enter:

dtlport <port #> <point #> ↵

where

<port #>	**5**
<point #>	**1** to **11**

The telemetry port parameter screen appears.

3 To edit the input telemetry point, enter:

edit ↵

The telemetry input point screen appears.

—continued—

Procedure 9-5 (continued)

Provisioning the telemetry input service impact (SA or NSA)

Step	**Action**
4	To provision the severity impact level, enter: **svcimpct <impact level>**↵ where <impact level> **sa** or **nsa** *A screen that shows the impact of a telemetry input event appears.*

—end—

Procedure 9-6
Changing the telemetry input description

Use this procedure to assign a description to a telemetry input. See *Alarms and Surveillance Description*, 323-3001-104, in *Description*, Volume 2A, for a complete description of telemetry surveillance.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step **Action**

1 Access the system administration screen and display the user profile parameters. Enter:

admin ip ↵

The system administration screen with the user profile parameters appears.

2 Display the input telemetry port parameters. Enter:

dtlport <port #> <point #> ↵

where

<port #>	**5**
<point #>	**1** to **11**

The telemetry port parameter screen appears.

3 To edit the input telemetry point, enter:

edit ↵

The telemetry input point screen appears.

—continued—

Procedure 9-6 (continued)
Changing the telemetry input description

Step	**Action**
4	To change the telemetry input description, enter:

descript <description>↵

where

<description> up to 30 characters within single quotes (’ ’) if you enter spaces or special characters (?, =), or if the first character is a number

A screen that shows the description for the telemetry input appears.

—end—

Procedure 9-7
Displaying the telemetry output port parameters

Use this procedure to display an output point on the telemetry output port and the parameters associated with it. Eight telemetry output points are available. See *Alarms and Surveillance Description*, 323-3001-104, in *Description*, Volume 2A, for a complete description of telemetry surveillance.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step	Action
1	Access the system administration screen and display the user profile parameters. Enter:
	admin ip ↵
	The system administration screen with the user profile parameters appears.
2	Display the output telemetry port parameters. Enter:
	dtlport <port #> <point #> ↵
	where
	<port #> **6**
	<point #> **1** to **18**
	A screen that displays the output telemetry port parameters appears.

—end—

Procedure 9-8
Querying another telemetry output port

Use this procedure to display the parameters for another, or all, output points on the external output port. Perform this procedure from the current external output port menu when another external output port's parameters are required. See *Alarms and Surveillance Description*, 323-3001-104, in *Description*, Volume 2A, for a complete description of the telemetry output port.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step	Action
1	Access the system administration screen and display the user profile parameters. Enter: **admin ip** ↵ *The system administration screen with the user profile parameters appears.*
2	Display the output telemetry port parameters. Enter: **dtlport <port #> <point #>** ↵ where <port #> **6** <point #> **1** to **18**
3	Query another input port. Enter: **query <point #>** ↵ where <point #> **1** to **18,** or **all** *A screen that shows the parameters for the external output port appears.*

—end—

Procedure 9-9
Changing the telemetry output port settings

Use this procedure to change the settings of a point on the telemetry output port. See *Alarms and Surveillance Description*, 323-3001-104, in *Description*, Volume 2A, for a complete description of the telemetry output port.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step **Action**

1 Access the system administration screen and display the user profile parameters. Enter:

admin ip ↵

The system administration screen with the user profile parameters appears.

2 Display the output telemetry port parameters by entering the following:

dtlport <port #> <point #> ↵

where

<port #>	**6**
<point #>	**1** to **18**

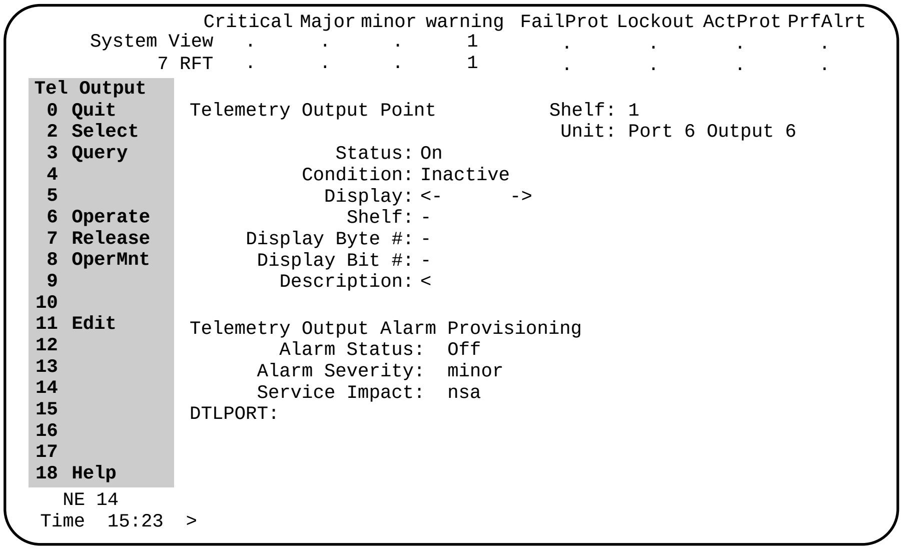
The output telemetry port parameter screen appears.

—continued—

Procedure 9-9 (continued)
Changing the telemetry output port settings

Step **Action**

SC-10296

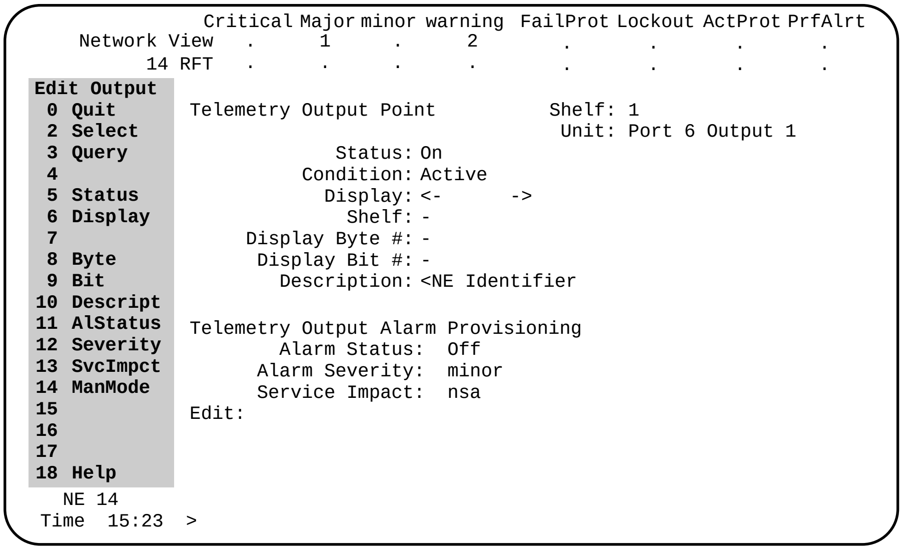


```
                 Critical Major minor warning  FailProt Lockout ActProt PrfAlrt
      System View   .      .     .      1        .       .       .       .
            7 RFT   .      .     .      1        .       .       .       .
Tel Output
 0 Quit       Telemetry Output Point          Shelf: 1
 2 Select                                      Unit: Port 6 Output 6
 3 Query                   Status: On
 4                      Condition: Inactive
 5                        Display: <-      ->
 6 Operate                  Shelf: -
 7 Release           Display Byte #: -
 8 OperMnt            Display Bit #: -
 9                      Description: <
10
11 Edit       Telemetry Output Alarm Provisioning
12                    Alarm Status:  Off
13                  Alarm Severity:  minor
14                  Service Impact:  nsa
15            DTLPORT:
16
17
18 Help
   NE 14
 Time  15:23  >
```

3 Edit the output telemetry point. Enter:

edit ↵

The following output telemetry point screen appears.



```
                 Critical Major minor warning  FailProt Lockout ActProt PrfAlrt
     Network View   .      1     .      2        .       .       .       .
           14 RFT   .      .     .      .        .       .       .       .
Edit Output
 0 Quit       Telemetry Output Point          Shelf: 1
 2 Select                                      Unit: Port 6 Output 1
 3 Query                   Status: On
 4                      Condition: Active
 5 Status                 Display: <-      ->
 6 Display                  Shelf: -
 7                   Display Byte #: -
 8 Byte               Display Bit #: -
 9 Bit                  Description: <NE Identifier
10 Descript
11 AlStatus   Telemetry Output Alarm Provisioning
12 Severity           Alarm Status:  Off
13 SvcImpct         Alarm Severity:  minor
14 ManMode          Service Impact:  nsa
15            Edit:
16
17
18 Help
   NE 14
 Time  15:23  >
```

—continued—

Procedure 9-9 (continued)

Changing the telemetry output port settings

Step	Action
4	Set or change any or all of the parallel telemetry alarm output parameters. If you are provisioning for the first time, set all of the parameters. Repeat this procedure for each alarm point.

Parameter	**Do the following**
status	Set the status of the output distribution point by entering: **status <value>** ↵ where <**value**> **on** or **off**
delete display ID	Check the accuracy of the display ID. Remove the specified display from the alarm point by entering: **ManMode** ↵ Confirm the removal. Enter y for yes or n for no. **y**↵
display type and ID	Set the display type and specify the display number by entering: **display <display type> <display id>** ↵ where <display type> **monitor** or **remote** <display id> **1** to **8** (for monitor display type), **1** to **32** (for remote display type) The system administrator cannot add a remote display type.
byte	Specify the byte number of the display to be used by entering: **byte <value>** ↵ where <value> **1** to **8**
bit	Specify the bit number of the byte to be used by entering: **bit <value>** ↵ where <value> **1** to **8**
description	Specify the alarm point description you want by entering: **descript <text>** ↵ where <text> up to 40 characters within single quotes if spaces or special characters (?, =) are included, or if the first character is a number

—continued—

Procedure 9-9 (continued)
Changing the telemetry output port settings

Step	Action
5	To change the settings of other telemetry output points, go to step 4. Otherwise, go to step 6.
6	Quit to the main menu screen.

If you are at the	**Then**
Telemetry Output Point screen	Enter: **quit 2** ↵ *The Network Element Status screen appears.*
Edit Output screen	Enter: **quit 3** ↵ *The Network Element Status screen appears.*

—end—

Procedure 9-10
Manually operating or releasing a telemetry output relay

Use this procedure to manually operate or release one of the relays of the telemetry outputs.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step **Action**

1 Access the system administration screen and display the user profile parameters. Enter:

admin ip ↵

The system administration screen with the user profile parameters appears.

2 Display the output telemetry port parameters. Enter:

dtlport <port #> <point #> ↵

where

<port #>	**6**
<point #>	**1** to **18**

3 To edit the output telemetry point. Enter:

edit ↵

4 To delete the display, enter:

ManMode ↵

Confirm your action (for off only), enter:

yes ↵

5 To exit the screen, enter:

quit ↵

—continued—

Procedure 9-10 (continued)
Manually operating or releasing a telemetry output relay

Step	**Action**
6	To enable or disable the point, enter: **<action>**↵ where <action> **operate** or **release** *A screen that shows the status of the telemetry output relay appears.*

—end—

Provisioning E2A telemetry information

The AccessNode allows you to manage E2A alarm and status information at the cluster level and to transmit the information to remote alarm-monitoring equipment. A cluster is composed of an operations controller (OPC) and up to three fiber central office terminal-remote fiber terminal (FCOT-RFT) pairs.

Parallel telemetry for an AccessNode cluster is managed through telemetry input and output ports along with parallel telemetry software. The E2A Alarm Manager is the OPC software tool that manages parallel telemetry for all network elements under the OPC span of control. The tool is located in the Network Admin toolset.

Using this tool, you can check the state of cluster-wide alarms or status conditions. In this document, both alarms and status conditions are referred to as alarms. You can also use the tool to assign an individual cluster-wide alarm to a specific signal distribution point (SDP). Signal distribution points as well as the types of alarms they can transmit are described in the following paragraphs.

Signal distribution points

Signal distribution points are relays located in the maintenance interface card (MIC) of the FCOT. Eighteen signal distribution points exist. Each signal distribution point indicates the presence or absence of a type of alarm in the OPC span of control.

When a specific alarm or alarm condition occurs, the relay is closed. The signal distribution point is then considered active. A parallel telemetry output port transmits status to the remote alarm-monitoring equipment. For more information on input and output ports, see *Alarms and Surveillance Description*, 323-3001-104, in *Description*, Volume 2A.

When a network element is first commissioned, signal distribution points are set to transmit telemetry for the local network element. The E2A Alarm Manager is used to reset these signal distribution points for cluster-level telemetry. These points are usually set during commissioning, but can also be done later, as necessary.

TBOS displays

Alarms and status conditions are organized into sets of serial telemetry data called displays. Displays contain 64 bits (that is, display points), where each bit has a value of 1 or 0 indicating:

- whether an alarm is raised
- whether the state of an alarm condition is on or off

All displays are transmitted using the telemetry byte-oriented serial (TBOS) protocol. The meaning of each alarm and its position in the display is predefined and cannot be changed.

Signal distribution points can be assigned to transmit alarms from two types of displays: monitor or cluster.

Monitor displays

Network element displays represent alarms and status conditions for an individual network element. For parallel telemetry, network element displays carry information for the local network element only. Local displays are assigned to a signal distribution point (or deleted) at the local network element user interface.

Each network element receives its parallel telemetry information from 11 external sensors called scan points. The scan points receive alarms indicating, for example, high temperatures or open cabinet doors.

Cluster display

The E2A Alarm Manager collects network element-level displays from all network elements in the cluster and creates a cluster display. This cluster display is derived from all 2 Monitor displays in the OPC span of control. Alarms from the cluster display are assigned to a signal distribution point at the OPC user interface, using the E2A Alarm Manager tool.

The cluster display is distributed to all active network elements in the cluster. (Active network elements contain the appropriate parallel telemetry software and parallel telemetry ports.)

In a cluster display, a state change indicates that an alarm or alarm condition has occurred in any network element in the OPC span of control. If a second alarm or status change of the same type occurs before the first is cleared, the cluster display does not change, since it already indicates the existence of that alarm in the cluster.

Like all displays, the cluster display has 64 bits (that is, display points). Table 10-1 on page 10-4 lists 64 display points in the cluster display. Except for point 64, which is reserved, you can use the E2A Alarm Manager tool to assign any cluster display point that is not empty to a signal distribution point.

Since only 18 signal distribution points exist, you can only transmit up to 18 alarms at the same time.

Table 10-1
Alarms in the cluster display

Point	Byte	Bit	Description
1	1	1	Critical alarm in cluster
2	1	2	Major alarm in cluster
3	1	3	Minor alarm in cluster
4	1	4	Cluster-level warning alarm
5	1	5	Cluster display inaccurate
6	1	6	Cluster ID C/M//m/w alarms
7	1	7	Cluster ID C/M/m alarms
8	1	8	Empty
9	2	1	Any OC-n indication in cluster
10	2	2	Any DS-n indication in cluster
11	2	3	OC-n/DS-n signal failure in cluster
12	2	4	OC-n/DS-n equipment failure in cluster
13	2	5	OC-n/DS-n protection switch complete in cluster
14	2	6	Empty
15	2	7	Empty
16	2	8	Empty
17	3	1	Common equipment failure in cluster
18	3	2	Empty
19	3	3	Empty
20	3	4	Empty
21	3	5	Empty
22	3	6	Empty
23	3	7	Empty
24	3	8	ac power fail in cluster
25	4	1	low battery in cluster
26	4	2	Empty
27	4	3	Empty
28	4	4	Empty
29	4	5	Empty
30	4	6	Empty
31	4	7	Empty
32	4	8	Empty

—continued—

Table 10-1 (continued)
Alarms in the cluster display

Point	Byte	Bit	Description
33	5	1	Empty
34	5	2	Empty
35	5	3	Empty
36	5	4	Environmental subset 1 alarm in cluster
37	5	5	Environmental subset 2 alarm in cluster
38	5	6	Empty
39	5	7	Empty
40	5	8	Empty
41	6	1	Empty
42	6	2	Remote NE ID C/M//m/w alarms
43	6	3	Remote NE ID C/M/m alarms
44	6	4	Empty
45	6	5	Empty
46	6	6	Empty
47	6	7	Empty
48	6	8	Empty
49	7	1	Empty
50	7	2	Empty
51	7	3	Empty
52	7	4	Empty
53	7	5	Empty
54	7	6	Empty
55	7	7	Empty
56	7	8	Empty
57	8	1	Empty
58	8	2	Empty
59	8	3	Empty
60	8	4	Empty
61	8	5	Empty
62	8	6	Always set (on)
63	8	7	Always clear (off)
64	8	8	Reserved

—end—

The E2A Alarm Manager groups alarms into the following categories:

- cluster alarms
- location alarms
- equipment alarms
- facility alarms
- environmental alarms

For further information on the E2A Alarm Manager tool, see the description in *OPC User Interface Description*, 323-3001-301, in this volume.

Chapter task list

This chapter includes the following tasks.

Procedure		**See**
10-1	Viewing the state of a signal distribution point	page 10-7
10-2	Assigning an alarm to a signal distribution point	page 10-8
10-3	Deleting an alarm from a signal distribution point	page 10-11
10-4	Assigning the default alarm to a signal distribution point	page 10-13

If you cannot complete these procedures, contact your next level of support.

Procedure 10-1
Viewing the state of a signal distribution point

Use this procedure to

- check the status of a signal distribution point (either on or off)
- check if an alarm has occurred in the cluster (that is, the alarm is either active or inactive)
- identify the alarm assigned to a signal distribution point

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the operations controller (OPC)
- read the command conventions for the interface you are using (CMT or graphical) in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step **Action**

1 Log in to the OPC and open the E2A Alarm Manager.

The E2A Alarm Manager main window appears.

2 In the Active Network Elements list, move to the network element (NE) where the signal distribution point is located, then press **Ctrl_A** (or Keypad **0**).

The network element is highlighted.

3 Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).

The list item menu appears.

4 Select the Detail command by pressing **Space** (or Keypad **0**).

Details for the selected NE appear in the Signal Distribution Point Assignments list.

5 To close the tool:

a. Display the window menu by pressing **Ctrl_L W** (or Keypad **6**).

The window menu appears.

b. Select the Exit command by pressing **Space** (or Keypad **0**).

The tool closes.

—end—

Procedure 10-2
Assigning an alarm to a signal distribution point

Use this procedure to assign a cluster alarm to a signal distribution point. Then, when this type of alarm occurs in the cluster, the signal distribution point displays “Active” in the Condition column. This state change is transmitted to remote alarm-monitoring equipment.

If another alarm of the same type occurs before the first alarm is cleared, the signal distribution point remains active. It stays active until all alarms of the same type are cleared.

The following list describes the 21 alarms that are available. You can only assign up to 18 alarms at the same time (see Notes 1 and 2):

Cluster alarms
Critical alarm in cluster*
Major alarm in cluster*
Minor alarm in cluster*
Cluster-level warning alarm
Cluster display inaccurate

Location alarms
Cluster ID—C/M/m alarms*
Cluster ID—C/M/m/w alarms
Remote NE ID—C/M/m alarms
Remote NE ID—C/M/m/w alarms

Equipment alarms
OC-n/DSn equipment failure in cluster*
OC-n/DSn protection switch complete in cluster *
Common equipment failure in cluster *

Facility alarms
Any OC-n indication in cluster*
Any DSn indication in cluster*
OC-n/DSn signal failure in cluster*

Environmental alarms
ac power failure in cluster*
Low battery in cluster*
Environmental subset 1 alarm in cluster*
Environmental subset 2 alarm in cluster*
Always set (on)
Always clear (off)

—continued—

Procedure 10-2 (continued)
Assigning an alarm to a signal distribution point

Note 1: Items with an asterisk (*) are cluster default assignments. See Procedure 10-4, “Assigning the default alarm to a signal distribution point.”

Note 2: You can only assign an alarm to one signal distribution point.

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the operations controller (OPC)
- read the command conventions for the interface you are using (CMT or graphical) in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC and open the E2A Alarm Manager. *The E2A Alarm Manager main window appears.*
2	In the Active Network Elements list, move to the network element (NE) where the signal distribution point is located, then press **Ctrl_A** (or Keypad **0**). *The NE is highlighted.*
3	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**). *The list item menu appears.*
4	Select the Detail command by pressing **Space** (or Keypad **0**). *Details for the selected NE are displayed in the Signal Distribution Point Assignments list.*
5	Tab to the Signal Distribution Point Assignments list.
6	Move to the signal distribution point you want to change (6 to 18), then press **Ctrl_A** (or Keypad **0**). *The signal distribution point is highlighted.*
7	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**). *The list item menu appears.*
8	Select the Assign SDP command by pressing **Space** (or Keypad **0**). *A dialog appears, showing the NE and signal distribution point ID you have selected. The Assigned Alarm field displays the current setting of the signal distribution point.*

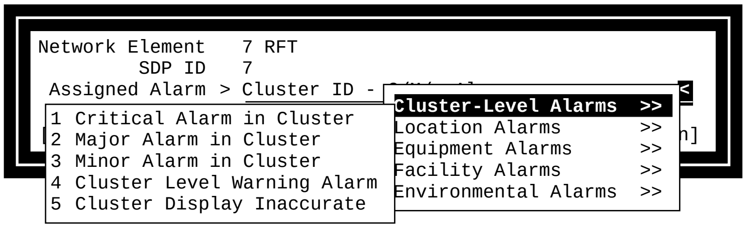
—continued—

Procedure 10-2 (continued)

Assigning an alarm to a signal distribution point

Step	Action
9	In the Assigned Alarm field, display the chooser menu by pressing **Ctrl_L /** (or Keypad **3**). *Chooser menus appear, showing the alarms you can assign to this signal distribution point.*

PC-20578



```
Network Element   7 RFT
         SDP ID   7
 Assigned Alarm > Cluster ID -
```

10 In the right cascade menu, use the down arrow key to move to the type of alarm you want to assign (that is, Cluster-level, Location, Equipment, Facility, or Environmental alarms).

The selected type of alarm is highlighted.

11 Use the left arrow key to move to the left cascade menu.

The cursor appears in the left cascade menu.

12 Use the down arrow key to move to the specific alarm you want to assign, then press **Space** (or Keypad **0**).

The cascade menus disappear. The selected alarm appears in the Assigned Alarm field.

13 Tab to the OK button, then press **Ctrl_A** (or Keypad **0**).

The Assign SDP dialog appears.

14 Tab to the OK button, then press **Ctrl_A** (or Keypad **0**).

The selected alarm is assigned to the signal distribution point.

15 To close the tool:

a. Display the window menu by pressing **Ctrl_L W** (or Keypad **6**).

The window menu appears.

b. Select the Exit command by pressing **Space** (or Keypad **0**).

The tool closes.

—end—

Procedure 10-3
Deleting an alarm from a signal distribution point

Use this procedure to remove the assignment between a cluster alarm and a signal distribution point.

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the operations controller (OPC)
- read the command conventions for the interface you are using (CMT or graphical) in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step **Action**

1 Log in to the OPC and open the E2A Alarm Manager.

The E2A Alarm Manager main window appears.

2 In the Active Network Elements list, move to the NE where the signal distribution point is located, then press **Ctrl_A** (or Keypad **0**).

The NE is highlighted.

3 Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).

The list item menu appears.

4 Select the Detail command by pressing **Space** (or Keypad **0**).

Details for the selected NE appear in the Signal Distribution Point Assignments list.

5 Tab to the Signal Distribution Point Assignments list.

6 Move to the signal distribution point you want (6 to 18), then press **Ctrl_A** (or Keypad **0**).

The signal distribution point is highlighted.

7 Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).

The list item menu appears.

8 Move to the Unassign SDP command, then press **Space** (or Keypad **0**).

The Unassign SDP dialog appears, prompting you to confirm your request.

9 Tab to the OK button, then press **Ctrl_A** (or Keypad **0**).

The Unassign SDP confirmation dialog closes. The selected alarm is no longer assigned to the signal distribution point.

—continued—

Procedure 10-3 (continued)
Deleting an alarm from a signal distribution point

Step	Action
10	To close the tool: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 10-4
Assigning the default alarm to a signal distribution point

Use this procedure to assign the default cluster alarm to a signal distribution point. Table 10-2 lists the default cluster alarms that are assigned to the signal distribution points with this procedure.

Table 10-2
Default cluster alarm assignments for signal distribution points

SDP	Default alarm
6	Cluster ID—C/M/m alarms
7	Critical alarm in cluster
8	Major alarm in cluster
9	Minor alarm in cluster
10	Any OC-n indication in cluster
11	Any DSn indication in cluster
12	OC-n/DSn equipment failure in cluster
13	OC-n/DSn Protection switch completion in cluster
14	Common equipment failure in cluster
15	ac power failure in cluster
16	Low battery in cluster
17	Environmental subset 1 alarm in cluster
18	Environmental subset 2 alarm in cluster

—continued—

Procedure 10-4 (continued)
Assigning the default alarm to a signal distribution point

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the operations controller (OPC)
- read the command conventions for the interface you are using (CMT or graphical) in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC and open the E2A Alarm Manager. *The E2A Alarm Manager main window appears.*
2	In the Active Network Elements list, move to the network element (NE) where the signal distribution point is located, then press **Ctrl_A** (or Keypad **0**). *The NE is highlighted.*
3	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**). *The list item menu appears.*
4	Select the Detail command by pressing **Space** (or Keypad **0**). *Details for the selected NE appear in the Signal Distribution Point Assignments list.*
5	Tab to the Signal Distribution Point Assignments list.
6	Move to the signal distribution point you want (6 to 18), then press **Ctrl_A** (or Keypad **0**). *The signal distribution point is highlighted.*
7	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**). *The list item menu appears.*
8	Move to the Cluster default command, then press **Space** (or Keypad **0**). *The Assign Cluster Default dialog appears, prompting you to confirm your request.*
9	Tab to the OK button, then press **Ctrl_A** (or Keypad **0**). *The Assign Cluster Default dialog closes. The default alarm for the selected signal distribution point replaces the existing alarm.*

—continued—

Procedure 10-4 (continued)

Assigning the default alarm to a signal distribution point

Step **Action**

10 To close the tool:

a. Display the window menu by pressing **Ctrl_L W** (or Keypad **6**).

The window menu appears.

b. Select the Exit command by pressing **Space** (or Keypad **0**).

The tool closes.

—end—

Setting network element parameters

This chapter has procedures to set the parameters of a network element (NE), including:

- the timing for scheduled events, such as making backup copies of data and running the equipment exerciser
- the NE name

Perform these procedures at the network element user interface (NEUI).

Chapter task list

This chapter includes the following tasks:

Procedure	Task	See
11-1	Displaying the network element profile parameters	page 11-2
11-2	Changing the network element name	page 11-3
11-3	Displaying the exerciser and backup schedule	page 11-4
11-4	Changing a scheduled shelf event or exercise	page 11-5

If you cannot complete these procedures, contact your next level of support.

Procedure 11-1
Displaying the network element profile parameters

Use this procedure to display the currently selected network element (NE) and its profile parameters.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step	Action
1	Access the system administration screen and display the network element profile parameters. Enter: **admin nep** ↵ *A screen that shows the profile parameters appears.*

—end—

Procedure 11-2
Changing the network element name

Use this procedure to change the name of the network element (NE).

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- You must be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step	Action
1	Access the system administration screen and display the NE profile parameters. Enter: **admin nep ↵** *The system administration screen appears.*
2	Query another NE. Enter: **nename <nename>↵** where <nename> up to 13 characters within single quotes if you include spaces or special characters(?, =), or if the first character is a number. An octothorpe character (#) is not valid for use within the network element name. The first character must be an alpha character. ***Note:*** When naming an NE, if the NE name will be used with TL1 TID and SID identifiers, you must use the TL1 TID/SID permissible character set. This character set includes uppercase or lowercase letters A to Z, numbers 0 to 9, and the special characters, dash, underscore, comma, and period. The special characters cannot appears as the first character in the name. *A screen that shows the NE name appears.*

—end—

Procedure 11-3
Displaying the exerciser and backup schedule

Use this procedure to display the execution schedule of the exerciser and the backup utility on the network element (NE). The exerciser is only available on terminal equipment.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step	Action
1	Access the system administration screen and display the NE profile parameters. Enter: **admin nep** ↵ *The system administration screen appears.*
2	Access the schedule screen. Enter: **schedule** ↵ *A screen that shows the network element schedule appears.*

—end—

Procedure 11-4
Changing a scheduled shelf event or exercise

Use this procedure to change the schedule of an event or exercise for a particular shelf. You can schedule a backup event that creates backup copies of data, or you can schedule when the equipment exerciser runs. A scheduled event or exercise runs automatically starting on the specified day and time, continuing at the specified frequency, and ending on the specified day and time.

The Schedule Active field indicates whether an event is currently running. For example, if the value for the Backup event is *, then a backup is currently running. If the value is. (period), then the event is not currently running.

Note that automatic shelf backup, described here, and manual shelf backup, described in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B, do essentially the same thing. The difference is that the automatic backup occurs regularly, while the manual backup occurs only in special circumstances.

Shelf database backups are stored at the operations controller (OPC) where up to three active backups, labeled oldest, middle, and newest, can be kept at any one time. When a manual or automatic backup is performed, the oldest copy is deleted, and the other copies are relabeled accordingly.

Requirements

Before starting this procedure, you must:

- be logged on the network element user interface (NEUI) and be at the main menu level
- be familiar with the VT100-type NEUI. For a reminder of how to use the interface, see *Network Element User Interface Description*, 323-3001-300, in this volume.

Action

Step	Action
1	Access the system administration screen and display the NE profile parameters. Enter: **admin nep** ↵ *The system administration screen appears.*

—continued—

Procedure 11-4 (continued)
Changing a scheduled shelf event or exercise

Step	Action
2	Access the schedule screen. Enter: **schedule** ↵ *The schedule screen appears.*
3	Access the edit schedule screen. Enter: **edit** ↵ *The edit schedule screen appears.* ***Note:*** To prevent a scheduled event from occurring, set the end date to be today.
4	Set or change any or all of the shelf scheduling parameters. If you are provisioning the event or exercise for the first time, set all of the parameters.

Parameter	Complete the following
frequency	Specify how often the event or exercise runs in a given period by entering: **frequency <item #> <time interval> <unit>** ↵ where <item #> **1** or **2**; **1** is exerciser, **2** is backup <time interval> **1** to **730**, for day, **1** to **17543**, for hour, **60** to **32767**, for minute, **3600** to **32767**, for second <unit> **d**, **h**, **m**, or **s**; for day, hour, minute or second
strttime	Specify the time for the event or exercise to start by entering: **strttime <item #> <hour> <minute>** where <item #> **1** or **2**; **1** is exerciser, **2** is backup <hour> **0** to **23**; defaults to current hour <minute> **0** to **59**; defaults to 0
strtdate	Specify the date for the event or exercise to start by entering: **strtdate <item #> <day> <month> <year>** ↵ where <item #> **1** or **2**; **1** is exerciser, **2** is backup <day> **1** to **31**; defaults to current day <month> **1** to **12**; defaults to 1 <year> **1976** to **2039**; defaults to 1976

—continued—

—continued—

Procedure 11-4 (continued)
Changing a scheduled shelf event or exercise

Step Action

Parameter	**Complete the following**
endtime	Specify the time for the event or exercise to stop by entering: **endtime <item #> <hour> <minute>** ↵ where <item #> **1** or **2**; **1** is exerciser, **2** is backup <hour> **0** to **23**; defaults to **-**, meaning forever <minute> **0** to **59**; defaults to 0 To schedule the exerciser forever, do not enter an endtime.
enddate	Specify the date for the event or exercise to stop by entering: **enddate <item #> <day> <month> <year>** ↵ where <item #> **1** or **2**; **1** is exerciser, **2** is backup <day> **1** to **31**; defaults to every day <month> **1** to **12**; defaults to 1 <year> **1976** to **2039**; defaults to 1976 To schedule the exerciser forever, do not enter a value for <day>, < month> or <year>. Press Return after <event #>.
—end—	

5 You can schedule the other event or exercise or quit.

If you want to	**Then go to**
schedule other	step 3
quit	step 6

6 Quit to the main menu screen.

If you are at the	**Then go to**
NE Schedule menu screen	step 7
Edit Sched menu screen	step 8

—continued—

Procedure 11-4 (continued)
Changing a scheduled shelf event or exercise

Step **Action**

7 From the NE Schedule menu screen, exit the main menu screen by entering:

quit 2 ↵

The Network Element Status screen appears.

8 From the Edit Sched menu screen, exit the main menu screen by entering:

quit 3 ↵

The Network Element Status screen appears.

Example

To display the scheduled events for the shelf, enter:

admin nep ↵

schedule ↵

Currently, backup copies of the shelf data do not run automatically. You want to set the scheduler to run backups automatically every 36 hours, beginning at 11:30 p.m., on October 5, 1997. Enter:

edit ↵

strtdate 2 5 10 97 ↵

strttime 2 23 30↵

frequency 2 36 h↵

enddate 2 ↵

endtime 2 ↵

—end—

Monitoring NE logs

This chapter has the procedures for setting log monitoring parameters for format and output. It also describes how to list the logs and log reports, how to display reports, how to clear reports, and how to start and stop log report output.

Chapter task list

This chapter includes the following tasks:

Procedure		See
	System Administration provisioning tasks	
12-1	Connecting a log output device and configuring a user interface port for a log output device	page 12-2
12-2	Setting the NE log format	page 12-5
12-3	Enabling or disabling user interface (UI) ports (1 or 2) for printing logs	page 12-6
	Occasional tasks	
12-2	Setting the NE log format	page 12-5
12-3	Enabling or disabling user interface (UI) ports (1 or 2) for printing logs	page 12-6
12-4	Listing NE logs and log reports	page 12-8
12-5	Displaying NE log reports	page 12-9
12-6	Redisplaying the last log report	page 12-11
12-7	Clearing log reports	page 12-12
12-8	Starting and stopping log output to a terminal	page 12-13

If you cannot complete these procedures, contact your next level of support.

Procedure 12-1
Connecting a log output device and configuring a user interface port for a log output device

Use this procedure to connect a log output device (terminal, printer or magnetic tape unit) and configure the communication parameters of the user interface port for the log output device. Configuration includes changing the baud rate and specifying the stop bits, the type of parity verification, and the character size.

Requirements

Before starting this procedure, you must:

- have admin level security clearance
- deactivate the user interface port (1 or 2) before changing its baud rate, stop bits, the type of parity verification or character size. A user interface port cannot be deactivated if a user is already logged in to this port.
- know the communication parameters of the output device and the port
- read the command conventions described in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step **Action**

1 From the Network Element Status screen, display the Interfaces Ports Status screen by entering:

admin ip ↵

The Interface Ports Status screen appears.

2 Display the settings for user interface port 2 by entering:

dtlport 2 ↵

The user interface port 2 configuration screen appears.

If port state reads	Then go to
IS (in service)	step 3
OOS (out of service)	step 4

—continued—

Procedure 12-1 (continued)

Connecting a log output device and configuring a user interface port for a log output device

Step	Action
3	Deactivate user interface port (1 or 2). Enter:
	chgstate OOS ↵
	Confirm your action. Enter:
	yes ↵
4	Access the Edit UI menu to change the configuration for this user interface port by entering:
	edit ↵
	The Edit UI menu appears.
5	Set or change any or all of the user interface port parameters listed in the table below. If you are provisioning for the first time, set all of the parameters. Set or change any parameter as often as required before proceeding to step 6.

Parameter	Complete the following
baudrate	Set the baud rate by entering: **baudrate <value>**↵ where <value> **300**, **1200**, **2400**, **4800**, or **9600**
parity	Set the parity error type by entering: **parity <type>**↵ where <type> **none**, **even**, or **odd**
charsize	Set the number of bits in a character by entering: **charsize <value>**↵ where <value> **7** or **8**
stopbit	Set the number of stopbits by entering: **stopbits <value>**↵ where <value> **1** or **2**

The parameter settings appear on screen as they are set or changed.

—continued—

Procedure 12-1 (continued)
Connecting a log output device and configuring a user interface port for a log output device

Step	Action
6	Activate the user interface port (1 or 2). Enter: **quit** ↵ **chgstate IS** ↵
7	Exit the Edit UI screen by entering: **quit 3** ↵ *The Network Element Status screen appears.*
8	At the output device, connect the modem cable to the modem connector on the output device according to the manufacturer’s instructions. (If your output device is not a terminal, you may have to disconnect the modem cable from the terminal that is already connected.)
9	Plug in the power cord of the output device and switch on the power.
10	Set the terminal communication parameters according to the manufacturer’s instructions using the parameters already defined for the modem port.

—end—

Procedure 12-2
Setting the NE log format

Use this procedure to set the log format between normal and short. The normal format is the default. This format displays summary information on the first line of the log report and detailed information below. The short format displays only one line of summary information.

Requirements

Before starting this procedure, you must:

- have admin level security clearance
- read the command conventions described in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step **Action**

1 From the Network Element Status screen, display the Network Element Profile screen by entering:

admin nep ↵

The Network Element Profile screen appears.

2 From the Network Element Profile screen, display the Log Utility screen by entering:

logs ↵

The Log Utility screen appears.

3 Set or change the format parameter by entering:

format <style>↵

where:

<style>	**normal** or **short**

The new format appears in the next log report that is output or that appears with the open command.

4 Return to the main menu by entering:

quitlogs ↵

The Network Element Profile screen appears.

—end—

Procedure 12-3
Enabling or disabling user interface (UI) ports (1 or 2) for printing logs

Use this procedure to activate a user interface port (1 or 2) for connection to a printer to print status logs.

Requirements

Before starting this procedure, you must:

- have admin level security clearance
- have a serial printer connected to the corresponding port and configured. (See Procedure 12-1 on page 12-2.)
- read the command conventions described in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step	Action
1	From the Network Element Status screen, display the Network Element Profile screen by entering: **admin nep** ↵ *The Network Element Profile screen appears.*
2	From the Network Element Profile screen, display the Log Utility screen by entering: **logs** ↵ *The Log Utility screen appears.*

—continued—

Procedure 12-3 (continued)
Enabling or disabling user interface (UI) ports (1 or 2) for printing logs

Step **Action**

3 Enable or disable UI port for printing logs.

If you want to	**Then**
enable UI port	Enable UI port by entering: **startdev <UI port>**↵ where <**UI port**> user interface port **ui_1** or **ui_2** *Log reports are directed to the specified output device as they are generated. Output continues until you issue a stopdev command.*
disable UI port	Disable UI port by entering: **stopdev <UI port>**↵ where <**UI port**> user interface port **ui_1** or **ui_2**

4 Return to the main menu screen by entering:

quitlogs 2 ↵

The Network Element Profile screen appears.

—end—

Procedure 12-4
Listing NE logs and log reports

Use this procedure to display a list of all logs and all log reports reported by the network element (NE) log utility.

Requirements

Before starting this procedure, you must:

- have admin level security clearance
- read the command conventions described in *Network Element User Interface Description*, 323-3001-300, in this volume

Action

Step **Action**

1 From the Network Element Status screen, display the Network Element Profile screen by entering:

admin nep ↵

The Network Element Profile screen appears.

2 From the Network Element Profile screen, display the Log Utility screen by entering:

logs ↵

The Log Utility screen appears.

3 You can display a list of all available logs and all available log reports.

If you want to list	Then
all available logs	List logs available from the NE by entering: **listlogs** ↵ *A list of available log names appears.*
all available log reports	List log reports available from the NE by entering: **listreps** ↵ *A list of available log reports appears.*

4 Return to the main menu screen by entering:

quitlogs ↵

The Network Element Profile screen appears.

—end—

Procedure 12-5
Displaying NE log reports

Use this procedure to display the contents of a log report.

Requirements

Before starting this procedure, you must:

- have admin level security clearance
- read the command conventions described in *Network Element User Interface Description*, 323-3001-300, in this volume

Action

Step **Action**

1 From the Network Element Status screen, display the Network Element Profile screen by entering:

admin nep ↵

The Network Element Profile screen appears.

2 From the Network Element Profile screen, display the Log Utility screen by entering:

logs ↵

The Log Utility screen appears.

3 List the logs available from the NE and identify the log name of the report you want to display. If you know the log name, skip to step 4.

listlogs ↵

A list of log names appears.

4 List logs reports available from the network element by entering:

open <log name>↵

where

<log name> one from list produced from listlogs

If the log contains a report, the first log reports appears. A log report contains the log name and a predefined log number.

—continued—

Procedure 12-5 (continued)
Displaying NE log reports

Step **Action**

5 Display other log reports for the same log.

If you want to display the	**Then enter**
next log	**forward** ↵
previous log	**back** ↵
first log	**start** ↵
last log	**last** ↵

The specified log report appears. If no next or previous log report is available to display, the log utility provides a message.

6 Return to the main menu screen by entering:

quitlogs ↵

The Network Element Profile screen appears.

—end—

Procedure 12-6
Redisplaying the last log report

Use this procedure to recall the contents of the last log report displayed.

Requirements

Before starting this procedure, you must:

- have admin level security clearance
- have used the open command and displayed a log report from the Log Utility screen
- read the command conventions described in *Network Element User Interface Description*, 323-3001-300, in this volume

Action

Step	Action
1	From the Network Element Status screen, display the Network Element Profile screen by entering: **admin nep** ↵ *The Network Element Profile screen appears.*
2	From the Network Element Profile screen, display the Log Utility screen by entering: **logs** ↵ *The Log Utility screen appears.*
3	Redisplay the last NE log displayed with the open command by entering: **type**↵ The last log report displayed appears.
4	Return to the main menu by entering: **quitlogs** ↵ *The Network Element Profile screen appears.*

—end—

Procedure 12-7
Clearing log reports

Use this procedure to clear all log reports with a specific log name.

Requirements

Before starting this procedure, you must:

- have admin level security clearance
- know the log name in full
- read the command conventions described in *Network Element User Interface Description*, 323-3001-300, in this volume

Action

Step **Action**

1 From the Network Element Status screen, display the Network Element Profile screen by entering:

admin nep ↵

The Network Element Profile screen appears.

2 From the Network Element Profile screen, display the Log Utility screen by entering:

logs ↵

The Log Utility screen appears.

3 Clear all log reports for a log by entering:

clearlog <logname>↵

where

<logname> one from list produced from the listlogs command

All log reports with the specified logname are cleared from the log buffer.

4 Return to the main menu screen by entering:

quitlogs ↵

The Network Element Profile screen appears.

—end—

Procedure 12-8
Starting and stopping log output to a terminal

Use this procedure to start and stop displaying log output at your terminal. This procedure is commonly used to view reports for maintenance purposes.

Requirements

Before starting this procedure, you must:

- have admin level security clearance
- read the command conventions described in *Network Element User Interface Description*, 323-3001-300, in this volume

Action

Step **Action**

1 From the Network Element Status screen, display the Network Element Profile screen by entering:

admin nep ↵

The Network Element Profile screen appears.

2 From the Network Element Profile screen, display the Log Utility screen by entering:

logs ↵

The Log Utility screen appears.

3 Start or stop displaying log reports at your terminal.

If you want to	**Then go to**
start displaying log output	step 4
stop displaying log output	step 5

4 Start displaying log output at your terminal by entering:

start ↵

Log reports appear on the terminal screen as they are generated. Output continues until you issue a stop command.

If you want to	**Then**
retire the FWPUI prompt	enter: **while (true) (sleep 100 mins)** ↵
redisplay the FWPUI prompt	press **Break** and enter: **Stop**

—continued—

Procedure 12-8 (continued)
Starting and stopping log output to a terminal

Step	**Action**
5	Stop log output being displayed at your terminal by entering: **stop** ↵ *Log reports stop appearing on the terminal screen as they are generated.*
6	Return to the main menu by entering: **quitlogs** ↵ *The Network Element Profile screen appears.*

—end—

Managing OS Connections

The X.25 virtual circuits provide an operations system (OS) interface to network elements (NE) through the operations controller (OPC). The OS Connection manager allows the OPC administrator to define the connection profiles and manage the X.25 virtual circuit connections.

To configure the OPC port to support X.25 virtual circuits, see Chapter 2, “Configuring OPC ports for X.25, terminal, or printer operation.”

A difference exists between the limit of virtual circuits entered in the OS Connection manager and the value set in the X.25 level 3 parameter (scc0 file). From the OS Connection manager tool, it is possible to have 15 virtual circuit profiles. In the X.25 level 3 parameter (scc0 file), the maximum value set is 8. The scc0 file limits the number of active virtual circuits on the X.25 link, but does not prevent the creation of TL1 virtual circuits in the OS Connection manager.

For further information on the OS Connection manager tool, see the description in *OPC User Interface Description*, 323-3001-301, in this volume.

Chapter task list

This chapter includes the following tasks:

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 13-5
13-4	Resetting a virtual connection to an operations system	page 13-6
13-5	Creating an operations system connection profile	page 13-7
13-6	Modifying an operations system connection profile	page 13-9
13-7	Deleting an operations system connection profile	page 13-10

—continued—

Procedure		**See**
13-8	Modifying the protocol identifier for an operations system connection	page 13-12
13-9	Assigning or modifying target identifiers for testing	page 13-14
13-10	Assigning or modifying target identifiers for surveillance and provisioning	page 13-16
—end—		

Procedure 13-1
Enabling and disabling security mode for TL1

If you are the root user, you can use this procedure to enable and disable security mode. Users other than root cannot change the security mode—the Enabled and Disabled buttons are only available to the root user.

Requirements

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

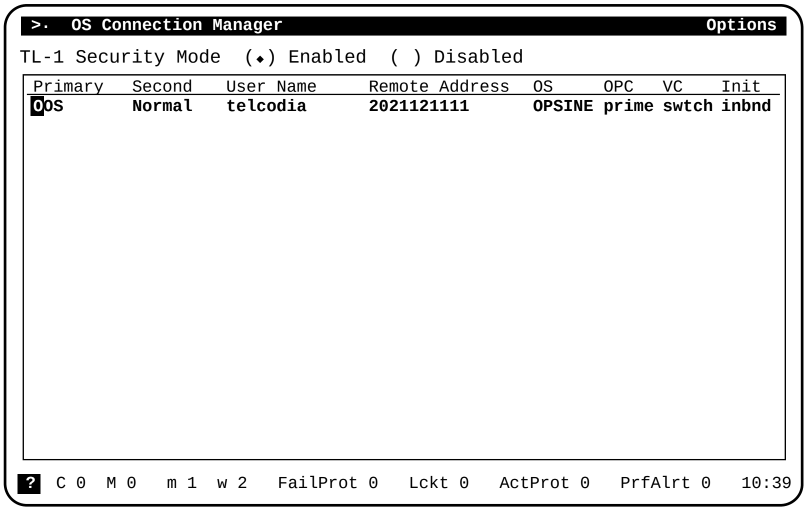
- You must have the root userID and password that permit access to the operations controller (OPC) and to open the OS Connection Manager tool
- You must be familiar with the command conventions for the interface you are using (CMT or graphical)

Action

Step	Action

1 Log in to the OPC and open the OS Connection manager tool.

The OS Connection Manager tool main window appears.



```
 >·  OS Connection Manager                                        Options
TL-1 Security Mode  (◆) Enabled  ( ) Disabled
 Primary   Second   User Name     Remote Address  OS     OPC   VC    Init
 OOS       Normal   telcodia      2021121111      OPSINE prime swtch inbnd

 ?  C 0  M 0   m 1  w 2   FailProt 0   Lckt 0   ActProt 0   PrfAlrt 0   10:39
```

2 Do one of the following:

- To enable security mode, select the Enabled radio button
- To disable security mode, select the Disabled radio button

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.

—end—

Procedure 13-2
Connecting to an operations system

Use this procedure to connect to an operations system. The connection must be in a disconnected state (Primary = OSS, Second = Normal).

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the operations controller (OPC) and to open the OS Connection Manager tool
- read the command conventions for the interface you are using (CMT or graphical) in *User Interface Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC and open the OS Connection Manager tool. *The OS Connection Manager tool main window appears. A text line indicates whether security mode is enabled or disabled.*
2	Move to the desired entry in the list, then press **Ctrl_A** (or Keypad **0**).
3	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).
4	Move to the Connect command, then press **Space** (or Keypad **0**). *The connection is initiated. Primary and secondary fields reflect the progress of the connection.*
5	Close the OS Connection Manager tool: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The User Session Manager appears.*

—end—

Procedure 13-3
Disconnecting from an operations system

Use this procedure to terminate a connection to an operations system. The connection may have been established by either end. The connection must be in a connected state (Primary = IS, Second = Normal).

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the OPC and to open the OS Connection Manager tool
- read the command conventions for the interface you are using (CMT or graphical) in *User Interface Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC and open the OS Connection Manager tool. *The OS Connection Manager tool main window appears. A text line indicates whether security mode is enabled or disabled.*
2	Move to the desired entry in the list, then press **Ctrl_A** (or Keypad **0**).
3	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).
4	Move to the Disconnect command, then press **Space** (or Keypad **0**). *The connection is terminated. Primary and secondary fields reflect the progress of the connection.* ***Note:*** If the primary column remains In Service, disconnect the termination in the X.25 Network interfacing software application.
5	Close the OS Connection Manager tool: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The User Session Manager appears.*

—end—

Procedure 13-4
Resetting a virtual connection to an operations system

Use this procedure to clear communications buffers in an established operations system (OS) connection. This process can alleviate communications problem, although it causes loss of data.

> ***Note:*** A reset is allowed if the virtual connection is in service (IS) and normal states. If connection is out of service (OOS), see Procedure 13-2 on page 13-4 for connecting to an operations system.

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the OPC and to open the OS Connection Manager tool
- read the command conventions for the interface you are using (CMT or graphical) in *User Interface Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC and open the OS Connection Manager tool. *The OS Connection Manager tool main window appears. A text line indicates whether security mode is enabled or disabled.*
2	Move to the desired entry in the list, then press **Ctrl_A** (or Keypad **0**).
3	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).
4	Move to the Reset command, then press **Space** (or Keypad **0**). *The connection is reset. The Second field indicates the progress of the reset.*
5	Close the OS Connection Manager tool: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The User Session Manager appears.*

—end—

Procedure 13-5
Creating an operations system connection profile

Use this procedure to create a new operations system (OS) connection profile. A connection profile is required to support connections to each operations system.

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the OPC and to open the OS Connection Manager tool
- read the command conventions for the interface you are using (CMT or graphical) in *User Interface Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC and open the OS Connection Manager tool. *The OS Connection Manager tool main window appears. A text line indicates whether security mode is enabled or disabled.*
2	Display the list menu by pressing **Ctrl_L** (or Keypad **3**).
3	Select the New User command by pressing **Space** (or Keypad **0**). *The OS Connection Profile dialog appears, with fields either blank, filled, or containing defaults.*
4	Enter a user name in the User Name field.
5	Tab to the Remote Address field and enter a unique address. ***Note:*** The Virtual Circuit Type and the Initialization Type fields are preselected in the X.25 provisioning.
6	Tab to the OS Type field, move to the radio button beside the desired type, then press **Ctrl_A** (or Keypad **0**).
7	Tab to the Physical OPC field, move to the radio button beside the desired type, then press **Ctrl_A** (or Keypad **0**).
8	Tab to the OK button, then press **Ctrl_A** (or Keypad **0**). (You can select the Cancel button to cancel the changes.) *A connection profile is created. A new entry is added to the list in the main window.*

—continued—

Procedure 13-5 (continued)
Creating an operations system connection profile

Step	**Action**
9	Close the OS Connection Manager tool: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The User Session Manager appears.*

—end—

Procedure 13-6
Modifying an operations system connection profile

Use this procedure to modify an existing OS Connection profile.

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the OPC and to open the OS Connection Manager tool
- read the command conventions for the interface you are using (CMT or graphical) in *User Interface Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC and open the OS Connection Manager tool. *The OS Connection Manager tool main window appears. A text line indicates whether security mode is enabled or disabled.*
2	Move to the profile you wish to modify, then press **Ctrl_A** (or Keypad **0**).
3	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).
4	Select the Edit command, by pressing **Space** (or Keypad **0**). *The OS Connection Profile dialog appears, containing the current profile values for the selected profile.*
5	Tab to the fields you want to modify, and enter the text or select the radio buttons as required.
6	Tab to the OK button, then press **Ctrl_A** (or Keypad **0**). (You can select the Cancel button to abort the changes.) *A connection profile is modified.*
7	Close the OS Connection Manager tool: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The User Session Manager appears.*

—end—

Procedure 13-7 **Deleting an operations system connection profile**

Use this procedure to delete an existing operations system (OS) connection profile. This action prevents the establishment of a connection with the operations system. You can delete more than one profile at a time.

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the OPC and to open the OS Connection Manager tool
- read the command conventions for the interface you are using (CMT or graphical) in *User Interface Description*, 323-3001-301, in this volume

Action

Step **Action**

1 Log in to the OPC and open the OS Connection Manager tool.

The OS Connection Manager tool main window appears. A text line indicates whether security mode is enabled or disabled.

2 In the displayed list, move to the first profile you wish to delete, then press **Ctrl_A** (or Keypad **0**).

3 If you want to delete additional profiles, move to these profiles in the list, then press **Ctrl_Y** (or Keypad **.**).

Note: The profile must be out of service (OOS) to select the delete command. To provision to OOS, see Procedure 13-3 on page 13-5.

4 Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).

5 Move to the Delete command, then press **Space** (or Keypad **0**).

A confirmation dialog appears.

6 Within this dialog, you can continue with the deletion of the listed entries, remove individual list entries before proceeding, or cancel the entire operation.

If you want to	Then go to
delete profile entries from the list	step 7
proceed to delete the profiles listed	step 11
cancel the deletion	step 12

7 Tab to the displayed list, move to the first profile you want to remove from the delete list, then press **Ctrl_A** (or Keypad **0**).

—continued—

Procedure 13-7 (continued)
Deleting an operations system connection profile

Step	**Action**
8	If you wish to remove additional profiles, move to these profiles in the list, then select each one by pressing **Ctrl_Y** (or Keypad **.**).
9	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).
10	Select the Un-Delete command by pressing **Space** (or Keypad **0**). *The selected entries are removed from the list.* Go to step 6.
11	Tab to the OK button, then press **Ctrl_A** (or Keypad **0**). *The connection profiles in the list are deleted. You are returned to the main window of the OS Connection Manager.* Go to step 13.
12	Tab to the Cancel button, then press **Ctrl_A** (or Keypad **0**). *No profiles are deleted. The main window of the OS Connection Manager appears.*
13	Close the OS Connection Manager tool: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes, revealing the User Session Manager.*

—end—

Procedure 13-8
Modifying the protocol identifier for an operations system connection

Use this procedure to define or change the protocol identifier, which is used to identify the type of messages from the operations system that the operations controller (OPC) processes. Its value must be obtained by consensus with the operations system or from the standards bodies.

> ***Note:*** For the new protocol ID to take effect after you have performed this procedure, you must reboot the OPC.

Requirements

Before starting this procedure, you must:

- have a userID and password
- obtain a value for the protocol identifier of the operations system
- read the command conventions for the interface you are using (CMT or graphical) in *User Interface Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC using the root userID and open the OS Connection Manager tool.
	The OS Connection Manager tool main window appears.
2	Display the list menu by pressing **Ctrl_L** (or Keypad **3**).
3	Move to the Edit Protocol ID command, then press **Space** (or Keypad **0**).
	The OS Connection Profile dialog appears, with fields either blank, filled, or containing defaults.
4	Select the Size in Bytes field by pressing **Ctrl_A** (or Keypad **0**).
5	Enter the length of the Protocol ID in the Size in Bytes field. This number refers to the number of pairs of hexadecimal digits that you enter in the next step.
6	Tab to the Protocol ID Bytes fields, and enter the pairs of hexadecimal digits that define the protocol identifier. You must tab to each field to enter the data. You must enter the same number of pairs of data as you specified in the Size in Bytes field.

—continued—

Procedure 13-8 (continued)
Modifying the protocol identifier for an operations system connection

Step **Action**

7 Tab to the OK button, then press **Ctrl_A** (or Keypad **0**).

The changes to the Protocol ID are saved. If you cannot select the OK button, you have not logged in to the OPC with the “root” userID.

(You can select the Cancel button to cancel the changes.)

8 Close the OS Connection Manager tool:

a. Display the window menu by pressing **Ctrl_L W** (or Keypad **6**).

The window menu appears.

b. Select the Exit command by pressing **Space** (or Keypad **0**).

The User Session Manager appears.

—end—

Procedure 13-9
Assigning or modifying target identifiers for testing

Use this procedure to assign or modify the target identifiers (TID) for line-and-loop testing of operations systems (OS). To add or change a TID for a surveillance or provisioning system, see Procedure 13-10 on page 13-16.

A TID defines a TL1 target identifier and fully supports Bellcore's format for naming network elements. The TID can be up to 20 characters. The following characters are allowed:

A–Z	hyphen (-)	period (.)
0–9	underscore (_)	

No spaces or other characters are allowed.

> ***Note:*** Although the maximum size of each TID field is 20 characters, different OSs support different TID sizes. You must therefore define the TID to support the OS that will establish connections to your system.

Requirements

Before you start this procedure, you must meet the following requirements:

- have a user ID and password that access the operations controller (OPC) at the root or admin level
- read the command conventions for the CMT or graphical interface (see *User Interface Description*, 323-3001-301, in this volume)

Action

Step	Action
1	Log in to the OPC and open the OS Connection Manager tool. *The OS Connection Manager tool main window appears.*
2	Display the Options menu by pressing **Ctrl_L T** (or Keypad **,**).
3	Move to the TID Mapper command, then press **Space** (or Keypad **0**). *The TID Mapper dialog appears, showing the current Testing and Non-testing OS TIDs for the network elements.*
4	Tab to the Network Element list, then press the up and down arrow keys to move to the network element you want to select.
5	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).

—continued—

Procedure 13-9 (continued)
Assigning or modifying target identifiers for testing

Step	**Action**

6 Move to the Edit TID command, then press **Space** (or Keypad **0**).

The TID Editor dialog appears, showing the current Testing and Non-testing OS TID values for the selected network element.

Note: Do not use this screen to add or change non-testing TIDs. Non-testing TIDS require the tidmap command from the UNIX shell. See Procedure 13-10 on page 13-16 for directions to use tidmap.

7 Complete the instructions in the following table:

To	**Do the following:**
assign a TID	Type the new target identifier in the Testing OS TID field.
change a TID	**a.** To display the menu, press **Ctrl_L** (or Keypad **Enter**). **b.** Move to the Select all command, then press **Space** (or Keypad **0**). *The entire field value is selected.* **c.** Type the new TID name.
save (or cancel) and leave the dialog	To display the window menu, press **Ctrl_L W** (or Keypad **6**). *The window menu appears.* To select the Exit command, press **Space** (or Keypad **0**). *The User Session Manager appears.*

8 Repeat step 7 for each TID you want to add or change.

—end—

Procedure 13-10
Assigning or modifying target identifiers for surveillance and provisioning

Use this procedure to assign or modify the target identifiers (TID) for surveillance and provisioning interfaces. To add or change a TID for a testing interface, see Procedure 13-9 on page 13-14.

A TID defines a TL1 target identifier and fully supports Bellcore's format for naming network elements. The TID can be up to 20 characters. The following characters are allowed:

A–Z

0–9

hyphen (-)

underscore (_)

period (.)

No spaces or other characters are allowed.

> ***Note 1:*** Although the maximum size of each TID field is 20 characters, different operations systems (OS) support different TID sizes. You must therefore define the TID to support the OS that will be establishing connections to your system.
>
> ***Note 2:*** This procedure uses the tidmap command. To display help for tidmap, enter:

```
tidmap↵
```

Requirements

Before you start this procedure, read the following information about upgrading from previous releases:

- If the previous release did not support 20-character TIDs, the network element names are converted to TIDs. If a network element name was not defined or it contains unsupported characters, the network element ID becomes the default TID.

  Note: The automatic TID assignment happens only when you run NMA or OPS. If you look at an operations controller (OPC) where neither NMA or OPS has been run, the TIDs are not defined even though the network element names and IDs are defined.

- If the previous release supported TIDs, the TIDs are preserved.

—continued—

Procedure 13-10 (continued)
Assigning or modifying target identifiers for surveillance and provisioning

Before you start this procedure, you need the following information:

- the network element ID of the network element for which you are assigning the TID
- the new TID name

Before you start this procedure, you must meet the following requirements:

- Have a user ID and password that access the OPC at the root or admin level.
- Read the command conventions for the CMT or graphical interface (see *User Interface Description*, 323-3001-301, in this volume).

Action

Step **Action**

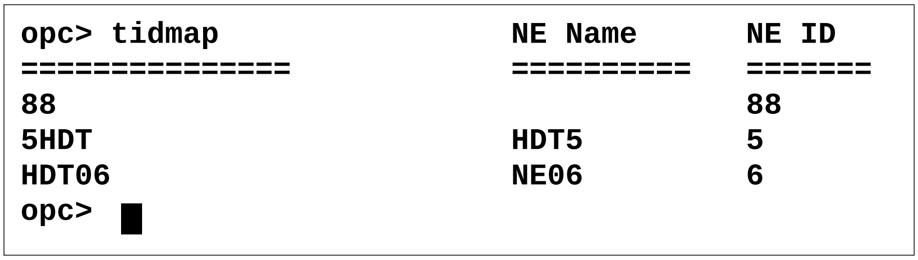
1 Log in to the OPC at the root or admin level.

If you are logging in as an admin user, you must open the UNIX shell tool (in the OPC Admin section) when the User Session Manager dialog appears.

2 To display the current network element ID, network element name, and TID for each network element in the OPC span of control, enter:

tidmap↵

A table similar to the following appears:



```
opc> tidmap                  NE Name      NE ID
===============              ==========   =======
88                                        88
5HDT                         HDT5         5
HDT06                        NE06         6
opc> █
```

Note: Entries appear under TID or NE Name only if the TID or network element name has been defined and you have run NMA or OPS.

—continued—

Procedure 13-10 (continued)
Assigning or modifying target identifiers for surveillance and provisioning

Step **Action**

3 To add or change a TID, enter:

tidmap -a <network element ID> <TID>↵

where

<network element ID>	current value of the network element ID
<TID>	new value for the TID

4 To verify the changes, enter:

tidmap↵

5 Exit the UNIX shell by entering:

exit↵

—end—

Managing an OPC activity switch

Usually within a span of control, the primary operations controller (OPC) is active and the backup OPC is inactive. However, if the primary OPC fails, the OPC system has a built-in feature called OPC WarmStandby (OWS) that keeps the backup OPC ready to become active if the primary OPC fails.

Included with the OWS feature is a tool that allows you to control the activity switching between the primary and backup OPC in a network. You use this tool to

- force the active OPC to inactive and the inactive OPC to active
- disable and enable the activity switch
- get information about the OPCs and whether they are able to switch

Forcing the backup OPC to active overrules revertive switching, but automatic switching caused by some communication failure still takes precedence.

An OPC returns to the state set by the OWS tool after a power shutdown.

Tool restrictions

Several conditions prevent the active OPC from becoming inactive and the inactive OPC from becoming active:

- no communication between OPCs
- OPCs are already in desired state
- network upgrade in progress
- requested operation is either impossible or illogical
- data synchronization is in progress

The forced state of an OPC is not preserved across an upgrade or install.

Chapter task list

The following tasks are included in this chapter:

Procedure		See
14-1	Switching the activity states of OPC pairs	page 14-3
14-2	Preventing an activity switch	page 14-7
14-3	Enabling an activity switch	page 14-8
14-4	Canceling an activity switch	page 14-9

If you cannot complete these procedures, contact your next level of support.

Procedure 14-1
Switching the activity states of OPC pairs

Use this procedure to switch the activity states of operations controller (OPC) pairs in a network. One OPC is active, usually the primary, and the other is inactive, usually the backup. You can also use this procedure to force the active OPC to become inactive and the inactive OPC active.

Requirements

Before starting this procedure, you must:

- have the root password that allows you access to the OPC
- read the command conventions described in *User Interfaces Description*, 323-3001-301, in this volume
- inform maintenance personnel about the OPC status being disturbed

Action

Step **Action**

1 Log in to the OPC using the root userID and open the UNIX shell tool.

2 At the login prompt, enter:

ows_swact↵

The user interface screen appears. The left side of this screen displays the current state of the primary and backup OPCs, indicates whether revertive switching is turned on, whether activity switching is enabled, and whether the backup OPC is locked in an inactive state. It also displays the state of the connections between the OPC, and if a data sync or network upgrade is in progress. The right side of the screen lists available command options.

Note 1: Command options can be entered as parameters of the ows_swact command. If you do not need to look at the settings on the user interface screen, you can enter the ows_swact followed by a space, hyphen, and a, i, p, or e. (Do not enter spaces between the hyphen and the option.) For example, to make the primary OPC active and the backup OPC inactive, enter:

ows_swact -a ↵

Note 2: To enable debug, verbose, or both, using the ows_swact command, enter d, v, or both before your selected option. Do not enter spaces between the hyphen and your selected options. For example, to enable debug and verbose and make the primary OPC inactive and the backup OPC active, enter:

ows_swact -dvi ↵

—continued—

Procedure 14-1 (continued)
Switching the activity states of OPC pairs

Step **Action**

When using the ows_swact command, entering d, v, or both after the a, i, p, or e options nulls the debug or verbose request. Therefore, always ensure the d or v options are entered before the a, i, p, or e options when using the ows_swact command.

The following options are available:

a Make the primary OPC active and the backup OPC inactive.

i Make the primary OPC inactive and the backup OPC active.

p Prevent users from switching activity by disabling force switch.

e Allow users to switch activity by enabling the force switch.

l Lock backup OPC inactive

r Release Inactive lock

c Cancel activity switch.

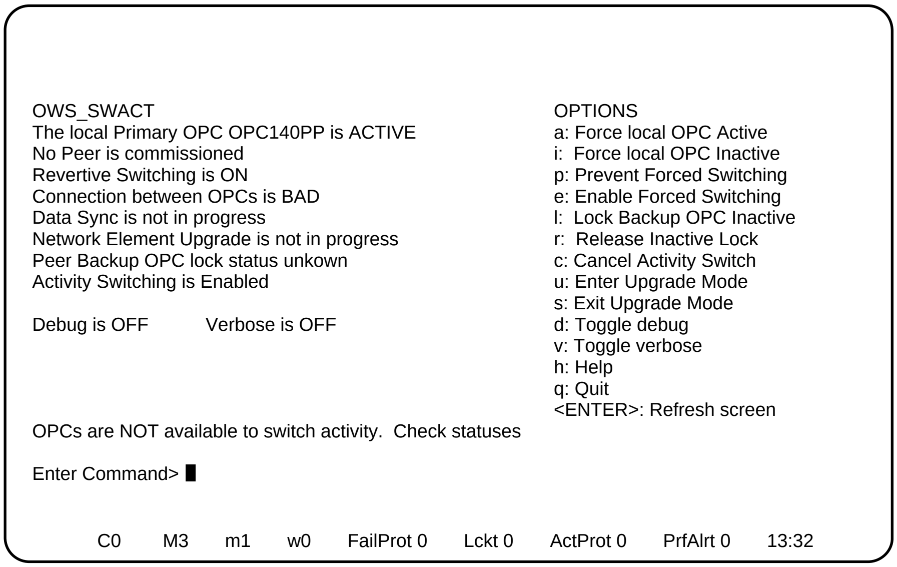
d Turn debug on.

v Show all messages.

h Display the help menu and terminate the program without forcing any activity switch.

q Quit

PC-21789



```
OWS_SWACT                                               OPTIONS
The local Primary OPC OPC140PP is ACTIVE                a: Force local OPC Active
No Peer is commissioned                                 i:  Force local OPC Inactive
Revertive Switching is ON                               p: Prevent Forced Switching
Connection between OPCs is BAD                          e: Enable Forced Switching
Data Sync is not in progress                            l:  Lock Backup OPC Inactive
Network Element Upgrade is not in progress              r:  Release Inactive Lock
Peer Backup OPC lock status unkown                      c: Cancel Activity Switch
Activity Switching is Enabled                           u: Enter Upgrade Mode
                                                        s: Exit Upgrade Mode
Debug is OFF          Verbose is OFF                    d: Toggle debug
                                                        v: Toggle verbose
                                                        h: Help
                                                        q: Quit
                                                        <ENTER>: Refresh screen
OPCs are NOT available to switch activity.  Check statuses

Enter Command> █


      C0     M3     m1     w0     FailProt 0     Lckt 0     ActProt 0     PrfAlrt 0     13:32
```

—continued—

Procedure 14-1 (continued)
Switching the activity states of OPC pairs

Step	Action

3 Make sure activity switching is enabled and that the backup OPC is not locked inactive.

If activity switching is disabled or the backup OPC is locked inactive, contact your next level of support to determine if you can change these options. If you can change these options, complete the appropriate steps listed in the following table:

If	Then
you need to enable activity switching	Enter: **e**↵ *A message appears asking you to confirm the command.* Enter: **y**↵ *Activity switching is enabled and the OPC login prompt appears.* Return to step 2.
the settings are correct	Determine the state of the local primary OPC. If it is active, go to step 4. If it is inactive, go to step 5.

4 Force the local primary OPC into an inactive state by entering:

i↵

A message appears asking you to confirm the command.

Enter:

y↵

The OPC status window appears for a moment. A screen appears stating that the OPC has just entered the inactive state.

Select the **Done** button.

The peer backup OPC is in an active state and the local primary OPC is in an inactive state. The OPC login prompt appears. You are finished with this procedure.

—continued—

Procedure 14-1 (continued)
Switching the activity states of OPC pairs

Step	Action
5	Force the local primary OPC into an active state by entering: **a**↵ *A message appears asking you to confirm the command.* Enter: ***y***↵ *The OPC status window appears for a moment. A screen appears stating that the OPC has just entered the active state.* Select the **Done** button. *The peer backup OPC is in an inactive state and the local primary OPC is in an active state. The OPC login prompt appears.*

—end—

Procedure 14-2
Preventing an activity switch

Use the following procedure to prevent an activity switch.

Requirements

Before starting this procedure, you must:

- have the root password that allows you access to the operations controller (OPC)
- read the command conventions described in *User Interfaces Description,* 323-3001-301, in this volume

Action

Step **Action**

1 Log in to the OPC using a root userID and open the UNIX shell tool.

2 At the login prompt, enter:

ows_swact -p ↵

The following prompt appears:

```
Are you sure you want to Prevent Force Activity Switching?
```

3 Confirm the prevent force activity switch by entering:

y ↵

The following message appears:

```
ows_swact command is successful.
```

The OPC login prompt appears. The status information on the user interface screen is also updated.

4 Display the user interface screen by entering:

ows_swact ↵

The user interface screen appears.

5 Verify that the command has taken effect (that is, the text “Activity Switching is Prevented” appears on the left side of the screen), then quit the user interface screen by entering:

q ↵

The user interface screen closes and the OPC login prompt appears.

—end—

Procedure 14-3
Enabling an activity switch

Use the following procedure to enable an activity switch.

Requirements

Before starting this procedure, you must:

- have the root password that allows you access to the operations controller (OPC)
- read the command conventions described in *User Interfaces Description,* 323-3001-301, in this volume

Action

Step **Action**

1 Log in to the OPC using a root userID and open the UNIX shell tool.

2 At the login prompt, enter:

ows_swact -e ↵

The following prompt appears:

```
Are you sure you want to Enable Force Activity Switching?
```

3 Confirm the enable force activity switch by entering:

y ↵

The following message appears:

```
ows_swact command is successful.
```

The OPC login prompt appears. The status information on the user interface screen is also updated.

4 Display the user interface screen by entering:

ows_swact ↵

The user interface screen appears.

5 Verify that the command has taken effect (that is, the text “Activity Switching is Enabled” appears on the left side of the screen), then quit the user interface screen by entering:

q ↵

The user interface screen closes and the OPC login prompt appears.

—end—

Procedure 14-4
Canceling an activity switch

Use the following procedure to cancel an activity switch and return the primary and backup operations controllers (OPCs) to their normal states.

> ***Note:*** This command could cause a Network split if the OPC activities have been switched and the peer does not receive this message.

Requirements

Before starting this procedure, you must:

- have the root password that allows you access to the OPC
- read the command conventions described in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step **Action**

1 Log in to the OPC using a root userID and open the UNIX shell tool.

2 At the login prompt, enter:

ows_swact -c ↵

The following message and prompt appears:

```
Cancelling Force Activity Switch causes the OPCs to revert
to normal state. Are you sure?
```

3 Confirm the cancel switch activity by entering:

y ↵

The following message appears:

```
ows_swact command is successful.
```

The OPC login prompt appears. The status information on the user interface screen is also updated.

If the “cancel” operation initiated a state change on the OPC, then a screen appears stating that the OPC (where you are logged in) has entered the active or inactive state, as applicable.

Press the **Done** button to remove this information screen.

4 Display the user interface screen by entering:

ows_swact ↵

The user interface screen appears.

—continued—

Procedure 14-4 (continued)
Canceling an activity switch

Step	**Action**
5	Verify that the command has taken effect (that is, the text “The local Primary OPC <OPC name> is <state>” and “The peer Backup OPC<OPC name> is <state>” appears on the left side of the screen). Verify that proper normal activity has also resumed (that is, if no association problems exist, normal operation is Primary ACTIVE, Backup INACTIVE). Quit the user interface screen by entering: **q** ↵ *The user interface screen closes and the OPC login prompt appears.*

—end—

Provisioning TBOS serial telemetry ports

The telemetry byte-oriented serial (TBOS) Mapping tool is in the Network Admin toolset. This tool allows you to centralize serial telemetry information and reduce the amount of equipment needed to transmit this information to remote alarm-monitoring equipment.

All network elements (NE) in an operations controller (OPC) span of control collect alarms and status conditions. Each NE assigns local alarms and status conditions to its local RS-422 serial output port. However, you can reconfigure these output ports so they also report alarms and status conditions for other NEs in the OPC span of control. These alarms and status conditions can represent either an individual remote NE or all NEs. The TBOS Mapping tool allows you to reassign remote or cluster-wide serial telemetry information to a specified NE. All telemetry information (local, remote, and cluster-wide) is then transmitted from the specified NE to remote E2A alarm-monitoring equipment.

Each AccessNode contains two RS-422 serial output ports. In this document, RS-422 serial output ports that are configured with TBOS alarm management software are referred to as active TBOS ports. For more information on TBOS ports, see *Alarms and Surveillance Description*, 323-3001-104, in *Description*, Volume 2A.

Serial telemetry is usually assigned to TBOS ports when the system is first commissioned, but it can also be reassigned at a later date, as necessary.

For further information on the TBOS Mapping tool, see the description in *OPC User Interface Description*, 323-3001-301, in this volume.

TBOS displays

Alarms and status conditions are organized into sets of serial telemetry data called displays. Displays have 64 bits, where each bit has a value of 1 or 0 indicating either

- an alarm is raised or not
- the state of an alarm condition (on or off)

In a display, a state change indicates that an alarm or status condition has occurred in an NE. If a second alarm of the same type occurs before the first is cleared, the display does not change, since it already indicates the existence of that alarm.

> ***Note:*** Individual bits in the display can be suppressed (that is, alarms can be disabled) at the network element user interface (NEUI). Therefore, when a specified alarm or status condition occurs, it does not appear in the display.

All displays are transmitted using the TBOS protocol. The meaning of each alarm and its position in the display is predefined and cannot be changed.

The TBOS Mapping tool shows all display assignments for a port, whether assigned by the NE or the TBOS Mapping tool. The TBOS Mapping tool shows the following types of displays: control, cluster, monitor, and unknown.

Control displays

Control displays carry commands from the remote alarm-monitoring equipment to an NE. The access bandwidth manager (ABM) and transport bandwidth manager (TBM) shelves receive two types of control displays: control 1 and control 2. You cannot use the TBOS Mapping tool to assign control displays.

Cluster display

The cluster display summarizes changes in alarms and status conditions for all NEs in the OPC span of control. This display is created at the OPC by E2A Alarm Manager software. You can use the TBOS Mapping tool to assign the cluster display.

Monitor displays

Monitor displays carry alarms and status conditions for an individual NE. Monitor displays can be either local or remote. Local displays represent the local NE. They are assigned using the local NEUI.

Remote displays represent a remote NE in the OPC span of control. An NE with active TBOS ports receives displays from remote NEs without active TBOS ports. These remote displays are stored in a series of OPC-reserved displays, referred to as Remote 1 through Remote 32. Remote displays are assigned to a position in the active TBOS port from the OPC, using the TBOS Mapping tool.

Table 15-1 lists the monitor displays that can be assigned, depending on the monitored source.

Table 15-1
Monitor displays for ABM and TBM

Monitor display	ABM shelf fiber central office terminal and remote fiber terminal	TBM shelf fiber central office terminal
Monitor 1	Network element alarms and status conditions	Network element alarms and status conditions
Monitor 2	Telemetry overview	Telemetry overview
Monitor 3	Equipment	Equipment
Monitor 4	Facility	DS-1 Facilities
Monitor 5	Protection	OC-n/DS1 protection
Monitor 6	Parallel-telemetry scan points and signal distribution points	OC-n/DS3 protection/facilities
Monitor 7	Modules in the copper-distribution drawers	Parallel-telemetry scan points and signal distribution points
Monitor 8	Maintenance	Reserved for future use
Monitor 9	Not applicable	Reserved for future use
Monitor 10	Not applicable	Maintenance

Unknown displays

An “Unknown” display indicates inconsistencies between the OPC database and NE databases. For example, unknown displays can be displayed after a database is restored from tape, or if the backup OPC has an out-of-date database when it becomes active.

Tool requirements and restrictions

Before you can use the TBOS Mapping tool to assign a display to a TBOS port, you must provision the port on an NE.

A “?” appearing to the left of an NE list item indicates a loss of communication from the OPC to an NE. Therefore, you cannot perform the procedures in this document.

You can assign only monitor displays or the cluster display using the TBOS Mapping tool. The control display must be assigned at the NEUI.

Alarms and status conditions in a display are predefined and cannot be changed. For a full description of the alarms and status conditions in each monitor display, see *Alarms and Surveillance Description*, 323-3001-104, in *Description,* Volume 2A.

You can only assign a display once to an individual TBOS port.

The TBOS Mapping tool does not allow you to view incoming alarms. Use the Network Alarm Status tool to view incoming alarms. See *Network Surveillance Procedures*, 323-3001-510, in *Maintenance,* Volume 5C.

If your system has a backup OPC, you do not assign displays while the backup OPC is active. Displays assigned while the backup OPC is active do not appear in the main window of the tool when the primary OPC becomes active again. Instead, the tool identifies these new assignments as “Unknown”. Use the TBOS Mapping tool to either reassign the display (if you know the previous assignment) or to delete the display.

Chapter task list

This chapter includes the following tasks:

Procedure		**See**
15-1	Viewing a display assignment	page 15-5
15-2	Assigning a display to a TBOS port	page 15-6
15-3	Deleting a display from a TBOS port	page 15-9
15-4	Assigning a remote alarm	page 15-11

If you cannot complete these procedures, contact your next level of support.

Procedure 15-1
Viewing a display assignment

Use this procedure to see which serial telemetry displays are assigned to a TBOS port and slot (position).

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the operations controller (OPC)
- read the command conventions for the interface you are using (CMT or graphical) in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step **Action**

1 Log in to the OPC and select the TBOS Mapping tool from the Network Admin toolset.

The TBOS Mapping tool main window appears.

2 In the TBOS Ports list, move to the network element (NE) with the port ID that you want, then press **Ctrl_A** (or Keypad **0**). If no NEs are displayed, no TBOS ports are assigned.

The list item is highlighted.

3 Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).

The list item menu appears.

4 Select the Detail command by pressing **Space** (or Keypad **0**).

The display assignments for that item appear in the Port Details list. The list shows the position in the port and any display that is assigned to a position.

5 To close the tool:

a. Display the window menu by pressing **Ctrl_L W** (or Keypad **6**).

The window menu appears.

b. Select the Exit command by pressing **Space** (or Keypad **0**).

The tool closes.

—end—

Procedure 15-2
Assigning a display to a TBOS port

Use this procedure to assign a serial telemetry display to a slot (position) in a TBOS port. You can assign a display to any network element (NE) that is within the current operations controller (OPC) span of control and has active TBOS ports.

> ***Note:*** A display can be assigned only once to an individual TBOS port. When a display has been assigned to a port, the display is dimmed in the chooser menu and cannot be selected again for the same port.

The TBOS Mapping tool allows you to assign two types of displays:

- cluster: the summary of alarms and status conditions for all NEs in the OPC span of control
- monitor: alarms and status conditions from an individual NE. Table 15-1 on page 15-3 lists the monitor displays that can be assigned, depending on the monitored source.

For a full description of the alarms and status conditions in each monitor display, see *Alarms and Surveillance Description*, 323-3001-104, in *Description*, Volume 2A.

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the OPC
- read the command conventions for the interface you are using (CMT or graphical) in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC and select the TBOS Mapping tool from the Network Admin toolset. *The TBOS Mapping tool main window appears.*
2	In the TBOS Ports list, move to the NE with the port ID that you want, then press **Ctrl_A** (or Keypad **0**). If no NEs are displayed, no TBOS ports are assigned. *The list item is highlighted.*

—continued—

Procedure 15-2 (continued)
Assigning a display to a TBOS port

Step	**Action**
3	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**). *The list item menu appears.*
4	Select the Detail command by pressing **Space** (or Keypad **0**). *The display assignments for that item appear in the Port Details list. The list shows the position in the port and any display that is assigned to a position.*
5	Tab to the Port Details list.
6	Move to the position you want to change, then press **Ctrl_A** (or Keypad **0**).
7	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**). *The list item menu appears.*
8	Select the Reassign Display command by pressing **Space** (or Keypad **0**). *The Mapping of Displays to TBOS Ports dialog appears. The NE, Type, Port ID, and Position fields are filled in.*
9	To change the position number, enter the new position number in the Position field.
10	Tab to the Mon. Source field and display the chooser menu by pressing **Ctrl_L /** (or Keypad **3**). *The chooser menu appears.*

If you want to assign	**Then**
the cluster display	Move to Span of Control, then press **Space** (or Keypad **0**). *The Display field is automatically filled in.* Go to step 13.
a network element display	Move to an NE, then press **Space** (or Keypad 0). *The Type and Display fields are automatically filled in.* Go to step 11.

11 Tab to the OK button, then press **Ctrl_A** (or Keypad **0**).

If	**Then**
A display is assigned to the position	Go to step 12.
No display is assigned to the position	After the display is assigned, the Mapping of Displays to TBOS Ports dialog closes. Go to step 14.

—continued—

Procedure 15-2 (continued)
Assigning a display to a TBOS port

Step	Action
12	A confirmation dialog appears, indicating that the existing display assignment will be overwritten.
13	In the confirmation dialog, tab to the OK button, then press **Ctrl_A** (or Keypad **0**). *The confirmation dialog closes. After the existing display assignment is overwritten with the new assignment, the Mapping of Displays to TBOS Ports dialog also closes.*
14	To close the tool: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 15-3
Deleting a display from a TBOS port

Use this procedure to delete a serial telemetry display from a slot (position) and TBOS port on a network element (NE).

Requirements

Before starting this procedure, you must:

- have a userID and password that permit access to the operations controller (OPC)
- read the command conventions for the interface you are using (CMT or graphical) in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step	Action
1	Log in to the OPC and select the TBOS Mapping tool from the Network Admin toolset. *The TBOS Mapping tool main window appears.*
2	In the TBOS Ports list, move to the NE with the port ID that you want, then press **Ctrl_A** (or Keypad **0**). *The list item is highlighted.*
3	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**). *The list item menu appears.*
4	Select the Detail command by pressing **Space** (or Keypad **0**). The display assignments for that item appear in the Port Details list. *The list shows the positions in the port and any display that is assigned to a position.*
5	Tab to the Port Details list.
6	Move to the position you want to change, then press **Ctrl_A** (or Keypad **0**).
7	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**). *The list item menu appears.*
8	Move to the Delete command, then press **Space** (or Keypad **0**). *A confirmation dialog appears, prompting you to confirm your request.*
9	Tab to the OK button, then press **Ctrl_A** (or Keypad **0**). *The confirmation dialog closes and the display assignment is deleted. In the Port Details list, a row of dashes appears to the right of the position number.*

—continued—

Procedure 15-3 (continued)
Deleting a display from a TBOS port

Step	Action
10	To close the tool: **a.** Display the window menu by pressing **Ctrl_L W** (or Keypad **6**). *The window menu appears.* **b.** Select the Exit command by pressing **Space** (or Keypad **0**). *The tool closes.*

—end—

Procedure 15-4
Assigning a remote alarm

Use this procedure to assign remote alarms. The operations controller (OPC) and network element (NE) must match port and display assignments before you assign an output point to report the remote alarm.

Requirements

Before starting this procedure,:

- have a userID and password that permit access to the OPC
- read the command conventions for the interface you are using (CMT or graphical) in *User Interfaces Description*, 323-3001-301, in this volume

Action

Step	**Action**
1	Log in to the OPC and select the NE Login Manager tool from the Utilities Admin toolset.
	The NE Login Manager tool main window appears.
2	Select the NE that will be used to report remote alarms.
3	Tab to the Auto login button, then press **Ctrl_A** (or Keypad **0**).
	The Network Element Status screen appears.
4	Verify if at least one serial port has been provisioned. To verify, access the system administration screen and display the user profile parameters by entering:
	admin ip ↵
	The system administration screen with the user profile parameters appears.
5	If any port does not exist, create it by entering:
	add <port #>↵
	where
	<port #> is **3** or **4**

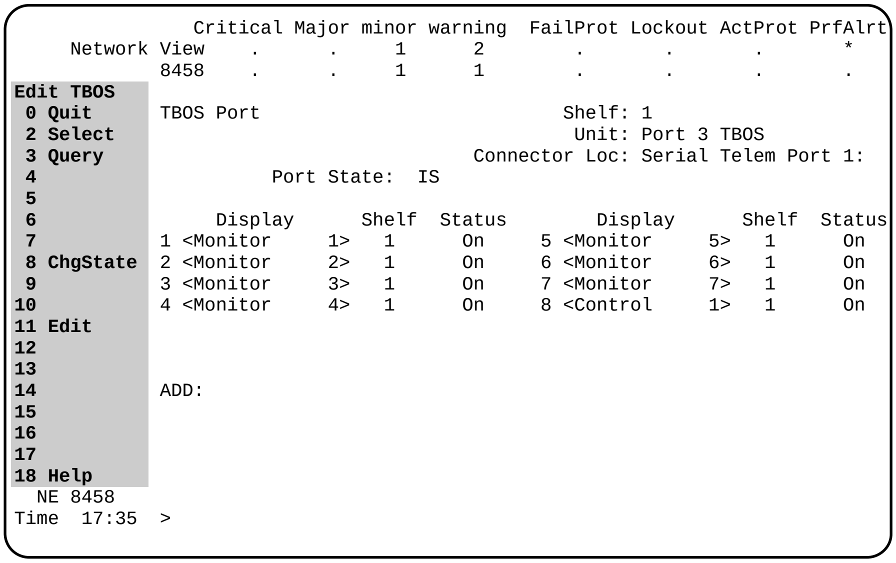
—continued—

Procedure 15-4 (continued)
Assigning a remote alarm

Step **Action**

The displays (as shown in the following screen) are assigned.

PC-22297



```
                Critical Major minor warning  FailProt Lockout ActProt PrfAlrt
     Network View    .      .     1      2        .       .       .       *
             8458    .      .     1      1        .       .       .       .
Edit TBOS
 0 Quit      TBOS Port                           Shelf: 1
 2 Select                                         Unit: Port 3 TBOS
 3 Query                                 Connector Loc: Serial Telem Port 1:
 4                     Port State:  IS
 5
 6               Display      Shelf  Status        Display      Shelf  Status
 7           1 <Monitor     1>   1      On     5 <Monitor     5>   1      On
 8 ChgState  2 <Monitor     2>   1      On     6 <Monitor     6>   1      On
 9           3 <Monitor     3>   1      On     7 <Monitor     7>   1      On
10           4 <Monitor     4>   1      On     8 <Control     1>   1      On
11 Edit
12
13
14           ADD:
15
16
17
18 Help
  NE 8458
Time  17:35  >
```

6 Keeping the NE login session open, move to the OPC user session manager by entering **Ctrl_T 0**.

7 Select the TBOS Mapping tool.

If you do not know how to do this, see *User Interfaces Description*, 323-3001-301, in this volume.

The TBOS Mapping tool main window appears.

8 Obtain the details of the port as follows:

a. Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).

The list item menu appears.

b. Select the Detail command by pressing **Space** (or Keypad **0**).

The display assignments for that item appear in the Port Details list. The list shows the positions in the port and any display that is assigned to a position.

—continued—

Procedure 15-4 (continued)
Assigning a remote alarm

Step **Action**

9 Reassign one of the 8 positions as follows:

a. Move using the arrow keys to the position you want to reassign.

b. Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**).

The list item menu appears.

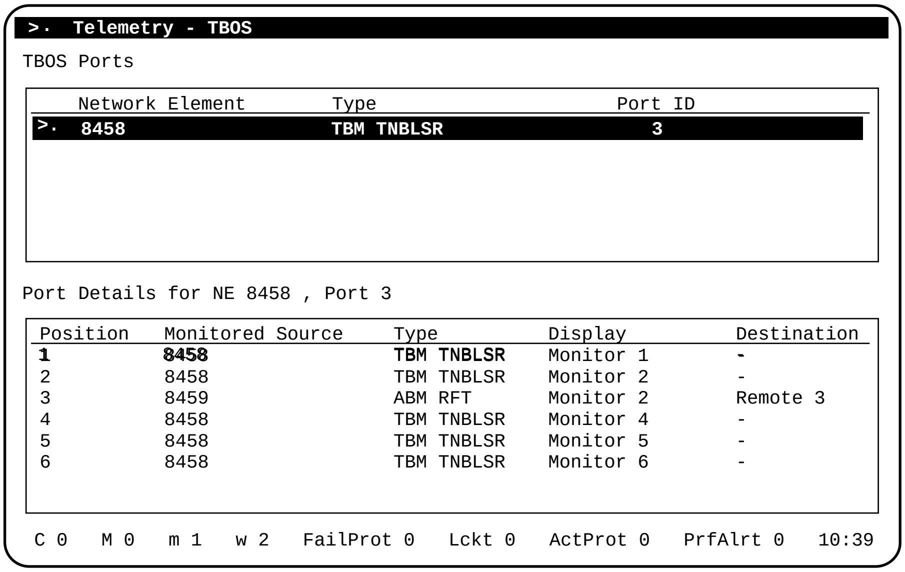
c. Move to the Reassign Display command, then press **Ctrl_A** (or Keypad **0**).

The Mapping of Displays to TBOS Ports dialog appears. The NE, Type, Port ID, and Position fields are filled in.

10 After you select the desired remote NE, the type and display fields are automatically filled in.

11 Write down the destination name assigned to the position, as displayed in the main window.

PC-22300



```
>.  Telemetry - TBOS
TBOS Ports

    Network Element        Type                        Port ID
>.  8458                   TBM TNBLSR                     3

Port Details for NE 8458 , Port 3

 Position   Monitored Source     Type          Display          Destination
 1          8458                 TBM TNBLSR    Monitor 1        -
 2          8458                 TBM TNBLSR    Monitor 2        -
 3          8459                 ABM RFT       Monitor 2        Remote 3
 4          8458                 TBM TNBLSR    Monitor 4        -
 5          8458                 TBM TNBLSR    Monitor 5        -
 6          8458                 TBM TNBLSR    Monitor 6        -

 C 0   M 0   m 1   w 2   FailProt 0   Lckt 0   ActProt 0   PrfAlrt 0   10:39
```

12 Verify that the information displayed at the NE matches the information at the OPC.

—end—

Index

SONET Products

AccessNode

System Administration Procedures

All information contained in this document is subject to change without notice. Nortel Networks reserves the right to make changes to equipment design or program components, as progress in engineering, manufacturing methods, or other circumstances may warrant.

Publication number: 323-3001-302
Document release: Issue 4.0
Date: October 1999
Printed in Canada

NORTEL NETWORKS™