NTN465GF **323-1059-302**

Nortel Networks

OPTera Metro 3500 Multiservice Platform

Security and Administration

Standard Release 12.0 Issue 1 November 2003

What's inside...

Printed in Canada

Contents

List of procedures

User account management and administration 3-1

List of procedures

Manual connection terminal, telnet terminal and communications log 4-1

List of procedures

Shelf graphics and inventory 5-1

List of procedures

Provisioning data and software management procedures 6-1

List of procedures

List of procedures

List of procedures

About this document

This document describes how to

- log in to a network element or network processor
- manage login profiles
- manage user accounts
- use the manual connection terminal, telnet terminal, and communications log
- view shelf graphics and inventory
- save and restore provisioning data
- manage software on a network element or network processor
- use the TL1 Command Builder
- provision time of day
- use the login banner and general broadcast tool

Supported software

This document supports the software releases for Nortel Networks OPTera Metro 3500 Multiservice Platform Release 12.0.

Supported hardware

This document supports the OPTera Metro 3500 shelf and Universal OPTera Metro 3500 shelf.

Hardware naming conventions

The following naming conventions are used throughout this document to identify the OPTera Metro 3500 hardware:

- The extended shelf processor (SPx) is referred to as the shelf processor.
- The extended network processor (NPx) is referred to as the network processor.

Audience

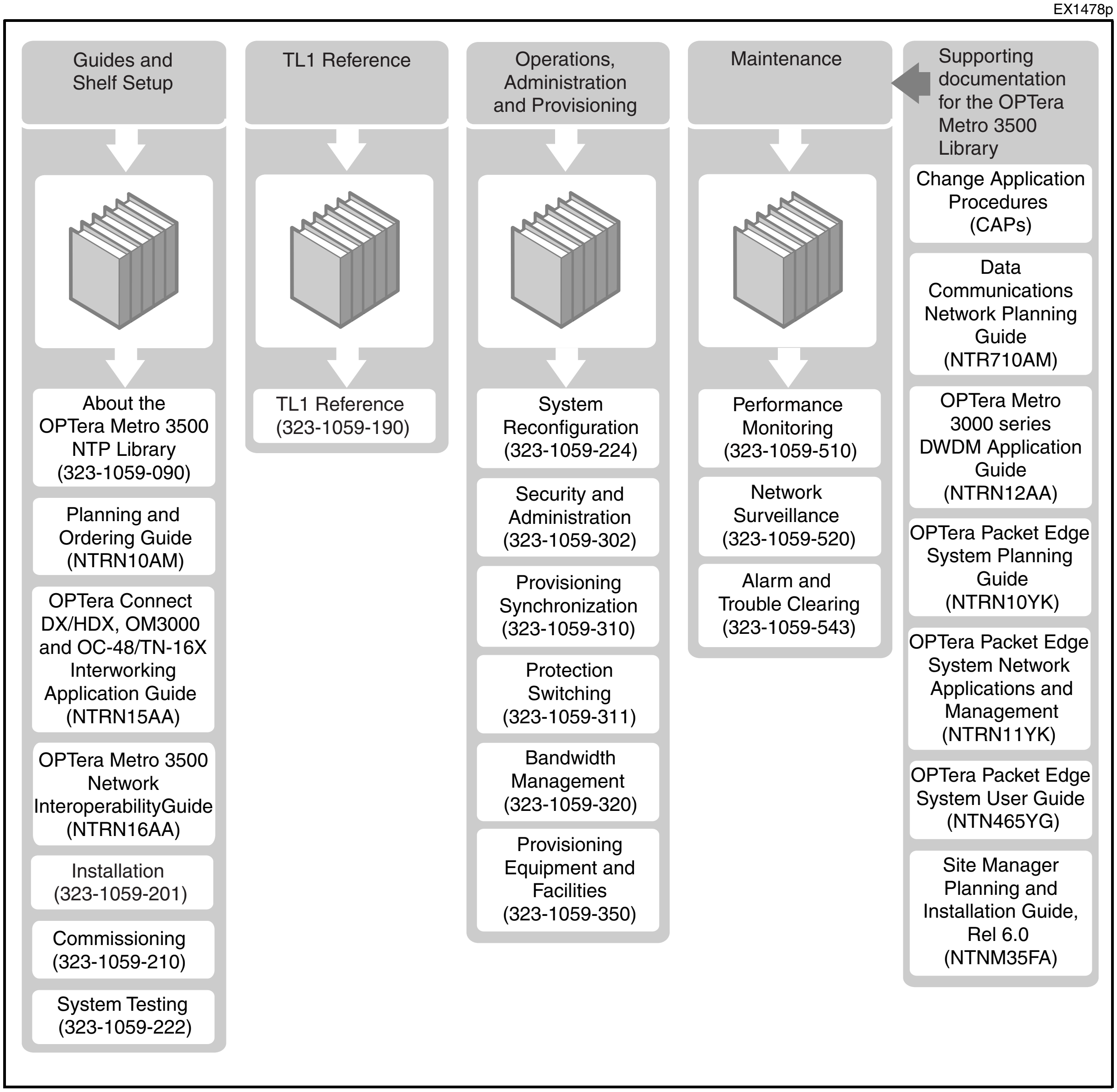
The following members of your company are the intended audience of this Nortel Networks technical publication (NTP):

- planners
- provisioners
- network administrators
- transmission standards engineers

Standards

The Telecommunications Industry Association (TIA) and the Electronics Industries Alliance (EIA) accepted RS-232 as a standard in 1997 and renumbered this standard as TIA/EIA-232. In this document, RS-232 is used to reflect current labels on the hardware and in the software for the OPTera Metro 3500 Multiservice Platform.

OPTera Metro 3500 NTP library



Guides and Shelf Setup

- About the OPTera Metro 3500 NTP Library (323-1059-090)
- Planning and Ordering Guide (NTRN10AM)
- OPTera Connect DX/HDX, OM3000 and OC-48/TN-16X Interworking Application Guide (NTRN15AA)
- OPTera Metro 3500 Network InteroperabilityGuide (NTRN16AA)
- Installation (323-1059-201)
- Commissioning (323-1059-210)
- System Testing (323-1059-222)

TL1 Reference

- TL1 Reference (323-1059-190)

Operations, Administration and Provisioning

- System Reconfiguration (323-1059-224)
- Security and Administration (323-1059-302)
- Provisioning Synchronization (323-1059-310)
- Protection Switching (323-1059-311)
- Bandwidth Management (323-1059-320)
- Provisioning Equipment and Facilities (323-1059-350)

Maintenance

- Performance Monitoring (323-1059-510)
- Network Surveillance (323-1059-520)
- Alarm and Trouble Clearing (323-1059-543)

Supporting documentation for the OPTera Metro 3500 Library

- Change Application Procedures (CAPs)
- Data Communications Network Planning Guide (NTR710AM)
- OPTera Metro 3000 series DWDM Application Guide (NTRN12AA)
- OPTera Packet Edge System Planning Guide (NTRN10YK)
- OPTera Packet Edge System Network Applications and Management (NTRN11YK)
- OPTera Packet Edge System User Guide (NTN465YG)
- Site Manager Planning and Installation Guide, Rel 6.0 (NTNM35FA)

Technical support and information

For technical support and information from Nortel Networks, refer to the following table.

Technical Assistance Service	
For service-affecting problems: For 24-hour emergency recovery or software upgrade support, that is, for: • restoration of service for equipment that has been carrying traffic and is out of service • issues that prevent traffic protection switching • issues that prevent completion of software upgrades	**North America:** 1-800-4NORTEL (1-800-466-7835) **International:** 001-919-992-8300
For non-service-affecting problems: For 24-hour support on issues requiring immediate support or for 14-hour support (8 a.m. to 10 p.m. EST) on upgrade notification and non-urgent issues.	**North America:** 1-800-4NORTEL (1-800-466-7835) ***Note:*** You require an express routing code (ERC). To determine the ERC, see our corporate Web site at www.nortelnetworks.com. Click on the Express Routing Codes link. **International:** Varies according to country. For a list of telephone numbers, see our corporate Web site at www.nortelnetworks.com. Click on the Contact Us link.
Global software upgrade support:	**North America:** 1-800-4NORTEL (1-800-466-7835) **International:** Varies according to country. For a list of telephone numbers, see our corporate Web site at www.nortelnetworks.com. Click on the Contact Us link.

Introduction to Site Manager

Site Manager is a graphical user interface (GUI) used to operate, administer, maintain, and provision optical networks. Use Site Manager to perform the following operations for optical network elements:

- monitor alarms and alarm history
- retrieve a historical listing of performance statistics for specific network elements
- provision performance thresholds according to your performance management parameters
- provision equipment and facilities
- control the protection status of network elements
- provision nodal and end-to-end connections within a span of control
- visualize remote equipment by using shelf level graphics

Note 1: If Site Manager does not support the product release or if the shelf processor is not running the same load as the rest of the network element, only the following applications are available: Active Alarms, Events, Backup and Restore, Upgrade Management, and Load Installation Management.

Note 2: If the connection to a network element is lost after you log in to the network element through Site Manager, Site Manager will not detect the loss of connection until a new command, such as a refresh, is sent to the network element.

Interface login and logout

Procedures for interface login and logout

Procedures for logging in to a network processor

Procedures for logging in to a network element

Other login and logout related procedures

Procedure 2-1
Starting Site Manager

Use this procedure to start a Site Manager session on a PC.

> ***Note:*** For information about starting Site Manager from a Nortel Networks Preside workstation, refer to the *Preside Interface Login User Guide*, 450-3101-012, or the Preside online information.

Step	**Action**
1	Click the Start button on the Task bar and select Programs, PresideSiteManager, PresideSiteManager.

—end—

Procedure 2-2
Logging in to a network processor using a network connection

Requirements

To perform this procedure, you must

- have the user identifier of the account
- have a valid account password

Step **Action**

1 Start Site Manager to open the Login dialog box. See Starting Site Manager on page 2-3.

Note 1: You can connect to only one network processor span of control at a time.

Note 2: If you have already logged in to a network processor and want to log in to another network processor, select Login from the File drop-down menu to open the Login dialog box.

Note 3: The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. If this is the case, select Login from the File drop-down menu in the main window to open the Login dialog box. For more information, see Setting the login preferences on page 2-36.

2 In the Connect Using area, select the Site Manager radio button.

Note: To log in using a terminal session, see Starting a terminal session using the network on page 4-2.

3 Select Network from the Connection Type drop-down list in the Connection Information area.

4 Select an equipment type from the Gateway Node Type drop-down list.

5 Select or enter an IP address in the Host Name/Address field.

6 Enter a port number in the Port box.

Note: The default port number is

— 10001 for OPTera Metro 3000/OC-48Lite

— 14001 for OPC

7 Select a value (in seconds) from the Timeout drop-down list.

If a manual connection is required, select the check box labelled Requires Manual Connection/Secure Modem at Gateway Node.

—continued—

Procedure 2-2 (continued)
Logging in to a network processor using a network connection

Step	Action
8	In the Login NE Information area, enter a network processor ID or select a network processor ID from the Login NE drop-down list. ***Note:*** You can click Find to display the Find Node dialog box, which contains node information on previous connections to network elements. The Find button is available only after you have logged in to a network element in the current user session. When you select an entry in the Find Node dialog box and click OK, the Login dialog box displays the associated Login NE and NE Type in the Login NE Information area.
9	Select a network element type from the NE Type drop-down list in the Login NE Information area. ***Note 1:*** You can log in to a maximum of 16 shelf processors at the same time. ***Note 2:*** Starting with Release 12, up to three Level 5 users can log into and have access to the same network processor at the same time if the user identifiers are different. Each of these Level 5 users can access and manage all 16 network elements within the span of control of this network processor.
10	To log in to the network processor using challenge-response authentication, select the Use Challenge/Response check box.
11	Enter an ID in the User ID field in the Login NE Information area. Then,

If	
you are using challenge-response authentication	go to step 16
otherwise	go to the next step

Step	Action
12	Enter a password in the Password field in the Login NE Information area.
13	If you want to save the current login settings as a new login profile, click Save As, enter a login profile name in the Profile Name field, and click OK.
14	Click Connect to log in to the network processor and start Site Manager. ***Note:*** The Node Information window for the network processor appears or the Manual Connection dialog box appears if in step 7 you selected the check box labelled Requires Manual Connection/Secure Modem at Gateway Node.
15	You have completed this procedure.

—continued—

Procedure 2-2 (continued)
Logging in to a network processor using a network connection

Step Action

Using challenge-response authentication

16 Click Connect to open the Challenge/Response Login dialog box. The User ID field displays the user identifier entered in the Login dialog box. The Challenge field displays the challenge retrieved from the network processor for this login session.

17 Do one of the following to enter the response for this login session:

- Request the response from your network operations center or approved administrator and enter it in the Response field.
- Click Show response generator, then
  - — select the required user privilege code for this login session from the Privilege Code drop-down list
  - — enter the shared secret for the network processor in the Shared Secret field
  - — click the Generate Response button to generate the response for this login session, based on the user identifier, privilege code, and shared secret

Note: The shared secret does not appear on screen. The default shared secret is nortelnetworks.

18 Click OK to log in to the network processor.

—end—

Procedure 2-3
Logging in to a network processor using a modem connection

Requirements

To perform this procedure, you must

- have the user identifier of the account
- have the account password

Step	Action
1	Start Site Manager to open the Login dialog box. See Starting Site Manager on page 2-3. ***Note 1:*** You can connect to only one network processor span of control at a time. ***Note 2:*** If you have already logged in to a network processor and want to log in to another network processor, select Login from the File drop-down menu to open the Login dialog box. ***Note 3:*** The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. If this is the case, select Login from the File drop-down menu in the main window to open the Login dialog box. For more information, see Setting the login preferences on page 2-36.
2	In the Connect Using area, select the Site Manager radio button. ***Note:*** To log in using a terminal session, see Starting a terminal session using a modem on page 4-3.
3	Select Modem from the Connection Type drop-down list.
4	Select an equipment type from the Gateway Node Type drop-down list.
5	Select or enter a telephone number in the Telephone Number drop-down list.
6	Select a value (in seconds) from the Timeout drop-down list.
7	If you want to define the modem settings, click the Advanced button. See Defining modem settings on page 2-14 for further instructions.
8	If a manual connection is required, select the check box labelled Requires Manual Connection/Secure Modem at Gateway Node.

—continued—

Procedure 2-3 (continued)
Logging in to a network processor using a modem connection

Step	**Action**
9	In the Login NE Information area, enter a network processor ID or select a network processor ID from the Login NE drop-down list.You can click Find to display the Find Node dialog box, which contains node information on previous connections to network elements. The Find button is available only after you have logged in to a network element in the current user session. When you select an entry in the Find Node dialog box and click OK, the Login dialog box displays the associated Login NE and NE Type in the Login NE Information area.
10	Select a network element type from the NE Type drop-down list in the Login NE Information area. ***Note 1:*** You can log in to a maximum of 16 shelf processors at the same time. ***Note 2:*** Starting with Release 12, up to three Level 5 users can log into and have access to the same network processor at the same time if the user identifiers are different. Each of these Level 5 users can access and manage all 16 network elements within the span of control of this network processor.
11	To log in to the network processor using challenge-response authentication, select the Use Challenge/Response check box.
12	Enter an ID in the User ID field in the Login NE Information area. Then,

If	
you are using challenge-response authentication	go to step 17
otherwise	go to the next step

13	Enter a password in the Password field in the Login NE Information area.
14	If you want to save the current login settings as a new login profile, click Save As, type a login profile name in the Profile Name field, and click OK.
15	Click Connect to log in to the network processor and start Site Manager. ***Note:*** The Node Information window for the network processor appears or the Manual Connection dialog box appears if in step 8 you have selected the check box labelled Requires Manual Connection/Secure Modem at Gateway Node.
16	You have completed this procedure.

—continued—

Procedure 2-3 (continued)

Logging in to a network processor using a modem connection

Step **Action**

Using challenge-response authentication

17 Click Connect to open the Challenge/Response Login dialog box. The User ID field displays the user identifier entered in the Login dialog box. The Challenge field displays the challenge retrieved from the network processor for this login session.

18 Do one of the following to enter the response for this login session:

- Request the response from your network operations center or approved administrator and enter it in the Response field.
- Click Show response generator, then
  - — select the required user privilege code for this login session from the Privilege Code drop-down list
  - — enter the shared secret for the network processor in the Shared Secret field
  - — click the Generate Response button to generate the response for this login session, based on the user identifier, privilege code, and shared secret

Note: The shared secret does not appear on screen. The default shared secret is nortelnetworks.

19 Click OK to log in to the network processor.

—end—

Procedure 2-4
Logging in to a network processor and configuring an X25 connection

Requirements

To perform this procedure, you must

- have the user identifier of the account
- have the account password

Step	Action
1	Log in to the network processor. See Logging in to a network processor using a network connection on page 2-4.
2	Select the network processor target identifier.
3	From the Configuration drop-down menu, select NP facility.
4	Select X25 from the list and click-on Add. ***Note:*** By performing step 4, you provision by default the X25 facility on the network processor as in-service.
5	Log out of the network processor. See Logging out of a network processor or a network element on page 2-40. ***Note:*** Do not disconnect from the gateway node. Select No.
6	From the File drop-down menu, select Login, and click-on the Terminal Session radio button. Select any port from 10002 to 10020. See Logging in to a network processor using a network connection on page 2-4.
7	Enter a valid X25 port number in the format of 0156 70X0X. The actual X25 port number is determined by the physical setup.
8	A banner for a TL1 session will appear.

—end—

Procedure 2-5
Logging in to a network processor using a direct cable connection

Requirements

To perform this procedure, you must

- have the user identifier of the account
- have the account password

Step	Action
1	Ensure you are logged in to the shelf processor using a direct cable connection. See Logging in to a network element using a direct cable connection on page 2-32.
2	Start Site Manager to open the Login dialog box. See Starting Site Manager on page 2-3. ***Note 1:*** You can connect to only one network processor span of control at a time. ***Note 2:*** If you have already logged in to a network processor and want to log in to another network processor, select Login from the File drop-down menu to open the Login dialog box. ***Note 3:*** The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. If this is the case, select Login from the File drop-down menu in the main window to open the Login dialog box. For more information, see Setting the login preferences on page 2-36.
3	In the Connect Using area, select the Site Manager radio button. ***Note:*** To log in using a terminal session, see Starting a terminal session using direct cable on page 4-4.
4	Select Direct Cable from the Connection Type drop-down list in the Connection Information area.
5	Select an equipment type from the Gateway Node Type drop-down list.
6	Select a port from the Port drop-down list.
7	Select a value (in seconds) from the Timeout drop-down list.
8	If you want to define the direct cable settings, click the Advanced button. See Defining direct cable settings on page 2-15 for further instructions.
9	If a manual connection is required, select the check box labelled Requires Manual Connection/Secure Modem at Gateway Node.

—continued—

Procedure 2-5 (continued)
Logging in to a network processor using a direct cable connection

Step	Action
10	In the Login NE Information area, enter a network processor ID or select a network processor ID from the Login NE drop-down list.
	Note: You can click Find to display the Find Node dialog box, which contains node information on previous connections to network elements. The Find button is available only after you have logged in to a network element in the current user session. When you select an entry in the Find Node dialog box and click OK, the Login dialog box displays the associated Login NE and NE Type in the Login NE Information area.
11	Select a network element type from the NE Type drop-down list in the Login NE Information area.
	Note 1: You can log in to a maximum of 16 shelf processors at the same time.
	Note 2: Starting with Release 12, up to three Level 5 users can log into and have access to the same network processor at the same time if the user identifiers are different. Each of these Level 5 users can access and manage all 16 network elements within the span of control of this network processor.
12	To log in to the network processor using challenge-response authentication, select the Use Challenge/Response check box.
13	Type an ID in the User ID field in the Login NE Information area. Then,

If	
you are using challenge-response authentication	go to step 18
otherwise	go to the next step

Step	Action
14	Type a password in the Password field in the Login NE Information area.
15	If you want to save the current login settings as a new login profile, click Save As, type a login profile name in the Profile Name field, and click OK.
16	Click Connect to log in to the network processor and start Site Manager.
	Note: The Node Information window for the network processor appears or the Manual Connection dialog box appears if in step 9 you have selected the check box labelled Requires Manual Connection/Secure Modem at Gateway Node.
17	You have completed this procedure.

—continued—

Procedure 2-5 (continued)
Logging in to a network processor using a direct cable connection

Step	Action

Using challenge-response authentication

18 Click Connect to open the Challenge/Response Login dialog box. The User ID field displays the user identifier entered in the Login dialog box. The Challenge field displays the challenge retrieved from the network processor for this login session.

19 Do one of the following to enter the response for this login session:

- Request the response from your network operations center or approved administrator and enter it in the Response field.
- Click Show response generator, then
  - — select the required user privilege code for this login session from the Privilege Code drop-down list
  - — enter the shared secret for the network processor in the Shared Secret field
  - — click the Generate Response button to generate the response for this login session, based on the user identifier, privilege code, and shared secret

Note: The shared secret does not appear on screen. The default shared secret is nortelnetworks.

20 Click OK to log in to the network processor.

—end—

Procedure 2-6
Defining modem settings

Use this procedure to define the modem settings when you are logging in to a network processor using a modem.

Step	Action
1	Select a modem string from the Initialize drop-down list in the Modem Information area.
2	Select a dial method from the Dial using drop-down list in the Modem Information area.
3	Select a serial port from the Port drop-down list in the Port Information area.
4	Select a serial bit rate from the Bit rate drop-down list in the Port Information area.
5	Select a serial data bit rate from the Data bits drop-down list in the Port Information area.
6	Select a serial stop bit rate from the Stop bits drop-down list in the Port Information area.
7	Select a serial parity option from the Parity drop-down list in the Port Information area.
8	Select a serial handshake option from the Handshake drop-down list in the Port Information area.
9	Click OK to return to the Login dialog box.

—end—

Procedure 2-7
Defining direct cable settings

Use this procedure to define the direct cable settings when you are logging in to a network processor using direct cable.

Step	**Action**
1	Select a serial bit rate from the Bit rate drop-down list.
2	Select a serial data bit rate from the Data bits drop-down list.
3	Select a serial stop bit rate from the Stop bits drop-down list.
4	Select a serial parity option from the Parity drop-down list.
5	Select a serial handshake option from the Handshake drop-down list.
6	Click OK to return to the Login dialog box.

—end—

Procedure 2-8
Logging in to a network processor using a login profile

Use this procedure to log in to a network processor using a predefined login profile.

> ***Note 1:*** You can connect to only one network processor span of control at a time.
>
> ***Note 2:*** Starting with Release 12, up to three Level 5 users can log into and have access to the same network processor at the same time if the user identifiers are different. Each of these Level 5 users can access and manage all 16 network elements within the span of control of this network processor.

Step	Action
1	Select Login Manager from the File drop-down menu to open the Login Manager dialog box. ***Note:*** The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. For more information, see Setting the login preferences on page 2-36.
2	Select a profile from the Profile Table. The details of the selected login profile are displayed in the Login Details area.
3	Click Connect.
4	Enter an ID in the User ID field.
5	Enter a password in the Password field.
6	Click Login. ***Note:*** The Node Information window for the network processor appears or the Manual Connection dialog box appears if when creating the profile you have selected the check box labelled Requires Manual Connection/Secure Modem at Gateway Node.

—end—

Procedure 2-9
Starting a remote login session from an OPTera Metro 3500 network element

Use this procedure to start a remote login session to any of the following products from an OPTera Metro 3500 network element:

- an OC-12 TBM network element
- an OC-48 (Classic) network element
- an OC-192 network element
- an operations controller (OPC)
- an OPTera Metro 3000 series network element

Requirements

To perform this procedure, you must ensure that the network element you want to reach is connected to the OPTera Metro 3500 network element through either an Ethernet (ILAN or COLAN) or a fiber connection. A fiber connection also requires that the SONET section data communication channel (SDCC) settings are compatible and activated on both ends.

If you are logging in to an OC-48 Rel. 16.1 or higher, or OC-12 TBM Rel. 14 or higher, ensure that the Secure DCC Access Control tool is ether disabled, or is enabled with access allowed between the OPTera Metro 3500 network element and the OC-48 or OC-12 TBM network element.

Step **Action**

1 Start a terminal session in Site Manager. Depending on the type of login setup, see one of the following procedures:

Starting a terminal session using the network on page 4-2

Starting a terminal session using a modem on page 4-3

Starting a terminal session using direct cable on page 4-4

Note 1: If you are using a network connection, you must use port 10010 for the terminal session.

Note 2: Before you start the remote login session, use the RTRV-RTG-INFO command in a TL1 session to review the list of accessible target identifiers (TIDs) in the network and ensure that the target network element is on the list.

—continued—

Procedure 2-9 (continued)
Starting a remote login session from an OPTera Metro 3500 network element

Step	Action
2	Do one of the following: • if you started a terminal session using the network, press Enter to display the Main Menu • if you started a terminal session using a modem or direct cable, press Enter, and select Send Break from the File drop-down menu in the Terminal window. Press Enter again to display the Main Menu.
3	Enter **1** for General utilities and press Enter to display the General Utility Access Menu.
4	Enter **1** for Login and press Enter to display the Login prompt.
5	At the login prompt, enter the user name. Press Enter to display the Password prompt. ***Note:*** The user account must have user privilege code (UPC) level 4 or higher.
6	At the password prompt, enter the password. Press Enter to display the General Utility Menu.
7	Enter **1** for Rlogin. Press Enter. The system prompts you for the remote OPC or network element name.
8	At the name prompt, enter the TID of the network element ***Note 1:*** The TID is case sensitive. ***Note 2:*** You must place the node name between single quotes (‘ ’) if it contains any non-alphanumeric characters.
9	Press Enter.
10	Once you are logged in to the remote network element, you can enter the required commands. ***Note:*** To terminate the remote login session, logout from the remote network element using the appropriate procedure. Then, press Ctrl+e to terminate the communication between the network elements and to return to the Main menu. For information about the appropriate logout procedure for each product, see the OC-12 TBM, OC-48, or OC-192 documentation.

—end—

Procedure 2-10
Adding a login profile for a Site Manager session using a network connection

Use this procedure to create a login profile using the Add Login Profile dialog box. A login profile allows you to save the login details for a particular connection, so that you do not have to reenter them each time you log in to the network processor.

You can also create a login profile while logging in to a network processor. In this case, you save the information after you enter it in the Login dialog box. For instructions, see Logging in to a network processor using a network connection on page 2-4.

Step	Action
1	Select Login Manager from the File drop-down menu to open the Login Manager dialog box. ***Note:*** The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. For more information, see Setting the login preferences on page 2-36.
2	Click Add to open the Add Login Profile dialog box.
3	Enter a name in the Profile Name field.
4	In the Connect Using area, select the Site Manager radio button.
5	Select Network from the Connection Type drop-down list in the Connection Information area.
6	Select an equipment type from the Gateway Node Type drop-down list.
7	Select or enter an IP address in the Host Name/Address field.
8	Enter a port number in the Port box. ***Note:*** The default port number is 10001.
9	Select a value (in seconds) from the Timeout drop-down list.
10	If a manual connection is required, select the check box labelled Requires Manual Connection/Secure Modem at Gateway Node.

—continued—

Procedure 2-10 (continued)

Adding a login profile for a Site Manager session using a network connection

Step	Action
11	In the Login NE Information area, enter a network processor ID or select a network processor ID from the Login NE drop-down list. ***Note:*** You can click Find to display the Find Node dialog box, which contains node information for previous connections to network elements. The Find button is available only after you have logged in to a network element in the current user session. When you select an entry in the Find Node dialog box and click OK, the Login dialog box displays the associated Login NE and NE Type in the Login NE Information area.
12	Select a network element type from the NE Type drop-down list in the Login NE Information area. ***Note:*** You can log in to a maximum of 16 shelf processors at the same time.
13	Enter a user ID in the User ID field.
14	Do one of the following: • Click Apply to save the current login profile and keep the Add Login Profile dialog box open so that you can create another profile • Click OK to save the current login profile and return to the Login Manager dialog box

—end—

Procedure 2-11
Adding a login profile for a terminal session using a network connection

Use this procedure to create a login profile using the Add Login Profile dialog box. A login profile allows you to save the login details for a particular connection, so that you do not have to re-enter them each time you log in to the network processor.

You can also create a login profile while logging in to a network processor. In this case, you save the information after you enter it in the Login dialog box. For instructions, see Logging in to a network processor using a network connection on page 2-4.

Step	Action
1	Select Login Manager from the File drop-down menu to open the Login Manager dialog box. ***Note:*** The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. For more information, see Setting the login preferences on page 2-36.
2	Click Add to open the Add Login Profile dialog box.
3	Enter a name in the Profile Name field.
4	In the Connect Using area, select the Terminal Session radio button.
5	Select Network from the Connection Type drop-down list in the Connection Information area.
6	Select or enter an IP address in the Host Name/Address field.
7	Enter a port number in the Port box.
8	Select a value (in seconds) from the Timeout drop-down list.
9	Do one of the following: • Click Apply to save the current login profile and keep the Add Login Profile dialog box open so that you can create another profile • Click OK to save the current login profile and return to the Login Manager dialog box

—end—

Procedure 2-12
Adding a login profile for a Site Manager session using a modem connection

Use this procedure to create a login profile using the Add Login Profile dialog box. A login profile allows you to save the login details for a particular connection, so that you do not have to reenter them each time you log in to the network processor.

You can also create a login profile while logging in to a network processor. In this case, you save the information after you enter it in the Login dialog box. For instructions, see Logging in to a network processor using a modem connection on page 2-7.

Step	Action
1	Select Login Manager from the File drop-down menu to open the Login Manager dialog box. ***Note:*** The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. For more information, see Setting the login preferences on page 2-36.
2	Click Add to open the Add Login Profile dialog box.
3	Enter a name in the Profile Name field.
4	In the Connect Using area, select the Site Manager radio button.
5	Select Modem from the Connection Type drop-down list in the Connection Information area.
6	Select an equipment type from the Gateway Node Type drop-down list.
7	Select or enter a telephone number in the Telephone Number drop-down list.
8	Select a value (in seconds) from the Timeout drop-down list.
9	If you want to define the modem settings, click the Advanced button. See Defining modem settings on page 2-14 for further instructions.
10	If you are connecting using a secure modem, select the check box labelled Requires Manual Connection/Secure Modem at Gateway Node.

—continued—

Procedure 2-12 (continued)
Adding a login profile for a Site Manager session using a modem connection

Step **Action**

11 In the Login NE Information area, enter a network processor ID or select a network processor ID from the Login NE drop-down list.

Note: You can click Find to display the Find Node dialog box, which contains node information for previous connections to network elements. The Find button is available only after you have logged in to a network element in the current user session. When you select an entry in the Find Node dialog box and click OK, the Login dialog box displays the associated Login NE and NE Type in the Login NE Information area.

12 Select a network element type from the NE Type drop-down list in the Login NE Information area.

Note: You can log in to a maximum of 16 shelf processors at the same time.

13 Enter an ID in the User ID field in the Login NE Information area.

14 Do one of the following:

- Click Apply to save the current login profile and keep the Add Login Profile dialog box open so that you can create another profile
- Click OK to save the current login profile and return to the Login Manager dialog box

—end—

Procedure 2-13
Adding a login profile for a terminal session using a modem connection

Use this procedure to create a login profile using the Add Login Profile dialog box. A login profile allows you to save the login details for a particular connection, so that you do not have to reenter them each time you log in to the network processor.

You can also create a login profile while logging in to a network processor. In this case, you save the information after you enter it in the Login dialog box. For instructions, see Logging in to a network processor using a modem connection on page 2-7.

Step	Action
1	Select Login Manager from the File drop-down menu to open the Login Manager dialog box. ***Note:*** The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. For more information, see Setting the login preferences on page 2-36.
2	Click Add to open the Add Login Profile dialog box.
3	Enter a name in the Profile Name field.
4	In the Connect Using area, select the Terminal Session radio button.
5	Select Modem from the Connection Type drop-down list in the Connection Information area.
6	Select or enter a telephone number in the Telephone Number drop-down list.
7	Select a value (in seconds) from the Timeout drop-down list.
8	If you want to define the modem settings, click the Advanced button. See Defining modem settings on page 2-14 for further instructions.
9	Do one of the following: • Click Apply to save the current login profile and keep the Add Login Profile dialog box open so that you can create another profile • Click OK to save the current login profile and return to the Login Manager dialog box

—end—

Procedure 2-14
Adding a login profile for a Site Manager session using a direct cable connection

Use this procedure to create a login profile using the Add Login Profile dialog box. A login profile allows you to save the login details for a particular connection, so that you do not have to reenter them each time you log in to the network processor.

You can also create a login profile while logging in to a network processor. In this case, you save the information after you enter it in the Login dialog box. For instructions, see Logging in to a network processor using a direct cable connection on page 2-11.

Step	Action
1	Select Login Manager from the File drop-down menu to open the Login Manager dialog box. ***Note:*** The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. For more information, see Setting the login preferences on page 2-36.
2	Click Add to open the Add Login Profile dialog box.
3	Enter a name in the Profile Name field.
4	In the Connect Using area, select the Site Manager radio button.
5	Select Direct Cable from the Connection Type drop-down list in the Connection Information area.
6	Select an equipment type from the Gateway Node Type drop-down list.
7	Select a port from the Port drop-down list.
8	Select a value (in seconds) from the Timeout drop-down list.
9	If you want to define the cable settings, click the Advanced button. See Defining direct cable settings on page 2-15 for further instructions.
10	If a manual connection is required, select the check box labelled Requires Manual Connection/Secure Modem at Gateway Node.

—continued—

Procedure 2-14 (continued)

Adding a login profile for a Site Manager session using a direct cable connection

Step	Action
11	In the Login NE Information area, enter a network processor ID or select a network processor ID from the Login NE drop-down list. ***Note:*** You can click Find to display the Find Node dialog box, which contains node information for previous connections to network elements. The Find button is available only after you have logged in to a network element in the current user session. When you select an entry in the Find Node dialog box and click OK, the Login dialog box displays the associated Login NE and NE type in the Login NE Information area.
12	Select a network element type from the NE Type drop-down list in the Login NE Information area.
13	Enter an ID in the User ID field.
14	Do one of the following: • Click Apply to save the current login profile and keep the Add Login Profile dialog box open so that you can create another profile • Click OK to save the current login profile and return to the Login Manager dialog box

—end—

Procedure 2-15
Adding a login profile for a terminal session using a direct cable connection

Use this procedure to create a login profile using the Add Login Profile dialog box. A login profile allows you to save the login details for a particular connection, so that you do not have to reenter them each time you log in to the network processor.

You can also create a login profile while logging in to a network processor. In this case, you save the information after you enter it in the Login dialog box. For instructions, see Logging in to a network processor using a direct cable connection on page 2-11.

Step	**Action**
1	Select Login Manager from the File drop-down menu to open the Login Manager dialog box.

Note: The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. For more information, see Setting the login preferences on page 2-36.

2 Click Add to open the Add Login Profile dialog box.

3 Enter a name in the Profile Name field.

4 In the Connect Using area, select the Terminal Session radio button.

5 Select Direct Cable from the Connection Type drop-down list in the Connection Information area.

6 Select a port from the Port drop-down list.

7 Select a value (in seconds) from the Timeout drop-down list.

8 If you want to define the cable setting, click the Advanced button. See Defining direct cable settings on page 2-15 for further instructions.

9 Do one of the following:

- Click Apply to save the current login profile and keep the Add Login Profile dialog box open so that you can create another profile
- Click OK to save the current login profile and return to the Login Manager dialog box

—end—

Procedure 2-16
Editing a login profile

Step **Action**

1 Select Login Manager from the File drop-down menu to open the Login Manager dialog box.

Note: The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. For more information, see Setting the login preferences on page 2-36.

2 Select a login profile from the Login Profile Summary table.

3 Click Edit to open the Edit Login Profile dialog box.

4 Make the required changes.

5 Click OK to return to the Login Manager dialog box.

—end—

Procedure 2-17
Deleting a login profile

Step **Action**

1 Select Login Manager from the File drop-down menu to open the Login Manager dialog box.

Note: The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. For more information, see Setting the login preferences on page 2-36.

2 Select a login profile from the Login Profile Summary table.

3 Click Delete.

Note: To select multiple login profiles, do one of the following:

- Hold down the Ctrl key, and click the specific profiles to be deleted
- Hold down the Shift key, and click the first and the last profile in the range of login profiles to be deleted

4 Click Yes.

5 Select Close from the File drop-down menu to close the Login Manager dialog box.

—end—

Procedure 2-18
Logging in to a network element automatically

Use this procedure to log in to a network element from the navigation tree using the user ID and password from the previous successful login.

> ***Note:*** You cannot automatically log in to a network element if the previous login used challenge-response authentication.

Step	Action
1	Select the network element in the navigation tree.
2	Select Autologin from the File drop-down menu. A black outline highlights the name of the network element to which you are logged in. ***Note 1:*** The system uses the user ID and password from your last successful login in the current session to log in to this network element. ***Note 2:*** If you are already logged in to the network element, the Autologin and the Login As commands are not available. ***Note 3:*** You can also log in automatically by double-clicking the network element in the navigation tree. ***Note 4:*** If the login fails, see Logging in to a network element manually on page 2-31.

—end—

Procedure 2-19
Logging in to a network element manually

Use this procedure to log in to a network element from the navigation tree.

> ***Note:*** You can log in to a maximum of four network elements at the same time.

Step	**Action**
1	Select the network element in the navigation tree.
2	Select Login As from the File drop-down menu to open the Login As dialog box. ***Note:*** If you are already logged in to the network element, the Login As command is not available.
3	Enter a user ID and password.
4	Click Login. A black outline highlights the name of the logged in network element. ***Note 1:*** If the login fails, ensure your user ID and password are correct. Try to log in again. ***Note 2:*** You can also log in manually by right-clicking on the network element in the navigation tree, and clicking Login As.

—end—

Procedure 2-20
Logging in to a network element using a direct cable connection

Requirements

To perform this procedure, you must

- have the user identifier of the account
- have the account password
- connect the PC directly to the shelf processor through the RS-232 port on the shelf processor

Step	Action
1	Start Site Manager to open the Login dialog box. See Starting Site Manager on page 2-3. ***Note:*** The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. If this is the case, select Login from the File drop-down menu in the main window to open the Login dialog box. For more information, see Setting the login preferences on page 2-36.
2	In the Connect Using area, select the Site Manager radio button. ***Note:*** To log in using a terminal session, see Starting a terminal session using direct cable on page 4-4.
3	Select Direct Cable from the Connection Type drop-down list in the Connection Information area.
4	Select an equipment type from the Gateway Node Type drop-down list.
5	Select a port from the Port drop-down list.
6	Select a value (in seconds) from the Timeout drop-down list.
7	If you want to define the direct cable settings, click the Advanced button. See Defining direct cable settings on page 2-15 for further instructions.
8	If a manual connection is required, select the check box labelled Requires Manual Connection/Secure Modem at Gateway Node.

—continued—

Procedure 2-20 (continued)
Logging in to a network element using a direct cable connection

Step	Action
9	In the Login NE field, enter the ID of the shelf processor to which the direct cable is connected.
10	Select a network element type from the NE Type drop-down list in the Login NE Information area.
11	To log in to the network processor using challenge-response authentication, select the Use Challenge/Response check box.
12	Type an ID in the User ID field in the Login NE Information area.

If	Then
you are using challenge-response authentication	go to step 17
otherwise	go to the next step

13 Type a password in the Password field in the Login NE Information area.

14 If you want to save the current login settings as a new login profile, click Save As, type a login profile name in the Profile Name field, and click OK.

15 Click Connect to log in to the shelf processor and start Site Manager.

The Node Information window for the shelf processor appears or the Manual Connection dialog box appears if in step 8 you have selected the check box labelled Requires Manual Connection/Secure Modem at Gateway Node.

16 You have completed this procedure.

Using challenge-response authentication

17 Click Connect to open the Challenge/Response Login dialog box. The User ID field displays the user identifier entered in the Login dialog box. The Challenge field displays the challenge retrieved from the shelf processor for this login session.

18 Do one of the following to enter the response for this login session:

- Request the response from your network operations center or approved administrator and enter it in the Response field.
- Click Show response generator, then
  - — select the required user privilege code for this login session from the Privilege Code drop-down list
  - — enter the shared secret for the shelf processor in the Shared Secret field
  - — click the Generate Response button to generate the response for this login session, based on the user identifier, privilege code, and shared secret

Note: The shared secret does not appear on screen. The default shared secret is nortelnetworks.

19 Click OK to log in to the shelf processor.

—end—

Procedure 2-21
Logging in to a network element through a DSM

Use this procedure to log in to a network element through a DS1 service module (DSM) using the RS-232 port of the DSM.

> ***Note 1:*** No matter how many DSMs you have connected to the shelf, you can have a maximum of two connections through DSMs to the same shelf processor.
>
> ***Note 2:*** Once you are logged in to the shelf processor, you can log in to any other node that is visible to the shelf processor.

Requirements

To perform this procedure, you must

- have the user identifier of the account
- have the account password
- connect the PC directly to the RS-232 port of the DSM
- ensure that the DSM is directly connected to the shelf processor to which you are logging in and that the OAM link is up

Step	Action
1	Start Site Manager to open the Login dialog box. See Starting Site Manager on page 2-3. ***Note:*** The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. If this is the case, select Login from the File drop-down menu in the main window to open the Login dialog box. For more information, see Setting the login preferences on page 2-36.
2	In the Connect Using area, select the Site Manager radio button. ***Note:*** To log in using a terminal session, see Starting a terminal session using direct cable on page 4-4.
3	Select Direct Cable from the Connection Type drop-down list in the Connection Information area.
4	Select an equipment type from the Gateway Node Type drop-down list.
5	Select a port from the Port drop-down list.
6	Select a value (in seconds) from the Timeout drop-down list.
7	If you want to define the direct cable settings, click the Advanced button. See Defining direct cable settings on page 2-15 for further instructions.
8	If a manual connection is required, select the check box labelled Requires Manual Connection/Secure Modem at Gateway Node.

—continued—

Procedure 2-21 (continued)
Logging in to a network element through a DSM

Step	**Action**
9	In the Login NE field, enter the ID of the shelf processor to which you are logging in.
10	Select a network element type from the NE Type drop-down list in the Login NE Information area.
11	To log in to the network processor using challenge-response authentication, select the Use Challenge/Response check box.
12	Type an ID in the User ID field in the Login NE Information area.

If	**Then**
you are using challenge-response authentication	go to step 17
otherwise	go to the next step

13 Type a password in the Password field in the Login NE Information area.

14 If you want to save the current login settings as a new login profile, click Save As, type a login profile name in the Profile Name field, and click OK.

15 Click Connect to log in to the shelf processor and start Site Manager.

The Node Information window for the shelf processor appears or the Manual Connection dialog box appears if in step 8 you have selected the check box labelled Requires Manual Connection/Secure Modem at Gateway Node.

16 You have completed this procedure.

Using challenge-response authentication

17 Click Connect to open the Challenge/Response Login dialog box. The User ID field displays the user identifier entered in the Login dialog box. The Challenge field displays the challenge retrieved from the shelf processor for this login session.

18 Do one of the following to enter the response for this login session:

- Request the response from your network operations center or approved administrator and enter it in the Response field.
- Click Show response generator, then
  - — select the required user privilege code for this login session from the Privilege Code drop-down list
  - — enter the shared secret for the shelf processor in the Shared Secret field
  - — click the Generate Response button to generate the response for this login session, based on the user identifier, privilege code, and shared secret

Note: The shared secret does not appear on screen. The default shared secret is nortelnetworks.

19 Click OK to log in to the shelf processor.

—end—

Procedure 2-22
Setting the login preferences

Use this procedure to choose whether the Login dialog box or the Login Manager dialog box opens automatically when you start Site Manager.

Step	**Action**
1	Select Preferences from the Edit drop-down menu to open the Edit Preferences dialog box.
2	Select one of the following radio buttons in the Login tab: • Login Dialog • Login Profile Manager
3	Click OK.

—end—

Procedure 2-23
Accessing the BCC CLI

Use this procedure to access the Bay command console (BCC) command line interface (CLI) running on the shelf processor. You can use the BCC for provisioning Packet Edge data. Site Manager provides access to the BCC through the Terminal window.

Requirements

If you are accessing the BCC CLI using a network connection, you must use port 10010 for your terminal session.

Step	Action
1	Open the Terminal window. Depending on the type of your login setup, see one of the following procedures: Starting a terminal session using the network on page 4-2 Starting a terminal session using a modem on page 4-3 Starting a terminal session using direct cable on page 4-4
2	In the Terminal window, do one of the following: • if you started a terminal session using the network, press Enter to display the Main Menu • if you started a terminal session using a modem or direct cable, press Enter, and select Send Break from the File menu in the Terminal window. Press Enter again to display the Main Menu.
3	Enter 1 for General utilities and press Enter to display the General Utility Access Menu.
4	Enter 1 for Login and press Enter to display the Login prompt.
5	At the login prompt enter admin. Press Enter to display the Password prompt. ***Note:*** Use your current user ID and password if they are different from admin.
6	At the password prompt enter admin. Press Enter to display the General Utility Menu.
7	Enter 1 for Rlogin. Press Enter. The system prompts you for the remote OPC or network element name.
8	Enter the target identifier (TID) of the network element where the Packet Edge circuit pack resides. ***Note:*** The TID is case sensitive.
9	Press Enter.

—continued—

Procedure 2-23 (continued)
Accessing the BCC CLI

Step	Action
10	Enter a break character (Ctrl+D).
11	Press Enter to display the Main Menu.
12	Enter 3 for BCC Packet Edge interface. Press Enter. The system prompts you for the slot# of the Packet Edge circuit pack.
13	At the prompt, enter the slot number of the Packet Edge circuit pack. Ensure that the Packet Edge circuit pack is in the slot you specify. ***Note:*** Valid slot numbers are: • for 4x100BT and 4x100FX - slots 3 through 10 • for 2xGigE - slots 3, 5, 7, and 9
14	Press Enter to display the Login prompt.
15	At the login prompt, enter rwa.
16	Press Enter to display the Password prompt.
17	At the password prompt, enter rwa.
18	Press Enter to display the Packet Edge prompt. ***Note:*** The prompt displays iPT100 for the 4x100BT circuit pack, 100FX for the 4x100FX circuit pack, and 1GE for the 2xGigE circuit pack.
19	At the Packet Edge prompt, enter the BCC CLI commands as required.
20	To end your CLI session, see Logging out of the BCC CLI on page 2-39.

—end—

Procedure 2-24
Logging out of the BCC CLI

Use this procedure to log out of the Bay command console (BCC) command line interface (CLI).

Step **Action**

1 Enter CTRL+] to display the message, Type q to quit.

2 Enter q.

3 Enter Ctrl+D.

4 Press Enter, then ; (semicolon) to return to the Terminal window prompt.

—end—

Procedure 2-25
Logging out of a network processor or a network element

Use this procedure to log out of a network processor or a network element and continue a Site Manager session. You cannot use this procedure to log out of the account of another user.

Step	Action
1	Select the network element or the network processor in the navigation tree.
2	Select Logout from the File drop-down menu. ***Note 1:*** You can also log out of a network element by right-clicking on it in the navigation tree, and selecting Logout from the pop-up menu. ***Note 2:*** You can log out of all network elements simultaneously by selecting Logout All from the File drop-down menu.
3	In the confirmation dialog box, click Yes to disconnect from the gateway node.

—end—

Procedure 2-26
Disconnecting from a network processor or a network element

Step	Action
1	Select the network element or the network processor in the navigation tree.
2	Select Disconnect from the File drop-down menu.
3	Click Yes in the confirmation dialog box.

—end—

Procedure 2-27
Closing Site Manager

Use this procedure to close a Site Manager session.

Step	Action
1	Select Exit from the File drop-down menu.
2	Click OK in the confirmation dialog box.

—end—

User account management and administration

Procedures for user account management and administration

User account

Passwords

Intrusion attempt handling

Customer managed network

Node information

Centralized security administration

Procedure 3-1
Displaying user account details for a network processor or network element

Use this procedure to view

- the number of accounts for a specific network processor (NP) or network element
- the details of these accounts
- the number of users currently logged in

Requirements

To perform this procedure, you must use an account with a level 4 or 5 user privilege code (UPC).

Step	Action
1	Login to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the NP or network element is selected in the navigation tree.
3	Select User Profile from the Security drop-down menu to open the User Profile window.

The existing user accounts for the selected NP or network element are listed in the User Profile window. The following user account details are provided in the table:

- the user IDs, which are the account names for the selected NP or network element
- the UPC associated with each account
- the status of the account indicating whether the user is currently logged in and the number of users logged in using the account
- the automatic timeout status indicating whether the account is set to automatically log out after a specified time of inactivity
- the timeout value in minutes
- the status of the user account password indicating if the password is in a assigned, valid or expired mode

Note 1: The user account password is in the assigned mode, when a user account is created or if the password is changed by the system administrator.

Note 2: The user account password is in the valid mode, when the user changes his password.

Note 3: The password is in the expired mode, when the user account password has expired.

—end—

Procedure 3-2
Adding a user account

Use this procedure to create a new user account.

This procedure sets the following user account parameters:

- user identifier
- password
- user privilege code (UPC)
- idle time out flag (Timeout)
- timeout value in minutes
- password
  - — expiry status
  - — expiry period
  - — warning period
  - — change period
  - — validation status
  - — validation period

Security levels are set with the UPC parameter when accounts are created. You can assign security levels between 1 and 5, with 5 being the highest. Level 5 privilege allows surveillance of all network elements in the network processor span of control. Level 4 privilege allows complete access to all commands, except for automatic surveillance of all network elements in the network processor span of control. Levels 1 through 4 are recommended for use to log in to a network element. Level 5 is recommended for use to log in to the span of control.

There are two password modes for level 1 through level 3 UPC accounts: Assigned and Valid.

When a new user account is created or if the password is changed by the system administrator, the password is in the assigned mode. When the user changes a password for the first time, the password enters the valid mode.

> ***Note:*** A maximum of 100 UIDs can be added to the password file. If you try to create UID 101, the error message “Status, List Exceeds Maximum” is displayed.

—continued—

Procedure 3-2 (continued)
Adding a user account

Requirements

To perform this procedure, you must:

- ensure you have all the documentation referenced in this procedure.
- use an account with a level 4 or 5 UPC
- note the user ID and password assigned

Password syntax requirements are as follows:

- a password must be between eight and ten characters in length
- a password is a combination of either:
  - alphabetic (A-Z) and numeric (0-9), or
  - alphabetic (A-Z), numeric (0-9) and special characters
- supported special characters are:

  ! “ # $ % ` ( ) * + - . / < = > @ [ ] ^ _ ' { | } ~
- unsupported special characters are:

  ; : &\ , ? and all control characters
- a double quote (“) must always be preceded by a backslash (\). The backslash is permitted in this combination only and is considered a character in the length of the password
- carriage returns (<ENTER>) are not considered as a character in the length of the password
- the string of characters must not contain the invalid passwords that are included in the invalid password list
- a password cannot contain the User ID

Step **Action**

1 Login to the network processor or the network element. See Procedures for interface login and logout on page 2-1.

2 Ensure that the network processor or network element for which you will create a user account is selected in the navigation tree.

3 Select User Profile from the Security drop-down menu to open the User Profile window.

4 Click Add to open the Add User Profile dialog box.

—continued—

Procedure 3-2 (continued)
Adding a user account

Step	Action
5	Enter a user identification in the User ID field. ***Note:*** A user ID must be between one and ten characters in length and must consist of alphabetical and numerical characters only.
6	Enter the password again in the Confirm field. ***Note:*** Passwords are not echoed on the screen. Asterisks are instead displayed in the Password field.
7	Select a user privilege code (UPC) from the Privilege code drop-down list.
8	Select the Automatic timeout check box to automatically log out the user after a specified period of inactivity.
9	In the Automatic logout interval field, enter the timeout value. ***Note:*** The value must be from 1 to 99 inclusive, and represents minutes of inactivity before auto-logout.
10	Select the Password expiry check box to have a password expire after a number of days.
11	In the Password expiry period field, enter the number of days after which the password is no longer valid. ***Note:*** The value must be from 0 to 999 days. The default value is 45 days.
12	In the Password warning period field, enter the number of days prior to password expiration. Site Manager displays a warning message when the user logs in to a network element. ***Note:*** The value must be from 1 to 14. The default value is 14 days.
13	In the Password change period field, enter the number of days after which the user can change the password. ***Note:*** The value must be from 0 to 999 days. The default value is 0 days. This parameter applies even when password expiry or password validation is turned off. However, this parameter does not apply when the password has been assigned and password validation is turned on
14	Select the Password validation check box to have the user change the default password assigned to the user account.
15	In the Password validation period field, enter the number of days the user has to change the password assigned to the user account. ***Note:*** The value must be from 0 to 30 days. The default value is 0 days.
16	Do one of the following: • Click Apply to save the current user account and keep the Add User Profile dialog box open so that you can create another account. • Click OK to save the current user account and return to the User Profile window.

—end—

Procedure 3-3
Creating a temporary user account

Use this procedure to create a temporary user account for a level 1 to 3 UPC.

This procedure sets the following user account parameters:

- user identifier
- password
- user privilege code (UPC)
- idle time out flag (Timeout)
- timeout value in minutes
- password
  - expiry status
  - warning period
  - validation status
  - validation period
  - change period

Security levels are set with the UPC parameter when accounts are created. You can assign security levels between 1 and 5, with 5 being the highest. Level 5 privilege allows surveillance of all network elements in the network processor span of control. Level 4 privilege allows complete access to all commands, except for automatic surveillance of all network elements in the network processor span of control. Levels 1 through 4 are recommended for use to log in to a network element. Level 5 is recommended for use to log in to the span of control.

—continued—

Procedure 3-3 (continued)
Creating a temporary user account

Requirements

To perform this procedure, you must:

- ensure you have all the documentation referenced in this procedure.
- use an account with a level 4 or 5 UPC
- note the user ID and password assigned

Password syntax requirements are as follows:

- a password must be between eight and ten characters in length
- a password is a combination of either:
  - alphabetic (A-Z) and numeric (0-9), or
  - alphabetic (A-Z), numeric (0-9) and special characters
- supported special characters are:

  ! “ # $ % ` ( ) * + - . / < = > @ [ ] ^ _ ' { | } ~
- unsupported special characters are:

  ; : &\ , ? and all control characters
- a double quote (“) must always be preceded by a backslash (\). The backslash is permitted in this combination only and is considered a character in the length of the password
- carriage returns (<ENTER>) are not considered as a character in the length of the password
- the string of characters must not contain the invalid passwords that are included in the invalid password list
- a password cannot contain the User ID

Step **Action**

1 Login to the network processor or the network element. See Procedures for interface login and logout on page 2-1.

2 Ensure that the network processor or network element for which you will create a temporary user account is selected in the navigation tree.

3 Select User Profile from the Security drop-down menu to open the User Profile window.

4 Click Add to open the Add User Profile dialog box.

5 Enter a user identification in the User ID field.

Note: A user ID must be between one and ten characters in length and must consist of alphabetical and numerical characters only.

—continued—

Procedure 3-3 (continued)
Creating a temporary user account

Step	Action
6	Enter a password in the Password field.
7	Enter the password again in the Confirm field. ***Note:*** Passwords are not echoed on the screen. Asterisks are instead displayed in the Password field.
8	Select a user privilege code (UPC) from the Privilege code drop-down list.
9	Select the Automatic timeout check box to automatically log out the user after a specified period of inactivity.
10	In the Automatic logout interval field, enter the timeout value. ***Note:*** The value must be from 1 to 99 inclusive, and represents minutes of inactivity before auto-logout.
11	Select the Password expiry check box.
12	In the Password warning period field, enter 0 days.
13	Disable the Password validation check box.
14	In the Password expiry period field, enter the number of days for the duration of the temporary user account. ***Note:*** The value must be from 0 to 999 days. The default is 45 days.
15	In the Password change period field, enter the number of days plus one for the duration of the temporary user account. ***Note:*** To create a temporary account of 10 days, for example, set the password expiry period to 10 days and the password change period to 11 days.
16	Do one of the following: • Click Apply to save the current user account and keep the Add User Profile dialog box open so that you can create another temporary user account. • Click OK to save the current user account and return to the User Profile window.

—end—

Procedure 3-4
Changing a user account and user privilege levels

Use this procedure to change the following parameters of a user account:

- password
- password attributes
  - — expiry status
  - — expiry period
  - — warning period
  - — change period
  - — validation status
  - — validation period
- user privilege code (UPC)
- timeout interval

You can assign security levels between 1 and 5, with 5 being the highest. Level 5 privilege allows surveillance of all network elements in the network processor span of control. Level 4 privilege allows complete access to all commands, except for automatic surveillance of all network elements in the network processor span of control. Levels 1 through 4 are recommended for use to log in to a network element. Level 5 is recommended for use to log in to the span of control.

Security levels are set with the UPC parameter when accounts are created. Security levels can be changed when a user requires a different level of access privilege.

The following rules apply to the administration of UPCs:

- Users cannot change their own UPCs, including users with a level 4 UPC
- You can change the UPC while the user is logged in, but the change does not affect the current session

Requirements

To perform this procedure, you must

- use an account with a level 4 or 5 UPC
- note the user ID and password assigned
- ensure you have all the documentation referenced in this procedure.

—continued—

Procedure 3-4 (continued)

Changing a user account and user privilege levels

Step	**Action**
1	Login to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the network processor or network element is selected in the navigation tree.
3	Select User Profile from the Security drop-down menu to open the User Profile window. The user accounts for logging in to the selected network processor or network element appear in the User Profile window.
4	Select the user account to be edited.
5	Click Edit to open the Edit User Profile dialog box.
6	

If you want to edit a user's	**Then** go to
password	step 7
privilege code	step 13
timeout settings	step 18
password expiry settings	step 25
password validation settings	step 35

Editing a user's password

7 Select the password tab.

8 In the Password field, type a new password.

9 In the Confirm Password field, re-type the new password.

10 Click Apply.

11

If you	**Then** go to
want to edit more user profile attributes	step 6
do not want to edit more user profile attributes	step 12

12 Click OK to return to the User Profile Window.

You have completed this procedure.

Editing a user's privilege code

13 Select the Privilege tab.

14 In the Privilege code menu, select a privilege code.

15 Click Apply.

—continued—

Procedure 3-4 (continued)
Changing a user account and user privilege levels

Step **Action**

16

If you	**Then** go to
want to edit more user profile attributes	step 6
do not want to edit more user profile attributes	step 17

17 Click OK to return to the User Profile Window.

You have completed this procedure.

Editing a user's timeout settings

18 Select the Timeout tab.

19 To enable automatic timeout, put a check mark in the Automatic Timeout box.

20 To disable automatic timeout, leave the Automatic Timeout box empty and go to step 23.

21 In the Timeout Interval field, type the desired number of minutes (1-99).

22 Click Apply.

23

If you	**Then** go to
want to edit more user profile attributes	step 6
do not want to edit more user profile attributes	step 24

24 Click OK to return to the User Profile Window.

You have completed this procedure.

Editing a user's password expiry settings

25 Select the Password Expiry tab.

26 To enable password expiry, put a check mark in the Password Expiry box.

27 To disable password expiry, leave the Password Expiry box empty and go to step 33.

28 To reset the password expiry attributes to the default parameters, click Reset to Defaults and go to step 33.

29 In the Password expiry period field, type the desired number of days (0-999).

Note: The default value is 45 days.

30 In the Password warning period field, type the desired number of days (0-14).

Note: The default value is 14 days.

31 In the Password change period field, type the desired number of days (0-999).

Note: The default value is 0 days. This parameter applies even when password expiry or password validation is turned off. However, this parameter does not apply when the password has been assigned and password validation is turned on.

32 Click Apply.

—continued—

Procedure 3-4 (continued)
Changing a user account and user privilege levels

Step **Action**

33

If you	**Then** go to
want to edit more user profile attributes	step 6
do not want to edit more user profile attributes	step 34

34 Click OK to return to the User Profile Window.

You have completed this procedure.

Editing a user's password validation settings

35 Select the Password Validation tab.

36 To enable password validation, put a check mark in the Password Validation box, click Apply and go to step 39.

37 In the Password validation period field, type the desired number of days (0-30).

Note: The default value is 0 days.

38 Click Apply.

39

If you	**Then** go to
want to edit more user profile attributes	step 6
do not want to edit more user profile attributes	step 40

40 Click OK to return to the User Profile Window.

—end—

Procedure 3-5
Changing password default values for security parameters

Use this procedure to change the default values of security parameters on user accounts listed in the defaults list.

Requirement

To perform this procedure, you must:

- use an account with a level 4 or 5 user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step **Action**

1 Log in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.

2 Ensure that the network processor or network element is selected in the navigation tree.

3 Select User Profile from the Security drop-down menu to open the User Profile window.

4 Select the user profile to be edited.

5 Click Defaults to open the Default Security Parameters dialog box.

6 Select the Password Expiry check box to have a password expire after a number of days.

7 In the Password expiry period field, enter the number of days after which the password is no longer valid.

Note: The value must be from 0 to 999 days. The default value is 45 days.

8 In the Password warning period field, enter the number of days after which Site Manager displays a warning message when the user logs in to a network element.

Note: The value must be from 1 to 14. The default value is 14 days.

9 In the Password change period field, enter the number of days after which the user can change the password.

Note: The value must be from 0 to 999 days. The default value is 0 days. This parameter applies even when password expiry or password validation is turned off. However, this parameter does not apply when the password has been assigned and password validation is turned on

—continued—

Procedure 3-5 (continued)

Changing password default values for security parameters

Step	Action
10	Select the Password Validation check box to have the user change the default password assigned to the user account.
11	In the Password validation period field, enter the number of days the user has to change the password assigned to the user account. ***Note:*** The value must be from 1 to 30 days. The default value is 0 days.
12	Click OK to save the current security parameters and return to the User Profile window.

—end—

Procedure 3-6
Deleting a user account

Use this procedure to delete a user account for a network element or network processor. User accounts are usually deleted when operating company personnel no longer use the network element or network processor.

Requirements

To perform this procedure you must:

- use an account with a level 4 or 5 user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step	Action
1	Login to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the network processor or network element is selected in the navigation tree.
3	Select User Profile from the Security drop-down menu to open the User Profile window. The user accounts for logging in to the selected network processor or network element appear in the User Profile window.
4	Select the user account to delete. ***Note:*** To select multiple user accounts, do one of the following: • Hold down the Ctrl key, and click the specific accounts to be deleted. • Hold down the Shift key, and click the first and the last account in the range of accounts to be deleted.
5	Click Delete.
6	Click Yes in the confirmation box.

—end—

Procedure 3-7
Changing a password

Use this procedure to change your account password for the network element or network processor you are logged in. All users have sufficient privilege to change their own password at any time.

There are two password modes for level 1 through level 3 UPC accounts:

- Assigned
- Valid

When a new user account is created or if the password is changed by the system administrator, the password is in the assigned mode. When the user changes his password for the first time, the password enters the valid mode.

Requirements

To perform this procedure, you must ensure you have all the documentation referenced in this procedure.

Password syntax requirements are as follows:

- a password must be between eight and ten characters in length
- a password is a combination of either:
  - alphabetic (A-Z) and numeric (0-9), or
  - alphabetic (A-Z), numeric (0-9) and special characters
- supported special characters are:

  ! “ # $ % ` ( ) * + - . / < = > @ [ ] ^ _ ' { | } ~
- unsupported special characters are:

  ; : &\ , ? and all control characters
- a double quote (“) must always be preceded by a backslash (\). The backslash is permitted in this combination only and is considered a character in the length of the password
- carriage returns (<ENTER>) are not considered as a character in the length of the password
- the string of characters must not contain the invalid passwords that are included in the invalid password list
- a password cannot contain the User ID

—continued—

Procedure 3-7 (continued)
Changing a password

Step	Action
1	Login to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the network processor or network element is selected in the navigation tree.
3	Select Change Password from the Security drop-down menu.
4	Enter your current password in the Old password field.
5	Enter your new password in the New password field.
6	Enter your new password again in the Confirm new password field.
7	Click OK.

—end—

Procedure 3-8
Displaying invalid passwords

Use this procedure to display a list of invalid passwords that cannot be assigned for any user account on the network element.

Requirements

To perform this procedure, you must ensure you have all the documentation referenced in this procedure.

Password syntax requirements are as follows:

- a password must be between eight and ten characters in length
- a password is a combination of either:
  - alphabetic (A-Z) and numeric (0-9), or
  - alphabetic (A-Z), numeric (0-9) and special characters
- supported special characters are:

  ! “ # $ % ` ( ) * + - . / < = > @ [ ] ^ _ ' { | } ~
- unsupported special characters are:

  ; : &\ , ? and all control characters
- a double quote (“) must always be preceded by a backslash (\). The backslash is permitted in this combination only and is considered a character in the length of the password
- carriage returns (<ENTER>) are not considered as a character in the length of the password
- the string of characters must not contain the invalid passwords that are included in the invalid password list
- a password cannot contain the User ID

Step **Action**

1 Log in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.

2 Ensure that the network processor or network element is selected in the navigation tree.

—continued—

Procedure 3-8 (continued)
Changing a password

Step	**Action**
3	Select Invalid Passwords from the Security drop-down menu to open the Invalid Passwords window. Passwords in the Invalid passwords list: • must be between 1 and 10 characters in length • cannot be admin or surveil because they are default system passwords for those accounts ***Note:*** The Invalid passwords list cannot contain more than 50 passwords.

—end—

Procedure 3-9
Adding invalid passwords

Use this procedure to add to the list of invalid passwords.

Requirements

To perform this procedure, you must:

- use an account with a level 4 or 5 user privilege code (UPC)
- ensure you have all the documentation referenced in this procedure.

Password syntax requirements are as follows:

- a password must be between eight and ten characters in length
- a password is a combination of either:
  - alphabetic (A-Z) and numeric (0-9), or
  - alphabetic (A-Z), numeric (0-9) and special characters
- supported special characters are:
  ! “ # $ % ` ( ) * + - . / < = > @ [ ] ^ _ ' { | } ~
- unsupported special characters are:
  ; : &\ , ? and all control characters
- a double quote (“) must always be preceded by a backslash (\). The backslash is permitted in this combination only and is considered a character in the length of the password
- carriage returns (<ENTER>) are not considered as a character in the length of the password
- the string of characters must not contain the invalid passwords that are included in the invalid password list
- a password cannot contain the User ID

Step **Action**

1 Log in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.

2 Ensure that the network processor or network element is selected in the navigation tree.

3 Select Invalid Passwords from the Security drop-down menu to open the Invalid Passwords window.

—continued—

Procedure 3-9 (continued)
Adding invalid passwords

Step	Action
4	Click Add to open the Add Invalid Passwords dialog box. ***Note 1:*** The Add button is disabled if the list already contains 50 invalid passwords. ***Note 2:*** Passwords on the list are invalid on their own or when combined with other characters.
5	Enter a password on each line, hitting the Enter key after each password.
6	Click OK to have the list of password validated.

—end—

Procedure 3-10
Deleting invalid passwords

Use this procedure to delete passwords from the list of invalid passwords.

Requirement

To perform this procedure, you must:

- use an account with a level 4 or 5 user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step	Action
1	Log in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure the network processor or network element is selected in the navigation tree.
3	Select Invalid Passwords from the Security drop-down menu to open the Invalid Passwords window.
4	(see table below)

4

If you want to delete	**Then** go to
one or selected invalid passwords	step 5
the entire list of invalid passwords	step 8

Step	Action
5	Select a password from the Invalid passwords list that you want to delete.
6	If you want to delete more than one invalid password from the list, hold down the CTRL key while clicking on each of the remaining invalid passwords you want to delete.
7	Go to step 11.
8	Select the first invalid password in the list by clicking once on it.
9	Scroll down to the last invalid password in the list.
10	Hold down the Shift key while clicking the last invalid password in the list.
11	Click Delete.
12	Click Yes in the confirmation box.

—end—

Procedure 3-11
Displaying intrusion attempts handling details

Use this procedure to display details about intrusion attempts handling settings.

> **CAUTION**
> **Risk of user lockout for all users**
> An intrusion attempt on all shelf or network processors can cause a lockout for all users on that shelf or network processor. Access to the affected shelf or network processors will be denied until the lockout period expires.

Requirement

To perform this procedure, you must:

- use an account with a level 4 or 5 user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step **Action**

1 Log in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.

2 Ensure that the network processor or network element is selected in the navigation tree.

3 Select Intrusion Attempt Handling from the Security drop-down menu to open the Instrusion Attempt Handling window.

Note: The lockout details provided in the Lockout status table include the true originating address (from either a direct or remote login attempt) and the Inhibit/Allow status.

—end—

Procedure 3-12
Setting intrusion attempts handling

Use this procedure to enable or to disable the intrusion attempts handling.

> **CAUTION**
> **Risk of user lockout for all users**
> An intrusion attempt on all shelf or network processors can cause a lockout for all users on that shelf or network processor. Access to the affected shelf or network processor will be denied until the lockout period expires.

Requirement

To perform this procedure, you must:

- use an account with a level 4 or 5 user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step	Action
1	Log in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the network processor or network element is selected in the navigation tree.
3	Select Intrusion Attempt Handling from the Security drop-down menu to open the Instrusion Attempt Handling window. Click Refresh. ***Note:*** The lockout details provided in the Lockout status table include the true originating address (from either a direct or remote login attempt) and the Inhibit/Allow status.
4	Click Settings to open the default intrusion parameter dialog box.
5	**If** you want to / **Then** go to disable the Intrusion Attempt Handling feature — step 6 enable the Intrusion Attempt Handling feature — step 7
6	Change the lockout duration field to 0 seconds and click OK. Click Yes in the confirmation dialog box. This procedure is complete.
7	Change the lockout duration field to a value greater than 0 seconds and click OK.

—end—

Procedure 3-13
Unlocking channel identifiers

Use this procedure to unlock channel identifiers on a network element.

> ***Note:*** This procedure will automatically clear the intrusion alarm if present.

Requirement

To perform this procedure, you must:

- use an account with a level 4 or 5 user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step	Action
1	Log in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the network processor or network element is selected in the navigation tree.
3	Select Intrusion Attempt Handling from the Security drop-down menu to open the Instrusion Attempt Handling window.
4	Click Unlock Channels. All channels are unlocked.
5	Click Yes in the confirmation dialog box.

—end—

Procedure 3-14
Clearing intrusion alarms

Use this procedure to clear an intrusion attempt alarm on a network element.

Requirement

To perform this procedure, you must:

- use an account with a level 4 or 5 user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step	Action
1	Log in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the network processor or network element is selected in the navigation tree.
3	Select Intrusion Attempt Handling from the Security drop-down menu to open the Instrusion Attempt Handling window.
4	Click Clear Intrusion Alarm. All security alarms (including intrusion alarms or CMN alarms) are cleared. ***Note:*** This procedure will not unlock channels.
5	Click Yes in the confirmation dialog box.

—end—

Procedure 3-15 **Changing default values for intrusion attempt handling**

Use this procedure to change the default intrusion attempt handling default settings.

Requirement

To perform this procedure, you must:

- use an account with a level 4 or 5 user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step **Action**

1 Log in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.

2 Ensure that the network processor or network element is selected in the navigation tree.

3 Select Intrusion Attempt Handling from the Security drop-down menu to open the Instrusion Attempt Handling window.

4 Click Settings to open the Intrusion Settings dialog box.

5 In the Maximum invalid login attempts field, enter the number of unsuccessful attempts the user can perform to log in to a network element.

Note: The value must be from 2 to 9 attempts. The default is 5 attempts.

6 In the Lockout duration field, enter the time interval that the user must wait before attempting to log in to a network element again.

Note: The value must be from 0 to 999 seconds. The default is 0 seconds.

7 Click OK.

—end—

Procedure 3-16
Retrieving security logs

Use this procedure to open the Security Logs window and to retrieve security log event data for a network element or a network processor.

Requirement

To perform this procedure, you must:

- use an account with a level 4 or 5 user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step	Action
1	Log in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure the network processor or network element is selected in the navigation tree.
3	Select Security Logs from the Security drop-down menu to open the Security Logs window.
4	Click Refresh to retrieve up-to-date security log events. ***Note:*** To order the data by a particular column category, click the required column header in the Security Logs window.

—end—

Procedure 3-17
Displaying customer managed network details

Use this procedure to display details about customer managed networks.

Requirement

To perform this procedure, you must:

- use an account with a level 4 or 5 user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step	Action
1	Log in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure the network processor or network element is selected in the navigation tree.
3	Select Customer Managed Network from the Security drop-down menu to open the Customer Managed Network window.

—end—

Procedure 3-18
Enabling the customer managed network

Use this procedure to enable the customer managed network feature.

Requirement

To perform this procedure, you must:

- use an account with a level 4 or 5 user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step	Action
1	Log in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the network processor or network element is selected in the navigation tree.
3	Select Customer Managed Network from the Security drop-down menu to open the Customer Managed Network window.
4	Click Edit to open the Edit Customer Managed Network dialog box.
5	Click the Enable radio button to enable the customer manager network.
6	Click OK.

—end—

Procedure 3-19
Disabling the customer managed network

Use this procedure to disable the customer managed network feature.

Requirement

To perform this procedure, you must:

- use an account with a level 4 or 5 user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step **Action**

1 Log in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.

2 Ensure that the network processor or network element is selected in the navigation tree.

3 Select Customer Managed Network from the Security drop-down menu to open the Customer Managed Network window.

4 Click Edit to open the Edit Customer Managed Network dialog box.

5 Click the Disable radio button to disable the customer manager network.

6 Click OK.

—end—

Procedure 3-20
Changing customer managed network details

Use this procedure to allow or deny access to targeted network elements on customer managed networks.

> *Note:* If you disable the Customer Managed Network feature, all network elements in the network will have access.

Requirement

To perform this procedure, you must:

- use an account with a level 4 or 5 user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step **Action**

1 Log in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.

2 Ensure that the network processor or network element is selected in the navigation tree.

3 Select Customer Managed Network from the Security drop-down menu to open the Customer Managed Network window.

4 Click Edit to open the Edit Customer Managed Network dialog box.

5

If you want to	**Then** go to
disable the Customer Managed Network feature	step 6
enable the Customer Managed Network feature	step 9

6 Select the Disable radio button, under Status.

7 Click OK.

8 Click Yes in the confirmation dialog box.

You have completed this procedure.

9 Select the Enable radio button, under Status.

10

If you want to allow	**Then** go to
all network elements	step 11
all but a few network elements	step 14
no network elements	step 18
selected network elements	step 21

11 Select All NEs in the Allow drop-down menu.

12 Click OK.

—continued—

Procedure 3-20 (continued)
Changing customer managed network details

Step	Action
13	Click Yes in the confirmation dialog box.
	You have completed this procedure.
14	Select All NEs except in the Allow drop-down menu.
15	Move network elements from the left field to the right field (or back) as required, by selecting a network element and clicking one of the arrows between the fields.
16	Click OK.
17	Click Yes in the confirmation dialog box.
	You have completed this procedure.
18	Select None (Deny all NEs) in the Allow drop-down menu.
19	Click OK.
20	Click Yes in the confirmation dialog box.
	You have completed this procedure.
21	Select Selected NEs in the Allow drop-down menu.
22	Move network elements from the left field to the right field (or back) as required, by selecting a network element and clicking one of the arrows between the fields.
23	Click OK.
24	Click Yes in the confirmation dialog box.

—end—

Procedure 3-21
Clearing security alarms for customer managed networks

Use this procedure to clear all security alarms for customer managed networks.

Requirement

To perform this procedure, you must:

- use an account with a level 4 or 5 user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step	**Action**
1	Log in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure the network processor or network element is selected in the navigation tree.
3	Select Customer Managed Network from the Security drop-down menu to open the Customer Managed Network window.
4	Click Clear Security Alarms. All security alarms (including intrusion alarms) clear.

—end—

Procedure 3-22
Retrieving information about the network element or network processor

Use this procedure to retrieve the following general and system information about a network element or network processor:

- name
- node type
- node function
- the release of the software installed
- date, time, and time zone
- default AINS value
- SDTH value

Requirements

To perform this procedure, you must ensure you have all the documentation referenced in this procedure.

Step	Action
1	Ensure that you are logged in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the network processor or network element is selected in the navigation tree.
3	Select Node Information from the Configuration drop-down menu to open the Node Information window. ***Note:*** The Node Information window is automatically displayed after you log in to a network element or network processor.

—end—

Procedure 3-23
Changing the name of a network element or network processor

Use this procedure to set up or change the name assigned to a network element or network processor. The network element or network processor name is called the system identifier (SID).

CAUTION
Risk of loss of functionality
Ensure every network element has a unique system identifier (SID). If you are changing the name of a network element, ensure the new name is unique within the OSI network.

Any change in the SID impacts the telemetry byte-oriented serial (TBOS) display mapping. To reassign the network element or network processor to the correct TBOS display, see 323-1059-520, Procedures for TBOS on page 1-1. Additionally, if the configuration is bidirectional linear switched ring (BLSR), any change to the SID requires that the entry be made to the BLSR configuration as well.

Requirements

To perform this procedure, you must:

- ensure you use an account with a level 3 or higher user privilege code (UPC)
- ensure the name of the network element or network processor is unique within the OSI network
- ensure there is not more than one user logged into the network element or network processor
- ensure there is no TBOS connection to the network element you want to rename
- ensure you have all the documentation referenced in this procedure.

Step	Action
1	Ensure that you are logged in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the network processor or network element is selected in the navigation tree.

—continued—

Procedure 3-23 (continued)
Changing the name of a network element or network processor

Step	Action
3	Select Node Information from the Configuration drop-down menu to open the Node Information window.
	Note: The Node Information window is automatically displayed after you log in to a network element or network processor.
4	Select the General tab.
5	On the General tab, Click Edit to open the Edit General dialog box.
6	Select Node name from the parameter drop-down list.
7	Enter the new node name in the New value field.
	Note: The network element name must be between 1 and 20 alphanumeric characters (inclusive). The first character must be a letter. The remaining characters can be any combination of letters, numbers, or dashes (-). The name cannot contain spaces or the following symbols:
	\ “
8	Click OK.
9	Click Yes in the confirmation dialog box. You will be logged out of the network element or network processor.
	Note: If there is more than one active user logged in to this node, you will get an error message.

10

If you have changed the name of	**Then**
a network element	go to step 11
a network processor	you have completed this procedure

11 Remove the network element with the old name from the network processor span of control. See 323-1059-520, Removing a network element from the span of control of a network processor on page 4-6.

12 Add the network element with the new name to the network processor span of control. See 323-1059-520, Adding a network element to the span of control of a network processor on page 4-3.

13

If you have changed the name of a network element and the network configuration it belongs to	**Then**
is a BLSR	go to step 14
is not a BLSR	you have completed this procedure

14 Log in to the network element with the new name. See Procedures for interface login and logout on page 2-1.

15 Select the network processor in the navigation tree.

—continued—

Procedure 3-23 (continued)
Changing the name of a network element or network processor

Step	Action
16	Select BLSR Ring Management from the Configuration menu.
17	In the BLSR Ring Configuration Information window, click on the Rings Configuration tab.
18	Select the NPx from the NE list.
19	Select the name of the ring this network element belongs to in the Ring list.
20	Select the network element with the old SID and note its APS ID, West Facility APS ID, and East Facility APS ID.
21	Delete the selected network element from the BLSR configuration.
22	Click Add.
23	In the Add Node dialog box, select the network element with the new SID in the NE list.
24	Select the APS ID of the network element with the new SID (noted in step 20, in the NE APS ID list.
25	Select the east optical facility (noted in step 20) of the network element with the new SID, in the East Facility list.
26	In the East APS ID list, select the East Facility APS ID (noted in step 20).
27	Select the west optical facility (noted in step 20) of the network element with the new SID, in the West Facility list.
28	In the West APS ID list, select the West Facility APS ID (noted in step 20).
29	Click OK.
30	Click Check. ***Note:*** If the Check fails, the entered BLSR configuration is invalid. Return to the BLSR configuration provisioning procedure to correct the problem. See 323-1059-320, Provisioning a BLSR configuration on page 6-34.
31	Select the Rings Commissioning tab.
32	Click Load NP->SP. ***Note:*** Allow enough time for the load to run.
33	Click Invoke. Click Yes in the warning dialog box. ***Note:*** Allow enough time for the invoke to run.
34	Click Commit. Click OK in the confirmation dialog box.

—end—

Procedure 3-24
Changing the network element or network processor date, time, and time zone

Use this procedure to set up or change the network element or network processor date, time, and time zone.

The date, time, and time zone are set up as part of commissioning.

> ***Note 1:*** It is recommended that you change the date and time on the network element if changes are required on the network processor. The network processor continuously retrieves data and time from the co-located shelf processor. The network processor synchronizes its date and time to the shelf processor date and time if the difference is more than 2 minutes.
>
> ***Note 2:*** Time zone offset and daylight savings time are time of day synchronization parameters. See Setting time offset and daylight savings offset on page 8-8 for provisioning these parameters.

Requirements

To perform this procedure, you must:

- use an account with a level 3 or higher user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step	Action
1	Ensure that you are logged in to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the network processor or network element is selected in the navigation tree.
3	Select Node Information from the Configuration drop-down menu to open the Node Information window. ***Note:*** The Node Information window is automatically displayed after you log in to a network element or network processor.
4	Select the General tab.
5	On the General tab, click Edit to open the Edit General dialog box.
6	Select Date and Time from the Parameter drop-down list.
7	Do one of the following: • Click Set to Local Date and Time • In the New value field, enter the new time using the format hour:minute:second (HH:MM:SS), and enter the new date using the format year-month-day (YYYY-MM-DD)

—continued—

Procedure 3-24 (continued)

Changing the network element or network processor date, time, and time zone

Step	**Action**
8	Click Apply.
9	If you need to change the time zone, select Time Zone from the Parameter drop-down list.
10	Select an option from the New value drop down list.
11	Click OK.

—end—

Procedure 3-25
Changing the network element type

Use this procedure to update the network element to support linear and UPSR add/drop multiplexer (ADM) capabilities.

> ***Note:*** You cannot use this procedure to change the network processor type.

Requirements

To perform this procedure you must:

- use an account with a level 3 or higher user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step	Action
1	Ensure that you are logged in to the network element. See Procedures for logging in to a network element on page 2-1.
2	Ensure that the network element is selected in the navigation tree.
3	Select Node Information from the Configuration drop-down menu to open the Node Information window. ***Note:*** The Node Information window is automatically displayed after you log in to a network element.
4	Select the General tab.
5	On the General tab, click Edit to open the Edit General dialog box.
6	Select Function from the Parameter drop-down list.
7	Select ADM from the New value drop-down list.
8	Click OK.

—end—

Procedure 3-26
Setting the common language location identifier

Use this procedure to set the common language location identifier (CLLI) for the network element. The CLLI is an 11-character alphanumeric code in the form AAAABBCCDDD where

- AAAA is the geographical or place code
- BB is the geopolitical or state/country code
- CC is the network site code
- DDD is the network entity code

The CLLI uniquely represents the geographic location of the network element.

Requirements

To perform this procedure you must:

- use an account with a level 3 or higher user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step	Action
1	Ensure that you are logged in to the network element. See Procedures for logging in to a network element on page 2-1.
2	Ensure that the network element is selected in the navigation tree.
3	Select Node Information from the Configuration drop-down menu to open the Node Information window. ***Note:*** The Node Information window is automatically displayed after you log in to a network element.
4	Select the General tab.
5	On the General tab, click Edit to open the Edit General dialog box.
6	Select CLLI from the Parameter drop-down list.
7	Enter the CLLI in the New value field. The CLLI must be 11 characters or less. The CLLI cannot include special characters but can include spaces. Spaces are included in the length of the CLLI. To maintain case sensitivity when the CLLI includes lowercase characters, enclose the CLLI in double quotes (“). The double quotes are not included in the length of the CLLI.
8	Click OK.

—end—

Procedure 3-27
Retrieving the centralized security administration attributes

Use this procedure to retrieve the centralized security administration (CSA) attributes for a shelf processor or network processor.

Requirements

Ensure you have all the documentation referenced in this procedure.

Step	Action
1	Log in to the network processor or shelf processor. See Procedures for logging in to a network processor on page 2-1 or Procedures for logging in to a network element on page 2-1.
2	Ensure that the network processor or shelf processor is selected in the navigation tree.
3	Select Centralized Security Administration from the Security menu.

—end—

Procedure 3-28
Setting the centralized security administration attributes

Use this procedure to set the

- authentication mode and the alternate authentication mode for a shelf processor or network processor
- the primary and security gateways for a shelf processor

Requirements

To perform this procedure you must:

- use an account with a level 4 or higher user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step	Action
1	Log in to the network processor or shelf processor. See Procedures for logging in to a network processor on page 2-1 or Procedures for logging in to a network element on page 2-1.
2	Ensure that the network processor or shelf processor is selected in the navigation tree.
3	Select Centralized Security Administration from the Security menu.
4	For a network processor, click Edit Mode to open the Edit Authentication Settings dialog box. For a shelf processor, click Edit to open the Edit Authentication Settings dialog box.
5	Select the authentication mode for the network processor or shelf processor from the Authentication Mode area. Centralized authentication uses Remote Authentication Dial-In User Service (RADIUS). Local authentication uses either local accounts or local challenge-response.
6	Select the alternate authentication mode for the network processor or shelf processor from the Alternate drop-down list. The system uses the alternate mode when centralized authentication is disabled or is enabled but unavailable.

—continued—

Procedure 3-28 (continued)
Setting the centralized security administration attributes

Step	Action
7	For a shelf processor, enter the target identifiers of the network processors to use as the primary and secondary security gateways in the Primary Security Gateway and Secondary Security Gateway fields. Alternatively, click on Find to open the Find Node dialog box and select the network processor from a list. The Find Node dialog box lists network processors and network elements on the routing table of the shelf processor. ***Note 1:*** The shelf processor must be in the span of control of the network processor that acts as a security gateway. ***Note 2:*** To deprovision the current primary or secondary gateway, select NONE from the Primary Security Gateway or Secondary Security Gateway field.
8	Click OK.

—end—

Procedure 3-29
Setting the primary or secondary RADIUS server

Use this procedure to set the primary or secondary RADIUS server of a network processor.

Requirements

To perform this procedure you must:

- use an account with a level 4 or higher user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step	Action
1	Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.
2	Ensure that the network processor is selected in the navigation tree.
3	Select Centralized Security Administration from the Security menu.
4	Select Primary to set the primary RADIUS server or select Secondary to set the secondary RADIUS server.
5	Click Edit Server to open the Edit RADIUS Server Settings dialog box.
6	Enable or disable the RADIUS server by selecting On or Off from the Status area.
7	Enter the IP address of the RADIUS server in the IP Address field.
8	Enter the timeout value (in seconds) for communication between the network processor and RADIUS server in the Timeout field. The timeout value can range between 1 and 120 seconds. ***Note 1:*** There can be a small delay from the time the system detects a timeout to the time the message displays on screen. Therefore, the timeout message might not appear precisely at the provisioned timeout value. ***Note 2:*** A timeout between the network processor and a RADIUS server does not count as an intrusion attempt.
9	Enter the UDP port number of the RADIUS server in the Port field.
10	Click OK.

—end—

Procedure 3-30
Changing the shared secret for a network processor or shelf processor

Use this procedure to change the shared secret for a network processor or shelf processor. The shared secret is used when logging in to the network processor or shelf processor using challenge-response authentication.

Requirements

To perform this procedure you must:

- use an account with a level 4 or higher user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step	Action
1	Log in to the network processor or shelf processor. See Procedures for logging in to a network processor on page 2-1 or Procedures for logging in to a network element on page 2-1.
2	Ensure that the network processor or shelf processor is selected in the navigation tree.
3	Select Centralized Security Administration from the Security menu.
4	Click Set Shared Secret to open the Set Shared Secret dialog box.
5	Enter the current shared secret in the Old Shared Secret field. The default shared secret is nortelnetworks.
6	Enter the new shared secret in the Shared Secret field. The shared secret can be any alphanumeric string between 8 and 20 characters.
7	Enter the new shared secret again in the Confirm Shared Secret field.
8	Click OK.

—end—

Procedure 3-31
Changing the shared secret for the primary or secondary RADIUS server

Use this procedure to change the shared secret for the primary or secondary RADIUS server of a network processor.

Requirements

To perform this procedure you must:

- use an account with a level 4 or higher user privilege code (UPC).
- ensure you have all the documentation referenced in this procedure.

Step	Action
1	Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.
2	Ensure that the network processor is selected in the navigation tree.
3	Select Centralized Security Administration from the Security menu.
4	Click Set Server Shared Secret to open the Set Server Shared Secret dialog box.
5	Select whether to set the shared secret for the primary or secondary RADIUS server from the Server drop-down list.
6	Enter the shared secret in the Shared Secret field. The shared secret can be any alphanumeric string between 8 and 20 characters.
7	Enter the shared secret again in the Confirm Shared Secret field.
8	Click OK.

—end—

Procedure 3-32
Calculating the response for a challenge-response login

Use this procedure to calculate the response for a challenge-response login to a shelf processor or network processor.

Step	Action
1	Log in to the network processor or shelf processor using challenge-response authentication. See Procedures for logging in to a network processor on page 2-1 or Procedures for logging in to a network element on page 2-1.
2	Select Challenge/Response Calculator from the Tools submenu of the File drop-down menu.
3	Enter the user identifier of the shelf processor or network processor in the User ID field.
4	Enter the challenge for the shelf processor or network processor in the Challenge field.
5	Select the required user privilege code for the login session in the Privilege Code field.
6	Enter the shared secret for the shelf processor or network processor. The secret does not appear on screen. The default shared secret is nortelnetworks.
7	Click Generate Response to generate the response for the login session, based on the user identifier, privilege code, and shared secret. The Response appears in the Response field.
8	Click OK to close the dialog box.

—end—

Manual connection terminal, telnet terminal and communications log

Procedures for using the manual connection terminal, telnet terminal, and the communications log

Procedure 4-1
Starting a terminal session using the network

In a terminal session, you can connect to a network element or any other type of remote system that supports a VT320, VT220, VT100, or ASCII character-based interface independently of Site Manager.

Step	Action
1	Start Site Manager to open the Login dialog box. See Starting Site Manager on page 2-3. ***Note 1:*** If you have already logged in to a network processor and want to log in to another network processor, select Login from the File drop-down menu to open the Login dialog box. ***Note 2:*** The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. If this is the case, select Login from the File drop-down menu in the main window to open the Login dialog box. For more information, see Setting the login preferences on page 2-36.
2	In the Connect Using area, select the Terminal Session radio button.
3	Select Network from the Connection Type drop-down list in the Connection Information area.
4	Select or enter an IP address in the Host Name/Address field.
5	Enter a port number in the Port box. ***Note 1:*** The default port value is 10001. ***Note 2:*** Enter port 10010 if you want to access the BCC CLI or to have a remote login session.
6	Select a value (in seconds) from the Timeout drop-down.
7	If you want to save the current login settings as a new login profile, click Save As, enter a login profile name in the Profile Name field, and click OK.
8	Click Connect to open the Terminal dialog box.

—end—

Procedure 4-2
Starting a terminal session using a modem

In a terminal session, you can connect to a network element or any other type of remote system that supports a VT320, VT220, VT100, or ASCII character-based interface independently of Site Manager.

Step	Action
1	Start Site Manager to open the Login dialog box. See Starting Site Manager on page 2-3. ***Note 1:*** If you have already logged in to a network processor and want to log in to another network processor, select Login from the File drop-down menu to open the Login dialog box. ***Note 2:*** The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. If this is the case, select Login from the File drop-down menu in the main window to open the Login dialog box. For more information, see Setting the login preferences on page 2-36.
2	In the Connect Using area, select the Terminal Session radio button.
3	Select Modem from the Connection Type drop-down list in the Connection Information area.
4	Select or enter a telephone number in the Telephone Number drop-down list.
5	Select a value (in seconds) from the Timeout drop-down list.
6	If you want to define the modem settings, click the Advanced button. See Defining modem settings on page 2-14 for further instructions.
7	If you want to save the current login settings as a new login profile, click Save As, type a login profile name in the Profile name field, and click OK.
8	Click Connect to open the Terminal dialog box.

—end—

Procedure 4-3
Starting a terminal session using direct cable

In a terminal session, you can connect to a network element or any other type of remote system that supports a VT320, VT220, VT100, or ASCII character-based interface independently of Site Manager.

Step	Action
1	Start Site Manager to open the Login dialog box. See Starting Site Manager on page 2-3. ***Note 1:*** If you have already logged in to a network processor and want to log in to another network processor, select Login from the File drop-down menu to open the Login dialog box. ***Note 2:*** The Login Manager dialog box opens automatically upon starting Site Manager if you have changed the default login settings. If this is the case, select Login from the File drop-down menu in the main window to open the Login dialog box. For more information, see Setting the login preferences on page 2-36.
2	In the Connect Using area, select the Terminal Session radio button.
3	Select Direct Cable from the Connection Type drop-down list in the Connection Information area.
4	Select a port number from the Port drop-down list.
5	Select a value (in seconds) from the Timeout drop-down list.
6	If you want to define the cable settings, click the Advanced button. See Defining direct cable settings on page 2-15 for further instructions.
7	If you want to save the current login settings as a new login profile, click Save As, type a login profile name in the Profile name field, and click OK.
8	Click Connect to open the Terminal dialog box.

—end—

Procedure 4-4
Starting a manual connection terminal session

You can connect manually to a network element by selecting the Requires Manual Connection/Secure Modem at Gateway Node check box when you log in to a network element. For instructions, see any of the following procedures:

- Logging in to a network processor using a network connection on page 2-4
- Logging in to a network processor using a modem connection on page 2-7
- Logging in to a network processor using a direct cable connection on page 2-11

—end—

Procedure 4-5 **Starting a Comm Log terminal session**

Use this procedure to start a Comm Log terminal session. The Comm Log terminal is used to track the messages sent between Site Manager and the network elements to which Site Manager is connected.

The Comm Log terminal can store 1000 lines of information. When the maximum log size is reached, the oldest entries are removed to create space for new entries. A Preside UNIX workstation can store 60,000 characters, and a personal computer can store 200,000 characters.

Step	Action
1	Select CommLog from the File drop-down menu to open the Comm Log dialog box.

—end—

Procedure 4-6
Printing the information in the telnet terminal dialog box

Step	Action
1	Select Print from the File drop-down menu.
2	Click OK.

—end—

Procedure 4-7
Printing the Comm Log

Use this procedure to print the comm log.

Step	Action
1	Select Print from the File drop-down menu.
2	Click OK.

—end—

Procedure 4-8
Closing a telnet terminal session

Step	Action
1	Do one of the following: • Select Close from the File drop-down menu. • Click the X button in the top right corner of the Terminal dialog box.
2	Click Yes in the confirmation dialog box.

—end—

Procedure 4-9
Closing a manual connection terminal session

Step	**Action**
1	Do one of the following: • Click Return to Site Manager. • Click Cancel or the X button in the top right corner of the Manual Connection dialog box, and click Yes in the confirmation dialog box.

—end—

Procedure 4-10
Closing a Comm Log session

Step	Action
1	Do one of the following: • Select Close from the File drop-down menu. • Click the X button in the top right corner of the Comm Log dialog box.

—end—

Shelf graphics and inventory

Procedures for shelf graphics and inventory

Procedure 5-1
Displaying shelf graphics

Use this procedure to display a graphical representation of the network element.

Step	**Action**
1	Log in to the network element for which you want to view the Shelf Level View. See Procedures for logging in to a network element on page 2-1.
2	Ensure that the network element is selected in the Navigation Tree.
3	Select Shelf Level View from the Configuration drop-down menu to open the Shelf Level View window. ***Note:*** After the Shelf Level View window appears on the screen, you can open it in a window separate from the main display by selecting Open in New Window from the File drop-down menu, or by right-clicking on the title bar of the Shelf Level View window and selecting Open in New Window from the pop-up menu.
4	Review the information in the Shelf Details area of the Shelf Level View window. ***Note:*** The squares that appear to the right of the Shelf Level View indicate alarms that are raised against non-circuit pack items, such as common equipment, facility, environment, and DS1 service module. You can display information about any of these alarms by right-clicking on a square and selecting Show Alarms from the pop-up menu. The Alarm Filtering dialog box appears.

—end—

Procedure 5-2
Displaying details for a shelf circuit pack

Use this procedure to display information about a circuit pack that is graphically represented in the Shelf Level View window.

Step	Action
1	Display the Shelf Level View for the selected network element. See Displaying shelf graphics on page 5-2.
2	Click on a circuit pack within the Shelf Level View area to select it.
3	Review the circuit pack information in the Selected Circuit Pack Details area. ***Note 1:*** When a new alarm is raised against a circuit pack, an alarm balloon appears on the circuit pack in the Shelf Level View window. You can remove the balloon by right-clicking on it and selecting Clear balloon from the pop-up menu. ***Note 2:*** You can display information about the alarms raised against a circuit pack by right-clicking on the circuit pack in the Shelf Level View display, and selecting Show Alarms from the pop-up menu. The Alarm Filtering dialog box appears.

—end—

Procedure 5-3
Displaying DSM graphics

Use this procedure to display a graphical representation of a DS1 service module (DSM).

> ***Note:*** When displaying a DSM shelf containing a connected, but unprotected DS1 termination module in slot 1 and an unconnected DS1 termination module in slot 2, only the DS1 termination module in slot 1 is displayed.

Step	Action
1	Display the Shelf Level View for the selected network element. See Displaying shelf graphics on page 5-2.
2	Do one of the following: • Click the Show DSM button to open the DSM window, and select an option from the Source drop-down list. • Right-click on an OC-3 or OC-3x4 circuit pack associated with a DSM, and select Show DSM from the pop-up menu to open the DSM window. Then, select an option from the Source drop-down list.
3	Review the graphics display in the DSM window. ***Note:*** The squares that appear to the right of the DSM graphics indicate alarms that are raised against non-circuit pack items, such as DSM-type alarms or environmental alarms. You can display information about any of these alarms by right-clicking on a square and selecting Show Alarms from the pop-up menu. The Alarm Filtering dialog box appears.

—end—

Procedure 5-4
Displaying details for a DSM DS1x84 TM

Use this procedure to display information about a DSM DS1x84 termination module (DSM DS1x84 TM) that is graphically represented in the DS1 service module (DSM) window.

Step	Action
1	Display the graphics for the selected DSM. See Displaying DSM graphics on page 5-4.
2	Click on a DSM DS1x84 TM (DS1TM) within the DSM window to select it.
3	Review the DSM DS1x84 TM information in the Selected DSM circuit pack details area.

Note 1: When a new alarm is raised against a DSM DS1x84 TM, an alarm balloon appears on the DSM DS1x84 TM in the DSM window. You can remove the balloon by right-clicking on it and selecting Clear Balloon from the pop-up menu.

Note 2: You can display information about the alarms raised against a DSM DS1x84 TM by right-clicking on it in the DSM graphics display, and selecting Show Alarms from the pop-up menu. The Active Alarms dialog box appears.

—end—

Procedure 5-5
Performing a lamp test for a DSM

Use this procedure to light up the LEDs on a specific DSM DS1x84 termination module (DSM DS1x84 TM) or the entire shelf and the DS1 service modules (DSMs) associated with it.

Step	**Action**
1	Display the Shelf Level View for the selected network element. See Displaying shelf graphics on page 5-2.
2	Click on the Lamp Test button to open the Lamp Test dialog box.
3	Do one of the following: • from the Equipment drop-down list**,** select a DSM DS1x84 TM (DS1TM) to light up the LEDs on that particular DSM DS1x84 TM • from the Equipment drop-down list, select All to light up the LEDs on the entire shelf and all DSMs associated with it
4	Click OK.

—end—

Procedure 5-6
Displaying equipment and facilities information

Use this procedure to display the equipment and facilities associated with a network element or its DS1 service modules (DSMs).

Step	Action
1	Depending on the type of equipment you want to review, open the Shelf Level View window or the DSM window. See Displaying shelf graphics on page 5-2 or Displaying DSM graphics on page 5-4.
2	Double-click on a provisioned circuit pack within the graphics area of the Shelf Level View window or the DSM window.

The Equipment & Facility Provisioning window opens.

Note 1: You can also open the Equipment & Facility Provisioning window by right-clicking on a circuit pack and selecting Show Equipment & Facilities from the pop-up menu.

Note 2: If you double-click on an unknown circuit pack or a circuit pack with no equipment associated with it, the following message appears in the status area: “There is no equipment associated with this circuit pack.”

Note 3: You can open the Add Equipment dialog box by double-clicking on an empty circuit pack slot within the Shelf Level View area or the DSM graphics area.

—end—

Procedure 5-7
Displaying shelf inventory information

Use this procedure to display inventory information about all equipment that is physically present in a network element.

Step	Action
1	Log in to the network element for which you want to view the shelf inventory data. See Procedures for logging in to a network element on page 2-1.
2	Ensure that the network element is selected in the Navigation Tree.
3	Select Inventory from the Configuration drop-down menu to open the Inventory window.
4	Click on a row in the table to select it.
5	Review the information in the General tab, and click the Engineering tab to view extra information about the selected hardware item.

—end—

Procedure 5-8
Displaying DSM inventory information

Use this procedure to display inventory information about all equipment that is physically present in a provisioned DS1 service module (DSM).

> ***Note:*** When the inventory is retrieved for a DSM shelf containing a connected, but unprotected DS1 termination module in slot 1 and an unconnected DS1 termination module in slot 2, complete inventory details will be displayed for the DS1 termination module in slot 1. Only the serial number is displayed for the DS1 termination module in slot 2.

Step	Action
1	Log in to the network element associated with the DSM. See Procedures for logging in to a network element on page 2-1.
2	Ensure that the network element is selected in the Navigation Tree.
3	Select Inventory from the Configuration drop-down menu to open the Inventory window.
4	If the DSM inventory information is not grouped together, click the Source column header to sort the information.
5	Based on the Site Address displayed in the Source column, find the grouping of DSM inventory.
6	If you want details about a specific DSM DS1x84 TM, click on its respective row in the table.
7	Review the information in the General tab, and click the Engineering tab to view extra information about the selected hardware item.

—end—

Procedure 5-9
Copying inventory information

Use this procedure to copy inventory information to the clipboard. You can paste this information into an application of your choice to view, print, or save to a file.

Step	Action
1	Log in to the network element for which you want to view the shelf inventory data. See Procedures for logging in to a network element on page 2-1.
2	Ensure that the network element is selected in the Navigation Tree.
3	Select Inventory from the Configuration drop-down menu to open the Inventory window.
4	Select information in the Inventory table.
5	Select Copy from the Edit drop-down menu.

A report is generated and placed on the clipboard. The report contains the following information as it appears in the Inventory window:

- column headings
- inventory data, one line per hardware item

Note: Extra columns are added to the clipboard to accommodate the additional DS1 service module (DSM) information displayed below the Inventory table.

—end—

Provisioning data and software management procedures

Procedures for provisioning data and software management

Procedure 6-1
Saving provisioning data from a shelf processor to a local PC

Use this procedure to save the shelf processor provisioning data to a PC that is connected to the shelf processor through direct cable. You can carry out a check before each save to determine if a condition exists that can prevent a save. These conditions include:

- a software upgrade is in progress
- an in-service rollover is in progress
- a database save and restore is in progress
- a duplicate SID exists
- a load mismatch exists. For example, the software version on the shelf processor is different from that on the other circuit packs.
- a Disk Full alarm is raised
- an Alarm and Event Throttling Active alarm is raised

Note: Before you save shelf processor data, make sure you save provisioning changes on all Packet Edge circuit packs in the shelf. Unsaved changes on a Packet Edge circuit pack are lost and a provisioning data lost trap is sent (if enabled) when you restore shelf processor data.

Requirements

To perform this procedure, you must use an account with a level 3 or higher user privilege code (UPC)

Step	Action
1	Create a directory on the PC that will contain the shelf processor provisioning data.
2	Connect the PC directly to the network element through an RS-232 connection. ***Note:*** You cannot complete this procedure if you are logged in to the network element from a remote location.
3	Start a Site Manager session on the PC and log in to the network element. See Procedures for interface login and logout on page 2-1.
4	Ensure that the network element is selected in the navigation tree.
5	Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.

—continued—

Procedure 6-1 (continued)

Saving provisioning data from a shelf processor to a local PC

Step **Action**

6 Select Local Computer from the Storage Type drop-down list.

The local IP address of the computer appears in the IP field.

7 Ensure that the Do not backup or restore if alarms exist on NE check box is selected.

> **CAUTION**
> **Risk of corrupting provisioning data**
> If you perform a save or restore with the Do not backup or restore if alarms exist on NE check box deselected, the following can occur:
>
> - you can save or restore invalid data
> - you can overwrite existing, valid data with invalid data
> - you can restore invalid data that can leave the network element in the wrong state

8 Do one of the following:

- Enter the drive and the directory where the provisioning data will be saved to.
- Click Browse and search for the drive and directory where the provisioning data will be saved to. Select the directory and click OK.

9 In the Backup and Restore window, click Save to Dir to save provisioning data from the shelf processor to the PC.

Note 1: To terminate a save that is in progress, click Cancel.

Note 2: When the Do not backup or restore if alarms exist on NE check box is selected and an alarm exists on the shelf processor, the save fails. One exception is the Database Save and Restore alarm. If this alarm is active on a shelf processor from which an attempt to save provisioning data is pending, the save command clears the alarm before proceeding with saving the data.

10 Wait until a Database save successfully completed message is displayed in the Status area.

—end—

Procedure 6-2
Restoring provisioning data from a local PC to a shelf processor

Use this procedure to restore provisioning data from a local PC to a shelf processor.

CAUTION
Risk of traffic loss
This procedure can affect traffic carried by the network element, including pass-through traffic. All pass-through traffic must be switched away from the network element. A warm restart of all circuit packs occurs as part of the final commit of the provisioning data.

By default, the Do not restore if backup TID does not match NE TID check box is deselected. This means that provisioning data of one shelf processor can be restored to a shelf processor that has a different target identifier (TID).

CAUTION
Risk of incorrect provisioning data
Before a restore procedure, ensure that the restored provisioning data is compatible with the network element. Restoring the wrong provisioning data to the network element can affect traffic through the network. Take all necessary steps to verify the data integrity before committing the data.

Before each restore, ensure there are no conditions that will prevent the restore. These conditions include:

- a software upgrade is in progress
- an in-service rollover is in progress
- a database save and restore is in progress
- a duplicate SID exists
- a load mismatch exists. For example, the software version on the shelf processor is different from that on the other circuit packs.
- a Disk Full alarm is raised
- an Alarm and Event Throttling Active alarm is raised

—continued—

Procedure 6-2 (continued)
Restoring provisioning data from a local PC to a shelf processor

Requirements

The software load in use during a restore must be the same release as the software load used during the save. If not, the restore fails.

To perform this procedure, you must

- use an account with a level 3 or higher user privilege code (UPC)
- connect the PC directly to the network element through an RS-232 connection. You cannot complete this procedure if you are logged in to the network element from a remote location.

Step	Action
1	Log in to the network element. See Procedures for logging in to a network element on page 2-1.
2	Ensure that the network element is selected in the navigation tree.
3	Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.
4	Select Local Computer from the Storage Type drop-down list. The local IP address of the computer appears in the IP field.
5	Ensure that the Do not backup or restore if alarms exist on NE check box is selected.

CAUTION
Risk of corrupting provisioning data
If you perform a save or restore with the Do not backup or restore if alarms exist on NE check box deselected, the following can occur:

- you can save or restore invalid data
- you can overwrite existing, valid data with invalid data
- you can restore invalid data that can leave the network element in the wrong state

—continued—

Procedure 6-2 (continued)
Restoring provisioning data from a local PC to a shelf processor

Step	Action
6	Select the Do not restore if backup TID does not match NE TID check box.
	Note 1: To restore provisioning data from one shelf processor to a different shelf processor, ensure that the Do not restore if backup TID does not match NE TID check box is not selected. Otherwise, the restore fails.
	Note 2: There is no confirmation that the configuration in the restored provisioning data is compatible with the network element configuration. To restore provisioning data to a different network element can result in an improperly provisioned network.
7	Do one of the following:
	• Enter the drive and the directory from which the provisioning data will be restored.
	• Click Browse and search for the drive and directory containing the file that contains the provisioning data. Select the backup file and click Open.
8	Click Restore from Dir to restore provisioning data from the PC to the shelf processor.
	Note 1: A Database Restore in Progress alarm is raised.
	Note 2: To terminate a restore that is in progress, click Cancel.
	Note 3: When the Do not backup or restore if alarms exist on NE check box is selected and an alarm exists on the shelf processor, the restore fails.
	Note 4: If the software version in use during the save is different from that in use during the restore, the restore fails.
9	Click Commit.
	Note: Any mention of DSM slots 19 through 58 in the response block (for data transfer validation), are in fact references to DSM extension slots. These DSM slot references will appear whether or not a DSM is installed.
10	Wait until a Database restore successfully completed message is displayed in the Status area.

—end—

Procedure 6-3
Saving provisioning data from a shelf processor to a network processor

Use this procedure to save the provisioning data from a shelf processor to a network processor.

You can carry out a check before each save to determine if a condition exists that can prevent a save. These conditions include:

- a software upgrade is in progress
- an in-service rollover is in progress
- a database save and restore is in progress
- a duplicate SID exists
- a load mismatch exists. For example, the software version on the shelf processor is different from that on the other circuit packs.
- a Disk Full alarm is raised
- an Alarm and Event Throttling Active alarm is raised

> ***Note:*** Before you save shelf processor data, make sure you save provisioning changes on all Packet Edge circuit packs in the shelf. Unsaved changes on a Packet Edge circuit pack are lost and a provisioning data lost trap is sent (if enabled) when you restore shelf processor data.

Requirements

To save shelf processor provisioning data to a network processor, the shelf processor must be in the span of control of the network processor that will contain the provisioning data. If the shelf processor is not in the network processor span of control, the save fails.

To perform this procedure, you must use an account with a level 3 or higher user privilege code (UPC).

Step	Action
1	Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.
2	Log in to the network element. See Procedures for logging in to a network element on page 2-1.
3	Ensure that the network element is selected in the Navigation Tree.

—continued—

Procedure 6-3 (continued)
Saving provisioning data from a shelf processor to a network processor

Step **Action**

4 Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.

5 Ensure that NP appears in the Storage Type drop-down.

6 Ensure that the Do not backup or restore if alarms exist on NE check box is selected.

> **CAUTION**
> **Risk of corrupting provisioning data**
> If you perform a save or restore with the Do not backup or restore if alarms exist on NE check box deselected, the following can occur:
>
> - you can save or restore invalid data
> - you can overwrite existing, valid data with invalid data
> - you can restore invalid data that can leave the network element in the wrong state

7 In the NP TID field, enter the target identifier code of the network processor you are saving to.

Note: The name of the directory in which the backup file will be stored appears automatically in the Directory field.

8 Click Save to NP to save provisioning data from the shelf processor to the network processor.

Note 1: To terminate a save that is in progress, click Cancel.

Note 2: When the Do not backup or restore if alarms exist on NE check box is selected and an alarm exists on the shelf processor, the save fails. One exception is the Database Save and Restore alarm. If this alarm is active on a shelf processor from which an attempt to save provisioning data is pending, the save command clears the alarm before proceeding with saving the data.

9 Wait until a Database save successfully completed message is displayed in the Status area.

—end—

Procedure 6-4
Restoring provisioning data from a network processor to a shelf processor

Use this procedure to restore provisioning data from a network processor to a shelf processor.

> **CAUTION**
> **Risk of traffic loss**
> This procedure can affect traffic carried by the network element, including pass-through traffic. All pass-through traffic must be switched away from the network element. A warm restart of all circuit packs occurs as part of the final commit of the provisioning data.

By default, the Do not restore if backup TID does not match NE TID check box is deselected. This means that provisioning data of one shelf processor can be restored to a shelf processor that has a different target identifier (TID).

> **CAUTION**
> **Risk of incorrect provisioning data**
> Before a restore procedure, ensure that the restored provisioning data is compatible with the network element. Restoring the wrong provisioning data to the network element can affect traffic through the network. Take all necessary steps to verify the data integrity before committing the data.

Before each restore, ensure there are no conditions that will prevent the restore. These conditions include:

- a software upgrade is in progress
- an in-service rollover is in progress
- a database save and restore is in progress
- a duplicate SID exists
- a load mismatch exists. For example, the software version on the shelf processor is different from that on the other circuit packs.
- a Disk Full alarm is raised
- an Alarm and Event Throttling Active alarm is raised

—continued—

Procedure 6-4 (continued)
Restoring provisioning data from a network processor to a shelf processor

Requirements

The software load in use during a restore must be the same release as the software load used during the save. Otherwise, the restore fails.

When you restore network processor provisioning data from an external repository, you cannot add or remove any network elements in the network processor span of control before the restore is complete.

To perform this procedure, you must use an account with a level 3 or higher user privilege code (UPC).

Step **Action**

1 Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.

2 Log in to the network element. See Procedures for logging in to a network element on page 2-1.

3 Ensure that the network element is selected in the Navigation Tree.

4 Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.

5 Ensure that NP appears in the Storage Type drop-down list.

6 Ensure that the Do not backup or restore if alarms exist on NE check box is selected.

> ⚠ **CAUTION**
> **Risk of corrupting provisioning data**
> If you perform a save or restore with the Do not backup or restore if alarms exist on NE check box deselected, the following can occur:
>
> - you can save or restore invalid data
> - you can overwrite existing, valid data with invalid data
> - you can restore invalid data that can leave the network element in the wrong state

—continued—

Procedure 6-4 (continued)
Restoring provisioning data from a network processor to a shelf processor

Step	Action
7	Select the Do not restore if backup TID does not match NE TID check box. ***Note 1:*** To restore provisioning data from one shelf processor to a different shelf processor, ensure that the Do not restore if backup TID does not match NE TID check box is not selected. Otherwise, the restore fails. ***Note 2:*** There is no confirmation that the configuration in the restored provisioning data is compatible with the network element configuration. To restore provisioning data to a different network element can result in an improperly provisioned network.
8	In the NP TID field, enter the target identifier code of the network processor you are restoring from.
9	In the Directory field, enter the directory and the name of the backup file. ***Note:*** If you do not know where the backup file is being stored, select the network processor in the navigation tree, and click View Backups in the Save and Restore window to open the SP Backups on NP dialog box. The SP Backups on NP dialog box provides information about the backup files and their storage location. For more information, see Retrieving a list of shelf processor provisioning data backups on page 6-45.
10	Click Restore from NP to restore provisioning data from the network processor to the shelf processor. ***Note 1:*** A Database Restore in Progress alarm is raised. ***Note 2:*** To terminate a restore that is in progress, click Cancel. ***Note 3:*** When the Do not backup or restore if alarms exist on NE check box is selected and an alarm exists on the shelf processor, the restore fails. ***Note 4:*** If the software version in use during the save is different from that in use during the restore, the restore fails.
11	Click Commit. ***Note:*** Any mention of DSM slots 19 through 58 in the response block (for data transfer validation), are in fact references to DSM extension slots. These DSM slot references will appear whether or not a DSM is installed.
12	Wait until a Database restore successfully completed message is displayed in the Status area.

—end—

Procedure 6-5
Saving provisioning data from all shelf processors in a span of control to the network processor

You can carry out a check before each save to determine if a condition exists that can prevent a save. These conditions include:

- a software upgrade is in progress
- an in-service rollover is in progress
- a database save and restore is in progress
- a duplicate SID exists
- a load mismatch exists. For example, the software version on the shelf processor is different from that on the other circuit packs.
- a Disk Full alarm is raised
- an Alarm and Event Throttling Active alarm is raised

Note: Before you save shelf processor data, make sure you save provisioning changes on all Packet Edge circuit packs in the shelf. Unsaved changes on a Packet Edge circuit pack are lost and a provisioning data lost trap is sent (if enabled) when you restore shelf processor data.

Requirements

To save shelf processor provisioning data to a network processor, the shelf processor must be in the span of control of the network processor that will contain the provisioning data. The network processor backs up only shelf processors that are in its span of control.

When you save network processor provisioning data to an external repository, you cannot add or remove any network elements in the network processor span of control before the save is complete.

To perform this procedure, you must use an account with a level 3 or higher user privilege code (UPC).

Step **Action**

1 Log in to the network processor to which you will save the provisioning data. See Procedures for logging in to a network processor on page 2-1.

Note: The only supported destination of the span of control provisioning data is the network processor in control.

2 Ensure that the network processor is selected in the Navigation Tree.

—continued—

Procedure 6-5 (continued)

Saving provisioning data from all shelf processors in a span of control to the network processor

Step **Action**

3 Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.

The NP is displayed in the Storage Type drop-down list by default.

4 Ensure that the Do not backup or restore if alarms exist on NE check box is selected.

> **CAUTION**
>
> **Risk of corrupting provisioning data**
>
> If you perform a save or restore with the Do not backup or restore if alarms exist on NE check box deselected, the following can occur:
>
> - you can save or restore invalid data
> - you can overwrite existing, valid data with invalid data
> - you can restore invalid data that can leave the network element in the wrong state

5 Click Save All SPs to NP.

Note 1: To terminate a save that is in progress, click Cancel. Any shelf processor saves that are complete are not affected.

Note 2: When the Do not backup or restore if alarms exist on NE check box is selected and an alarm exists on a shelf processor, the save fails.

Note 3: If a save from one or more shelf processors fails, the saves from all remaining shelf processors in the span of control continue. If a SOC Database Save Failed message is displayed in the Status box, see Saving provisioning data from a shelf processor to a network processor on page 6-8 to save the failed shelf processor(s) individually without affecting the saved shelf processors.

6 Wait until a Database save successfully completed message is displayed in the Status area.

—end—

Procedure 6-6
Saving provisioning data from a shelf processor directly to a remote location

Use this procedure to save the data of a single shelf processor in an NP span of control and store it directly in a remote location with a TID or IP address. You can carry out a check before each save to determine if a condition exists that can prevent a save. These conditions include:

- upgrade in progress
- in-service rollover on the shelf processor
- reconfiguration or BLSR configuration in progress
- provisioning of data in progress
- FPGA download in progress
- transmit data recovery failed
- SP version or loads mismatch
- database corruption
- load install
- disk full
- shelf ID mismatch
- duplicate SID on the shelf processor or network processor
- database save and restore in progress
- exclusion lock on the save and restore directory
- remote destination is not reachable with the given user name and password from the network processor if the destination information is provided
- an Alarm and Event Throttling Active alarm is raised

Note: Before you save shelf processor data, make sure you save provisioning changes on all Packet Edge circuit packs in the shelf. Unsaved changes on a Packet Edge circuit pack are lost and a provisioning data lost trap is sent (if enabled) when you restore shelf processor data.

Requirements

To save shelf processor provisioning data to a remote location, the shelf processor must be in the span of control of a network processor.

To perform this procedure, you must use an account with a level 3 or higher user privilege code (UPC).

—continued—

Procedure 6-6 (continued)

Saving provisioning data from a shelf processor directly to a remote location

Step	Action
1	Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.
2	Ensure the network element with the target shelf processor is selected in the Navigation Tree.
3	Start a TL1 Command Builder session. See Procedures for using the TL1 Command Builder on page 7-1.
4	Check the shelf processor for conditions that can prevent a save by entering

```
CHK-PROV-SP:[TID]::CTAG::[USERID][,PASSWRD]:
[TRGTID=Domain][,DESTTYPE=Domain],[DESTADDR=Domain]
[,DIR=Domain][,CHKALM=Domain];
```

For more information about this TL1 command, see *TL1 Reference-Part 1 of 4*, 323-1059-190.

Step	Action
5	Click Run Command.
6	Wait until a completed message is displayed in the Status area.
7	Save the shelf processor provisioning data by entering

```
SAV-PROV-SP:[TID]::CTAG::[USERID][,PASSWRD]:[DESTTYPE=Do
main][,DESTADDR=Domain][,DIR=Domain][,CHKALM=Domain];
```

For more information about this TL1 command, see *TL1 Reference-Part 1 of 4*, 323-1059-190.

Step	Action
8	Click Run Command.
9	Wait until a completed message is displayed in the Status area.

Note: To terminate a save in progress, enter the following command:

```
CANC-PROV-SP:[TID]::CTAG:::[TRGTID=Domain];
```

For more information about this TL1 command, see *TL1 Reference-Part 1 of 4*, 323-1059-190.

—end—

Procedure 6-7
Restoring provisioning data from a remote location directly to a shelf processor

Perform this procedure to restore provisioning data from a remote location (with a TID or IP address) directly to a shelf processor.

You can carry out a check before each restore to determine if a condition exists that can prevent a restore. These conditions include:

- upgrade in progress
- in-service rollover on the shelf processor
- reconfiguration or BLSR configuration in progress
- provisioning of data in progress
- FPGA download in progress
- transmit data recovery failed
- SP version mismatch
- loads mismatch
- database corruption
- load install
- disk full
- shelf ID mismatch
- duplicate SID on the SP or NP
- database save and restore in progress
- exclusion lock on the save and restore directory
- remote destination is not reachable with the given user name and password from the NP if the destination information is provided
- an Alarm and Event Throttling Active alarm is raised

Requirements

To restore provisioning data from a remote location directly to a shelf processor, the shelf processor must be in the span of control of a network processor.

To perform this procedure, you must use an account with a level 3 or higher user privilege code (UPC).

—continued—

Procedure 6-7 (continued)

Restoring provisioning data from a remote location directly to a shelf processor

Step	Action
1	Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.
2	Ensure the network element with the target shelf processor is selected in the Navigation Tree.
3	Start a TL1 Command Builder session. See Procedures for using the TL1 Command Builder on page 7-1.
4	Check the shelf processor for conditions that can prevent a restore by entering `CHK-PROV-SP:[TID]::CTAG::[USERID][,PASSWRD]:[TRGTID=Domain][,DESTTYPE=Domain],[DESTADDR=Domain][,DIR=Domain][,CHKALM=Domain];` For more information about this TL1 command, see *TL1 Reference-Part 1 of 4*, 323-1059-190.
5	Click Run Command.
6	Wait until a completed message is displayed in the Result area.
7	Restore the shelf processor provisioning data by entering `RST-PROV-SP:[TID]::CTAG::[USERID],[PASSWD]:[TRGTID=Domain][,DESTTYPE=Domain][,DESTADDR=Domain][,DIR=Domain][,CHKTID=Domain][,CHKALM=Domain];` For more information about this TL1 command, see *TL1 Reference-Part 1 of 4*, 323-1059-190.
8	Click Run Command.
9	Wait until a completed message is displayed in the Result area. ***Note:*** To terminate a restore in progress, enter the following command: `CANC-PROV-SP:[TID]::CTAG:::[TRGTID=Domain];` For more information about this TL1 command, see *TL1 Reference-Part 1 of 4*, 323-1059-190.
10	Commit the provisioning data to the shelf processor by entering `CMMT-PROV-SP:[TID]::CTAG:::[TRGTID=Domain];` For more information about this TL1 command, see *TL1 Reference-Part 1 of 4*, 323-1059-190.
11	Wait until a completed message is displayed in the Result area.

—end—

Procedure 6-8
Saving provisioning data from a network processor to a remote PC that has an FTP server running

Use this procedure to save provisioning data from a network processor to a remote computer that is running a stand-alone FTP server.

You can check the network processor before each save to determine if a condition exists that can prevent a save. These conditions include:

- a software upgrade is in progress
- a database save and restore is in progress
- a duplicate SID exists
- a load mismatch exists. For example, the software version on the network processor is different from that on the shelf processor.
- a Disk Full alarm is raised
- a Corrupt Network Backup alarm is raised on the network processor. This alarm prevents any save except for a save of all shelf processors in a span of control to a network processor.
- an Alarm and Event Throttling Active alarm is raised

Requirements

When you save network processor provisioning data to an external repository, you cannot add or remove any network elements in the network processor span of control before the save is complete.

To perform this procedure, you must

- use an account with a level 3 or higher user privilege code (UPC)
- use a PC that has a stand-alone FTP server running

Step	**Action**
1	Create a directory on the PC that will contain the network processor provisioning data.
2	Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.
3	Ensure that the network processor is selected in the Navigation Tree.
4	Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.
5	Select Remote Computer from the Storage Type drop-down list.

—continued—

Procedure 6-8 (continued)

Saving provisioning data from a network processor to a remote PC that has an FTP server running

Step **Action**

6 Ensure that the Do not backup or restore if alarms exist on NE check box is selected.

> **CAUTION**
>
> **Risk of corrupting provisioning data**
>
> If you perform a save or restore with the Do not backup or restore if alarms exist on NE check box deselected, the following can occur:
>
> - you can save or restore invalid data
> - you can overwrite existing, valid data with invalid data
> - you can restore invalid data that can leave the network element in the wrong state

7 In the IP field, enter the IP address of the remote PC.

8 Enter the drive and the directory where the provisioning data will be saved to.

9 Click Save to Dir to save provisioning data from the network processor to the PC.

10 In the Remote Login dialog box that appears, enter your user ID and password to the remote PC, and click Login.

Note 1: To terminate a save that is in progress, click Cancel.

Note 2: When the Do not backup or restore if alarms exist on NE check box is selected and an alarm exists on the network processor, the save fails.

11 Wait until a Database save successfully completed message is displayed in the Status area.

—end—

Procedure 6-9
Restoring provisioning data to a network processor from a remote PC that has an FTP server running

Use this procedure to restore provisioning data from a remote PC to a network processor.

CAUTION
Risk of traffic loss
This procedure can affect traffic carried by the network element, including pass-through traffic. All pass-through traffic must be switched away from the network element. A warm restart of all circuit packs occurs as part of the final commit of the provisioning data.

By default, the Do not restore if backup TID does not match NE TID check box is deselected. This means that provisioning data of one network processor can be restored to a shelf processor or network processor that has a different target identifier (TID).

CAUTION
Risk of incorrect provisioning data
Before a restore procedure, ensure that the restored provisioning data is compatible with the network element. Restoring the wrong provisioning data to the network element can affect traffic through the network. Take all necessary steps to verify the data integrity before committing the data.

Before each restore, ensure there are no conditions that will prevent the restore. These conditions include:

- a software upgrade in progress
- a database save and restore is in progress
- a duplicate SID exists
- a load mismatch exists. For example, the software version on the network processor is different from that on the shelf processor.
- a Disk Full alarm is raised
- an Alarm and Event Throttling Active alarm is raised

—continued—

Procedure 6-9 (continued)
Restoring provisioning data to a network processor from a remote PC that has an FTP server running

Requirements

The software load in use during a restore must be the same release as the software load used during the save. Otherwise, the restore fails.

When you restore network processor provisioning data from an external repository, you cannot add or remove any network elements in the network processor span of control before the restore is complete.

To perform this procedure, you must

- use an account with a level 3 or higher user privilege code (UPC)
- use a PC that has a stand-alone FTP server running

Step	Action
1	Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.
2	Ensure that the network processor is selected in the Navigation Tree.
3	Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.
4	Select Remote Computer from the Storage Type drop-down list.
5	Ensure that the Do not backup or restore if alarms exist on NE check box is selected.

CAUTION
Risk of corrupting provisioning data
If you perform a save or restore with the Do not backup or restore if alarms exist on NE check box deselected, the following can occur:

- you can save or restore invalid data
- you can overwrite existing, valid data with invalid data
- you can restore invalid data that can leave the network element in the wrong state

Step	Action
6	In the IP field, enter the IP address of the remote PC.
7	Enter the drive and the directory from which the provisioning data will be restored.

—continued—

Procedure 6-9 (continued)

Restoring provisioning data to a network processor from a remote PC that has an FTP server running

Step	Action
8	Click Restore from Dir.
9	In the Remote Login dialog box that appears, enter your user ID and password to the remote PC, and click Login. ***Note 1:*** A Database Restore in Progress alarm is raised. ***Note 2:*** To terminate a restore that is in progress, click Cancel. ***Note 3:*** When the Do not backup or restore if alarms exist on NE check box is selected and an alarm exists on the network processor, the restore fails. ***Note 4:*** If the software version in use during the save is different from that in use during the restore, the restore fails.
10	Click Commit. ***Note:*** Any mention of DSM slots 19 through 58 in the response block (for data transfer validation), are in fact references to DSM extension slots. These DSM slot references will appear whether or not a DSM is installed.
11	Wait until a Database restore successfully completed message is displayed in the Status area.
12	Click OK in the confirmation dialog box.
13	Click OK in the warning dialog box to disconnect communications. The connection will be lost. Wait for 5 minutes before you log back in to the network processor.

—end—

Procedure 6-10 **Saving provisioning data from a network processor to a UNIX workstation**

Use this procedure to save provisioning data from a network processor to a UNIX workstation. The provisioning data includes the provisioning files that are saved to the network processor from shelf processors within its span of control (SOC).

You can check the network processor before each save to determine if a condition exists that can prevent a save. These conditions include:

- a software upgrade is in progress
- a database save and restore is in progress
- a duplicate SID exists
- a load mismatch exists. For example, the software version on the network processor is different from that on the shelf processor.
- a Disk Full alarm is raised
- a Corrupt Network Backup alarm is raised on the network processor. This alarm prevents any save except for a save of all shelf processors in a span of control to a network processor.
- an Alarm and Event Throttling Active alarm is raised

Requirements

To perform this procedure, you must use an account with a level 3 or higher user privilege code (UPC).

Step	Action
1	Create a directory on the UNIX workstation for the network processor provisioning data.
2	Log in to the network processor that contains the provisioning data. See Procedures for logging in to a network processor on page 2-1.
3	Ensure that the network processor is selected in the Navigation Tree.
4	Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.
5	Select Remote Computer from the Storage Type drop-down list.

—continued—

Procedure 6-10 (continued)

Saving provisioning data from a network processor to a UNIX workstation

Step **Action**

6 Ensure that the Do not backup or restore if alarms exist on NE check box is selected.

> **CAUTION**
>
> **Risk of corrupting provisioning data**
>
> If you perform a save or restore with the Do not backup or restore if alarms exist on NE check box deselected, the following can occur:
>
> - you can save or restore invalid data
> - you can overwrite existing, valid data with invalid data
> - you can restore invalid data that can leave the network element in the wrong state

7 In the IP field, enter an IP address of the UNIX workstation to which the provisioning data will be saved.

8 In the Directory field, enter the full path and name of the directory that you created in step 1.

9 In the Backup and Restore window, click Save to Dir to save the provisioning data from the network processor to the UNIX workstation.

10 In the Remote Login dialog box that appears, enter your user ID and password to the UNIX workstation, and click Login.

Note 1: A Database Save in Progress alarm is raised.

Note 2: To terminate a save that is in progress, click Cancel.

Note 3: When the Do not backup or restore if alarms exist on NE check box is selected and an alarm exists on the network processor, the save fails.

Note 4: When you save network processor provisioning data to an external repository, you cannot add or remove any network elements in the network processor span of control before the save is complete.

11 Wait until a Database save successfully completed message is displayed in the Status area.

—end—

Procedure 6-11
Restoring provisioning data from a UNIX workstation to a network processor

Use this procedure to restore provisioning data from a UNIX workstation to a network processor.

CAUTION
Risk of traffic loss
This procedure can affect traffic carried by the network element, including pass-through traffic. All pass-through traffic must be switched away from the network element. A warm restart of all circuit packs occurs as part of the final commit of the provisioning data.

By default, the Do not restore if backup TID does not match NE TID check box is deselected. This means that provisioning data of one network processor can be restored to a shelf processor or network processor that has a different target identifier (TID).

CAUTION
Risk of incorrect provisioning data
Before a restore procedure, ensure that the restored provisioning data is compatible with the network element. Restoring the wrong provisioning data to the network element can affect traffic through the network. Take all necessary steps to verify the data integrity before committing the data.

Before each restore, ensure there are no conditions that will prevent the restore. These conditions include:

- a software upgrade in progress
- a database save and restore is in progress
- a duplicate SID exists
- a load mismatch exists. For example, the software version on the network processor is different from that on the shelf processor.
- a Disk Full alarm is raised
- an Alarm and Event Throttling Active alarm is raised

—continued—

Procedure 6-11 (continued)
Restoring provisioning data from a UNIX workstation to a network processor

Requirements

The software load in use during a restore must be the same release as the software load used during the save. Otherwise, the restore fails.

When you restore network processor provisioning data from an external repository, you cannot add or remove any network elements in the network processor span of control before the restore is complete.

To perform this procedure, you must use an account with a level 3 or higher user privilege code (UPC).

Step **Action**

1 Log in to the network processor to which you will restore the provisioning data. See Procedures for logging in to a network processor on page 2-1.

2 Ensure that the network processor is selected in the Navigation Tree.

3 Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.

4 Select Remote Computer from the Storage Type drop-down list.

5 Ensure that the Do not backup or restore if alarms exist on NE check box is selected.

> **CAUTION**
> **Risk of corrupting provisioning data**
> If you perform a save or restore with the Do not backup or restore if alarms exist on NE check box deselected, the following can occur:
>
> - you can save or restore invalid data
> - you can overwrite existing, valid data with invalid data
> - you can restore invalid data that can leave the network element in the wrong state

—continued—

Procedure 6-11 (continued)

Restoring provisioning data from a UNIX workstation to a network processor

Step Action

6 Select the Do not restore if backup TID does not match NE TID check box to prevent the provisioning data from one network processor being restored to a different network processor.

Note 1: To restore provisioning data from one network processor to a different network processor, ensure that the Do not restore if backup TID does not match NE TID check box is not selected. Otherwise, the restore fails.

Note 2: There is no confirmation that the configuration in the restored provisioning data is compatible with the network element configuration. If you restore incompatible provisioning data, the network processor facilities can be incorrectly provisioned and the wrong span of control can be monitored.

7 In the IP field, enter an IP address of the UNIX workstation from which the provisioning data will be restored.

8 In the Directory field, enter the full path and name of the directory that contains the provisioning data.

9 Click Restore from Dir to restore the provisioning data from the UNIX workstation to the network processor, and click OK in the warning dialog box.

10 In the Remote Login dialog box that appears, enter your user ID and password to the UNIX workstation, and click Login.

Note 1: A Database Restore in Progress alarm is raised.

Note 2: To terminate a restore that is in progress, click Cancel.

Note 3: When the Do not backup or restore if alarms exist on NE check box is selected and an alarm exists on the network processor, the restore fails.

Note 4: If the software version in use during the save is different from that in use during the restore, the restore fails.

11 Click Commit.

Note: Any mention of DSM slots 19 through 58 in the response block (for data transfer validation), are in fact references to DSM extension slots. These DSM slot references will appear whether or not a DSM is installed.

12 Wait until a Database restore successfully completed message is displayed in the Status area.

13 Click OK in the Restore warning dialog box.

14 Click OK in the Message warning dialog box.

15 Click OK in the Connection Lost dialog box.

A restart occurs.

—end—

Procedure 6-12
Saving provisioning data from a network processor to a local PC using an Ethernet connection

Use this procedure to save provisioning data from a network processor to a local PC that is connected to the system through an Ethernet connection. The provisioning data includes the provisioning files that are saved to the network processor from shelf processors within its span of control (SOC).

You can check the network processor before each save to determine if a condition exists that can prevent a save. These conditions include:

- a software upgrade is in progress
- a database save and restore is in progress
- a duplicate SID exists
- a load mismatch exists. For example, the software version on the network processor is different from that on the shelf processor.
- a Disk Full alarm is raised
- a Corrupt Network Backup alarm is raised on the network processor. This alarm prevents any save except for a save of all shelf processors in a span of control to a network processor.
- an Alarm and Event Throttling Active alarm is raised

Requirements

When you save network processor provisioning data to an external repository, you cannot add or remove any network elements in the network processor span of control before the save is complete.

To perform this procedure, you must:

- connect the PC to the system through an Ethernet connection
- use an account with a level 3 or higher user privilege code (UPC)

Step	Action
1	Create a directory on the PC that will contain the network processor provisioning data.
2	Log in to the network processor that contains the provisioning data. See Procedures for logging in to a network processor on page 2-1.
3	Ensure that the network processor is selected in the Navigation Tree.
4	Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.

—continued—

Procedure 6-12 (continued)

Saving provisioning data from a network processor to a local PC using an Ethernet connection

Step **Action**

5 Select Local Computer from the Storage Type drop-down list.

The IP address of the PC appears in the IP field.

6 Ensure that the Do not backup or restore if alarms exist on NE check box is selected.

> ⚠ **CAUTION**
>
> **Risk of corrupting provisioning data**
>
> If you perform a save or restore with the Do not backup or restore if alarms exist on NE check box deselected, the following can occur:
>
> - you can save or restore invalid data
> - you can overwrite existing, valid data with invalid data
> - you can restore invalid data that can leave the network element in the wrong state

7 Do one of the following:

- In the Directory field, enter the drive and the directory to which the provisioning data will be saved.
- Click Browse and search for the drive and directory to which the provisioning data will be saved. Select the directory and click OK.

8 Click Save to Dir to save the provisioning data from the network processor to the PC.

Note 1: To terminate a save that is in progress, click Cancel.

Note 2: When the Do not backup or restore if alarms exist on NE check box is selected and an alarm exists on the network processor, the save fails.

9 Wait until a Database save successfully completed message is displayed in the Status area.

—end—

Procedure 6-13
Restoring provisioning data from a local PC to a network processor using an Ethernet connection

Use this procedure to restore provisioning data to a network processor from a local PC that is connected to the system through an Ethernet connection.

CAUTION
Risk of traffic loss
This procedure can affect traffic carried by the network element, including pass-through traffic. All pass-through traffic must be switched away from the network element. A warm restart of all circuit packs occurs as part of the final commit of the provisioning data.

By default, the Do not restore if backup TID does not match NE TID check box is deselected. This means that provisioning data of one network processor can be restored to a shelf processor or network processor that has a different target identifier (TID).

CAUTION
Risk of incorrect provisioning data
Before a restore procedure, ensure that the restored provisioning data is compatible with the network element. Restoring the wrong provisioning data to the network element can affect traffic through the network. Take all necessary steps to verify the data integrity before committing the data.

Before each restore, ensure there are no conditions that will prevent the restore. These conditions include:

- a software upgrade in progress
- a database save and restore is in progress
- a duplicate SID exists
- a load mismatch exists. For example, the software version on the network processor is different from that on the shelf processor.
- a Disk Full alarm is raised
- an Alarm and Event Throttling Active alarm is raised

—continued—

Procedure 6-13 (continued)
Restoring provisioning data from a local PC to a network processor using an Ethernet connection

Requirements

The software load in use during a restore must be the same release as the software load used during the save. Otherwise, the restore fails.

When you restore network processor provisioning data from an external repository, you cannot add or remove any network elements in the network processor span of control before the restore is complete.

To perform this procedure, you must use an account with a level 3 or higher user privilege code (UPC).

Step **Action**

1 Log in to the network processor to which you will restore the provisioning data. See Procedures for logging in to a network processor on page 2-1.

2 Ensure that the network processor is selected in the Navigation Tree.

3 Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.

4 Select Local Computer from the Storage Type drop-down list.

The IP address of the PC appears in the IP field.

5 Ensure that the Do not backup or restore if alarms exist on NE check box is selected.

> **CAUTION**
> **Risk of corrupting provisioning data**
> If you perform a save or restore with the Do not backup or restore if alarms exist on NE check box deselected, the following can occur:
>
> - you can save or restore invalid data
> - you can overwrite existing, valid data with invalid data
> - you can restore invalid data that can leave the network element in the wrong state

—continued—

Procedure 6-13 (continued)

Restoring provisioning data from a local PC to a network processor using an Ethernet connection

Step	**Action**
6	Select the Do not restore if backup TID does not match NE TID check box to prevent the provisioning data from one network processor being restored to a different network processor. ***Note 1:*** To restore provisioning data from one network processor to a different network processor, ensure that the Do not restore if backup TID does not match NE TID check box is not selected. Otherwise, the restore fails. ***Note 2:*** There is no confirmation that the configuration in the restored provisioning data is compatible with the network element configuration. If you restore incompatible provisioning data, the network processor facilities can be incorrectly provisioned and the wrong span of control can be monitored.
7	Do one of the following: • In the Directory field, enter the drive and the directory from which the provisioning data will be restored. • Click Browse and search for the drive and directory containing the file with the provisioning data. Select the backup file and click Open.
8	Click Restore from Dir to restore the provisioning data from the PC to the network processor.
9	Click OK in the Restore warning dialog box. ***Note 1:*** A Database Restore in Progress alarm is raised. ***Note 2:*** To terminate a restore that is in progress, click Cancel. ***Note 3:*** When the Do not backup or restore if alarms exist on NE check box is selected and an alarm exists on the network processor, the restore fails. ***Note 4:*** If the software version in use during the save is different from that in use during the restore, the restore fails.
10	Click Commit. ***Note:*** Any mention of DSM slots 19 through 58 in the response block (for data transfer validation), are in fact references to DSM extension slots. These DSM slot references will appear whether or not a DSM is installed.
11	Wait until a Database restore successfully completed message is displayed in the Status area.
12	Click OK in the Restore warning dialog box.
13	Click OK in the Message warning dialog box.
14	Click OK in the Connection Lost dialog box. A restart occurs.

—end—

Procedure 6-14
Saving provisioning data from a network processor to an OPC over an OSI link

Use this procedure to save provisioning data from a network processor to an operations controller (OPC). The provisioning data includes the provisioning files that are saved to the network processor from shelf processors within its span of control (SOC).

You can check the network processor before each save to determine if a condition exists that can prevent a save. These conditions include:

- a software upgrade is in progress
- a database save and restore is in progress
- a duplicate SID exists
- a load mismatch exists. For example, the software version on the network processor is different from that on the shelf processor.
- a Disk Full alarm is raised
- a Corrupt Network Backup alarm is raised on the network processor. This alarm prevents any save except for a save of all shelf processors in a span of control to a network processor.
- an Alarm and Event Throttling Active alarm is raised

Requirements

When you save network processor provisioning data to an external repository, you cannot add or remove any network elements in the network processor span of control before the save is complete.

To perform this procedure, you must:

- establish an Open Systems Interconnection (OSI) link between the OPTera Metro 3500 system and the system that includes the OPC
- use an account with a level 3 or higher user privilege code (UPC)

Step	Action
1	Create a directory on the OPC that will contain the network processor provisioning data. ***Note:*** Directories must be created in the users/VFS/ folder on the OPC. The directories must be made available to the FTAM user group, or the save fails.
2	Log in to the network processor that contains the provisioning data. See Procedures for logging in to a network processor on page 2-1.

—continued—

Procedure 6-14 (continued)

Saving provisioning data from a network processor to an OPC over an OSI link

Step **Action**

3 Ensure that the network processor is selected in the Navigation Tree.

4 Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.

5 Select OPC from the Storage Type drop-down list.

6 Ensure that the Do not backup or restore if alarms exist on NE check box is selected.

> **CAUTION**
>
> **Risk of corrupting provisioning data**
>
> If you perform a save or restore with the Do not backup or restore if alarms exist on NE check box deselected, the following can occur:
>
> - you can save or restore invalid data
> - you can overwrite existing, valid data with invalid data
> - you can restore invalid data that can leave the network element in the wrong state

7 In the TID (Target ID) field, enter the name of the OPC to which you will save the provisioning data.

8 In the Directory field, enter the sub-path to the directory that you created in step 1.

Note: Do not type /users/VFS/ but only the sub-path to the created directory. For example, if the directory that you created in step 1 is called “prov,” then you must type /prov in the Directory field. You must not type /users/VFS/prov.

9 Click Save to Dir to save the provisioning data from the network processor to the OPC.

10 In the OPC Login dialog box that appears, enter your user ID and password to the OPC, and click OK.

Note 1: To terminate a save that is in progress, click Cancel.

Note 2: When the Do not backup or restore if alarms exist on NE check box is selected and an alarm exists on the network processor, the save fails.

11 Wait until a Database save successfully completed message is displayed in the Status area.

—end—

Procedure 6-15
Restoring provisioning data from an OPC to a network processor over an OSI link

Use this procedure to restore provisioning data from an operations controller (OPC) to a network processor.

> **CAUTION**
> **Risk of traffic loss**
> This procedure can affect traffic carried by the network element, including pass-through traffic. All pass-through traffic must be switched away from the network element. A warm restart of all circuit packs occurs as part of the final commit of the provisioning data.

By default, the Do not restore if backup TID does not match NE TID check box is deselected. This means that provisioning data of one network processor can be restored to a shelf processor or network processor that has a different target identifier (TID).

> **CAUTION**
> **Risk of incorrect provisioning data**
> Before a restore procedure, ensure that the restored provisioning data is compatible with the network element. Restoring the wrong provisioning data to the network element can affect traffic through the network. Take all necessary steps to verify the data integrity before committing the data.

Before each restore, ensure there are no conditions that will prevent the restore. These conditions include:

- a software upgrade in progress
- a database save and restore is in progress
- a duplicate SID exists
- a load mismatch exists. For example, the software version on the network processor is different from that on the shelf processor.
- a Disk Full alarm is raised
- an Alarm and Event Throttling Active alarm is raised

—continued—

Procedure 6-15 (continued)
Restoring provisioning data from an OPC to a network processor over an OSI link

Requirements

The software load in use during a restore must be the same release as the software load used during the save. Otherwise, the restore fails.

When you restore network processor provisioning data from an external repository, you cannot add or remove any network elements in the network processor span of control before the restore is complete.

To perform this procedure, you also must:

- establish an Open Systems Interconnection (OSI) link between the OPTera Metro 3500 system and the system that includes the OPC
- use an account with a level 3 or higher user privilege code (UPC)

Step	Action
1	Log in to the network processor to which you will restore the provisioning data. See Procedures for logging in to a network processor on page 2-1.
2	Ensure that the network processor is selected in the Navigation Tree.
3	Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.
4	Select OPC from the Storage Type drop-down list.
5	Ensure that the Do not backup or restore if alarms exist on NE check box is selected.

CAUTION
Risk of corrupting provisioning data
If you perform a save or restore with the Do not backup or restore if alarms exist on NE check box deselected, the following can occur:

- you can save or restore invalid data
- you can overwrite existing, valid data with invalid data
- you can restore invalid data that can leave the network element in the wrong state

—continued—

Procedure 6-15 (continued)
Restoring provisioning data from an OPC to a network processor over an OSI link

Step **Action**

6 Select the Do not restore if backup TID does not match NE TID check box to prevent the provisioning data from one network processor being restored to a different network processor.

Note 1: To restore provisioning data from one network processor to a different network processor, ensure that the Do not restore if backup TID does not match NE TID check box is not selected. Otherwise, the restore fails.

Note 2: There is no confirmation that the configuration in the restored provisioning data is compatible with the network element configuration. If you restore incompatible provisioning data, the network processor facilities can be incorrectly provisioned and the wrong span of control can be monitored.

7 In the TID (Target ID) field, enter the name of the OPC from which you will restore the provisioning data.

8 In the Directory field, enter the sub-path to the directory that contains the provisioning data.

Note 1: Directories containing the saved provisioning data were created in the users/VFS/ folder on the OPC. The directories must be made available to the FTAM user group or the restore fails.

Note 2: Do not type /users/VFS/ but only the sub-path to the directory that contains the provisioning data. For example, if the directory that contains the provisioning data is called “prov,” then you must type /prov in the Directory field. You must not type /users/VFS/prov.

9 Click Restore from Dir to restore the provisioning data from the OPC to the network processor.

10 Click OK in the Restore warning dialog box.

11 In the OPC Login dialog box that appears, enter your user ID and password to the OPC, and click OK.

Note 1: A Database Restore in Progress alarm is raised.

Note 2: To terminate a restore that is in progress, click Cancel.

Note 3: When the Do not backup or restore if alarms exist on NE check box is selected and an alarm exists on the network processor, the restore fails.

Note 4: If the software version in use during the save is different from that in use during the restore, the restore fails.

—continued—

Procedure 6-15 (continued)

Restoring provisioning data from an OPC to a network processor over an OSI link

Step	Action
12	Click Commit.
	Note: Any mention of DSM slots 19 through 58 in the response block (for data transfer validation), are in fact references to DSM extension slots. These DSM slot references will appear whether or not a DSM is installed.
13	Wait until a Database restore successfully completed message is displayed in the Status area.
14	Click OK in the Restore warning dialog box.
15	Click OK in the Message warning dialog box.
16	Click OK in the Connection Lost dialog box.
	A restart occurs.

—end—

Procedure 6-16
Saving provisioning data from a network processor to an OPC over a TCP/IP link

Use this procedure to save provisioning data from a network processor to an operations controller (OPC). The provisioning data includes the provisioning files that are saved to the network processor from shelf processors within its span of control (SOC).

You can check the network processor before each save to determine if a condition exists that can prevent a save. These conditions include:

- a software upgrade is in progress
- a database save and restore is in progress
- a duplicate SID exists
- a load mismatch exists. For example, the software version on the network processor is different from that on the shelf processor.
- a Disk Full alarm is raised
- a Corrupt Network Backup alarm is raised on the network processor
- an Alarm and Event Throttling Active alarm is raised

Requirements

When you save network processor provisioning data to an external repository, you cannot add or remove any network elements in the network processor span of control before the save is complete.

To perform this procedure, you must:

- establish a TCP/IP link between the OPTera Metro 3500 system and the system that includes the OPC
- use an account with a level 3 or higher user privilege code (UPC)

Step	Action
1	Create a directory on the OPC that will contain the network processor provisioning data. ***Note:*** The directory must be made available to the FTAM user group, or the save fails.
2	Log in to the network processor that contains the provisioning data. See Procedures for logging in to a network processor on page 2-1.
3	Ensure that the network processor is selected in the Navigation Tree.

—continued—

Procedure 6-16 (continued)

Saving provisioning data from a network processor to an OPC over a TCP/IP link

Step **Action**

4 Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.

5 Select Remote Computer from the Storage Type drop-down list.

6 Ensure that the Do not backup or restore if alarms exist on NE check box is selected.

> **CAUTION**
>
> **Risk of corrupting provisioning data**
>
> If you perform a save or restore with the Do not backup or restore if alarms exist on NE check box deselected, the following can occur:
>
> - you can save or restore invalid data
> - you can overwrite existing, valid data with invalid data
> - you can restore invalid data that can leave the network element in the wrong state

7 In the IP field, enter the IP address of the OPC to which you will save the provisioning data.

8 In the Directory field, enter the full path and name of the directory that you created in step 1.

9 Click Save to Dir to save the provisioning data from the network processor to the OPC.

10 In the Remote Login dialog box that appears, enter your user ID and password to the OPC, and click OK.

Note 1: To terminate a save that is in progress, click Cancel.

Note 2: When the Do not backup or restore if alarms exist on NE check box is selected and an alarm exists on the network processor, the save fails.

11 Wait until a Database save successfully completed message is displayed in the Status area.

—end—

Procedure 6-17
Restoring provisioning data from an OPC to a network processor over a TCP/IP link

Use this procedure to restore provisioning data from an operations controller (OPC) to a network processor.

CAUTION
Risk of traffic loss
This procedure can affect traffic carried by the network element, including pass-through traffic. All pass-through traffic must be switched away from the network element. A warm restart of all circuit packs occurs as part of the final commit of the provisioning data.

By default, the Do not restore if backup TID does not match NE TID check box is selected. This means that provisioning data of one network processor cannot be restored to a shelf processor or network processor that has a different target identifier (TID).

CAUTION
Risk of incorrect provisioning data
Before a restore procedure, ensure that the restored provisioning data is compatible with the network element. Restoring the wrong provisioning data to the network element can affect traffic through the network. Take all necessary steps to verify the data integrity before committing the data.

Before each restore, ensure there are no conditions that will prevent the restore. These conditions include:

- a software upgrade in progress
- a database save and restore is in progress
- a duplicate SID exists
- a load mismatch exists. For example, the software version on the network processor is different from that on the shelf processor.
- a Disk Full alarm is raised
- an Alarm and Event Throttling Active alarm is raised

—continued—

Procedure 6-17 (continued)
Restoring provisioning data from an OPC to a network processor over a TCP/IP link

Requirements

The software load in use during a restore must be the same release as the software load used during the save. Otherwise, the restore fails.

When you restore network processor provisioning data from an external repository, you cannot add or remove any network elements in the network processor span of control before the restore is complete.

To perform this procedure, you also must:

- establish a TCP/IP link between the OPTera Metro 3500 system and the system that includes the OPC
- use an account with a level 3 or higher user privilege code (UPC)

Step	Action
1	Log in to the network processor to which you will restore the provisioning data. See Procedures for logging in to a network processor on page 2-1.
2	Ensure that the network processor is selected in the Navigation Tree.
3	Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.
4	Select Remote Computer from the Storage Type drop-down list.
5	Ensure that the Do not backup or restore if alarms exist on NE check box is selected.

CAUTION
Risk of corrupting provisioning data
If you perform a save or restore with the Do not backup or restore if alarms exist on NE check box deselected, the following can occur:

- you can save or restore invalid data
- you can overwrite existing, valid data with invalid data
- you can restore invalid data that can leave the network element in the wrong state

—continued—

Procedure 6-17 (continued)
Restoring provisioning data from an OPC to a network processor over a TCP/IP link

Step	**Action**
6	Select the Do not restore if backup TID does not match NE TID check box to prevent the provisioning data from one network processor being restored to a different network processor. ***Note 1:*** To restore provisioning data from one network processor to a different network processor, ensure that the Do not restore if backup TID does not match NE TID check box is not selected. Otherwise, the restore fails. ***Note 2:*** There is no confirmation that the configuration in the restored provisioning data is compatible with the network element configuration. If you restore incompatible provisioning data, the network processor facilities can be incorrectly provisioned and the wrong span of control can be monitored.
7	In the IP field, enter the IP address of the OPC from which you will restore the provisioning data.
8	In the Directory field, enter the full path and name of the directory that contains the provisioning data.
9	Click Restore from Dir to restore the provisioning data from the OPC to the network processor.
10	Click OK in the Restore warning dialog box.
11	In the Remote Login dialog box that appears, enter your user ID and password to the OPC, and click Login. ***Note 1:*** A Database Restore in Progress alarm is raised. ***Note 2:*** To terminate a restore that is in progress, click Cancel. ***Note 3:*** When the Do not backup or restore if alarms exist on NE check box is selected and an alarm exists on the network processor, the restore fails. ***Note 4:*** If the software version in use during the save is different from that in use during the restore, the restore fails.
12	Click Commit. ***Note:*** Any mention of DSM slots 19 through 58 in the response block (for data transfer validation), are in fact references to DSM extension slots. These DSM slot references will appear whether or not a DSM is installed.
13	Wait until a Database restore successfully completed message is displayed in the Status area.
14	Click OK in the Restore warning dialog box.
15	Click OK in the Message warning dialog box.
16	Click OK in the Connection Lost dialog box. A restart occurs.

—end—

Procedure 6-18
Retrieving a list of shelf processor provisioning data backups

Use this procedure to retrieve a list of the shelf processor backups on a network processor. If a backup is present, the display lists the shelf processor target identifiers (TIDs), their related directory names, and the time stamp for each backup.

> ***Note 1:*** If a shelf processor is removed from the network processor span of control, the backup for that shelf processor is automatically deleted from the network processor.
>
> ***Note 2:*** If you retrieve a list of shelf processor backups after a restore but before a commit, the list of backups may be different from the network processor span of control list. The list does not include any changes made to the network processor span of control since the save. The list will only be updated when the provisioning data is committed to the network processor.

Step	Action
1	Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.
2	Ensure that the network processor is selected in the Navigation Tree.
3	Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.
4	Select NP from the Storage Type drop-down list.
5	Click View Backups to open the SP Backups on NP dialog box.
6	Click OK to close the SP Backups on NP dialog box.

—end—

Procedure 6-19
Deleting shelf processor provisioning data backups from a network processor

Use this procedure to delete a shelf processor provisioning data backup from a network processor.

Requirements

To perform this procedure, you must use an account with a level 3 or higher user privilege code (UPC).

Step	Action
1	Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.
2	Log in to the network element. See Procedures for logging in to a network element on page 2-1.
3	Ensure that the network element is selected in the Navigation Tree.
4	Select Backup and Restore from the Configuration drop-down menu to open the Backup and Restore window.
5	Select NP from the Storage Type drop-down list.
6	Click View Backups to open the SP Backups on NP dialog box.
7	Select the backup file to be deleted.
8	Click Delete.
	Note: To delete all backup files, click Delete All.
9	Click OK to close the SP Backups on NP dialog box.

—end—

Procedure 6-20
Loading and executing a TL1 script file on a network element

Use this procedure to

- download a TL1 script file from a remote destination with a TID or IP address and temporarily store it on the network processor
- commit the TL1 commands contained in the TL1 script file (stored on the NP) to a designated network element.

While the download command is running, a TL1 Script file Load in Progress alarm becomes active. This alarm remains active until the TL1 script file is committed to the target network element, or the download command is cancelled.

The download command is not successful if one of the following occurs

- there is an unsuccessful download of the TL1 script file from the remote location
- the file validation fails

The commit command is not successful if one of the following occurs

- any command in the TL1 script file does not complete successfully
- a timeout period elapses before an event or alarm is generated, indicating that the save command is completed

If the download or commit command is not successful, a TL1 Script file Load Failed alarm becomes active. To clear this alarm, you must cancel the download or commit command.

Requirements

To perform this procedure, you must use an account with a level 3 or higher user privilege code (UPC).

—continued—

Procedure 6-20 (continued)
Loading and executing a TL1 script file on a network element

Step	Action
1	Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.
2	Ensure that the target network element is selected in the Navigation Tree.
3	Start a TL1 Command Builder session. See Procedures for using the TL1 Command Builder on page 7-1.
4	Load the TL1 script file from a remote location on to the network processor by entering `LOAD-TL1SCRPT-NE:[TID]::CTAG:::[TRGTID=Domain] [,DESTTYPE=Domain][,DESTADDR=Domain][,DIR=Domain] [,CHKALM=Domain][,CHKTID=Domain];` For more information about this TL1 command, see *TL1 Reference-Part 1 of 4*, 323-1059-190.
5	Click Run Command.
6	Wait until a completed message is displayed in the Status area. ***Note:*** To terminate a download in progress, enter the following command: `CANC-TL1SCRPT-NE:[TID]::CTAG;` For more information about this TL1 command, see *TL1 Reference-Part 1 of 4*, 323-1059-190.
7	Commit the TL1 script file to the target network element by entering `CMMT-TL1SCRPT-NE:[TID]::CTAG;` For more information about this TL1 command, see *TL1 Reference-Part 1 of 4*, 323-1059-190.
8	Click Run Command.
9	Wait until a completed message is displayed in the Status area. ***Note:*** To terminate a commit in progress, enter the following command: `CANC-TL1SCRPT-NE:[TID]::CTAG;` For more information about this TL1 command, see *TL1 Reference-Part 1 of 4*, 323-1059-190.

—end—

Procedure 6-21
Installing a software load on a shelf processor from a local computer

Use this procedure to install a software load on a shelf processor from a computer that has a direct connection to the shelf processor.

When you install a load, you replace only the shelf processor load (by upgrading or downgrading it) and the load of the traffic circuit packs remains unaffected. The software load to be installed must be the same as the software release that is currently running on the shelf.

Requirements

To perform this procedure you must

- connect the computer to the RS-232 interface on the shelf processor
- use an account with a level 3 or higher user privilege code (UPC)

Step	Action
1	Log in to the shelf processor. See Procedures for logging in to a network element on page 2-1.
2	Ensure that the network element is selected in the Navigation Tree.
3	Select Load Installation Management from the Configuration drop-down menu to open the Load Installation Management window. The ID of the target shelf processor appears at the top of the Load Installation Management window.
4	Select Local computer from the Storage type drop-down list.
5	Do one of the following: • In the Directory field, enter the drive and directory that contain the upgrade software release. • Click Browse, and search for the drive and directory. Select the directory and click OK. The Install to field displays the name of the directory that appears in the Directory text field.

—continued—

Procedure 6-21 (continued)
Installing a software load on a shelf processor from a local computer

Step	Action
6	Click Check. ***Note 1:*** Wait until the message, Checking install ... Done, is displayed in the Status area. ***Note 2:*** If an Incomplete Load Lineup alarm, Circuit Pack Unknown alarm, or Transport Data Recovery Failed alarm exists, the following message appears: “Checking upgrade... failed. Slot(s)....15 Passed.” Click OK in the Check failed confirmation dialog box and continue with the next step. If the check fails because of another reason, use the appropriate trouble clearing procedure or contact your next level of support.
7	Click Load.
8	Click OK in the confirmation dialog box that appears. ***Note 1:*** Wait until the message, Loading install...Done, is displayed in the Status area. If the load fails, use the appropriate trouble clearing procedure or contact your next level of support. ***Note 2:*** After you see the message Loading install...Done, you can cancel the load installation or proceed with the next step. If you cancel the load installation, the Incomplete Load Lineup alarm appears.
9	Click Invoke.
10	Click OK in the confirmation dialog box. The following message appears: “You are about to logout because the NE is rebooting, please wait 5 minutes then log back in.”
11	Click OK in the Session Dropped confirmation dialog box. The login session is closed. Wait for 5 minutes.
12	Log in to the target shelf processor again. See Procedures for logging in to a network element on page 2-1.
13	Select Load Installation Management from the Configuration drop-down menu to open the Load Installation Management window.
14	Click Invoke.
15	Click OK in the confirmation dialog box. ***Note 1:*** Wait until the message, Invoking install... Done, is displayed in the Status area. If there is an error, use the appropriate trouble clearing procedure or contact your next level of support. ***Note 2:*** After you see the message “Invoking Install...Done,” you can cancel the load installation or proceed with the next step.

—continued—

Procedure 6-21 (continued)
Installing a software load on a shelf processor from a local computer

Step	Action
16	Click Commit.
17	Click OK in the confirmation dialog box that appears.
	Note: Wait until the message, Committing install... Done, is displayed in the Status area. If there is an error, use the appropriate trouble clearing procedure or contact your next level of support.
18	Perform a cold restart of the shelf processor. See 323-1059-543, Restarting the shelf processor on page 2-47.
	Note: FPGA load mismatches that occur after the shelf processor software upgrade are detected only after a cold restart of the shelf processor.

—end—

Procedure 6-22
Installing a software load on a shelf processor using an Ethernet connection

Use this procedure to install a software load on a shelf processor over an Ethernet connection from another shelf processor, a network processor, or an operations controller (OPC).

When you install a load, you replace only the shelf processor load (by upgrading or downgrading it) and the load of the traffic circuit packs remains unaffected. The software load to be installed must be the same as the software release that is currently running on the shelf.

Requirements

To perform this procedure you must:

- connect your PC to the shelf processor through an Ethernet connection
- use an account with a level 3 or higher user privilege code (UPC)

Step **Action**

1 Log in to the shelf processor. See Procedures for logging in to a network element on page 2-1.

2 Ensure that the network element is selected in the Navigation Tree.

3 Select Load Installation Management from the Configuration drop-down menu to open the Load Installation Management window.

The ID of the target shelf processor appears at the top of the Load Installation Management window.

4 Select Network element from the Storage type drop-down list.

5 Do one of the following:

- In the Source field, enter the TID of the network element or OPC that contains the upgrade software release.
- Click Find to open the Find Node dialog box. Select the TID of the network element or OPC that contains the upgrade software release and click OK.

  The release number which will be installed on the shelf processor is retrieved from the server and appears in the Upgrade to field.

—continued—

Procedure 6-22 (continued)
Installing a software load on a shelf processor using an Ethernet connection

Step	Action
6	Click Check. ***Note 1:*** Wait until the message, Checking install ... Done, is displayed in the Status area. ***Note 2:*** If an Incomplete Load Lineup alarm, Circuit Pack Unknown alarm, or Transport Data Recovery Failed alarm exists, the following message appears: "Checking upgrade... failed. Slot(s)....15 Passed." Click OK in the Check failed confirmation dialog box and continue with the next step. If the check fails because of another reason, use the appropriate trouble clearing procedure or contact your next level of support.
7	Click Load.
8	Click OK in the confirmation dialog box that appears. ***Note 1:*** Wait until the message, Loading install...Done, is displayed in the Status area. If the load fails, use the appropriate trouble clearing procedure or contact your next level of support. ***Note 2:*** After you see the message Loading install...Done, you can cancel the load installation or proceed with the next step. If you cancel the load installation, the Incomplete Load Lineup alarm appears.
9	Click Invoke.
10	Click OK in the confirmation dialog box. The following message appears: "You are about to logout because the NE is rebooting, please wait 5 minutes then log back in."
11	Click OK in the Session Dropped confirmation dialog box. The login session is closed. Wait for 5 minutes.
12	Log in to the target shelf processor again. See Procedures for logging in to a network element on page 2-1.
13	Select Load Installation Management from the Configuration drop-down menu to open the Load Installation Management window.
14	Click Invoke.
15	Click OK in the confirmation dialog box that appears. ***Note 1:*** Wait until the message, Invoking install... Done, is displayed in the Status area. If there is an error, use the appropriate trouble clearing procedure or contact your next level of support. ***Note 2:*** After you see the message "Invoking Install...Done," you can cancel the load installation or proceed with the next step.
16	Click Commit.

—continued—

Procedure 6-22 (continued)
Installing a software load on a shelf processor using an Ethernet connection

Step	**Action**
17	Click OK in the confirmation dialog box that appears. ***Note:*** Wait until the message, Committing install... Done, is displayed in the Status area. If there is an error, use the appropriate trouble clearing procedure or contact your next level of support.
18	Perform a cold restart of the shelf processor. See 323-1059-543, Restarting the shelf processor on page 2-47. ***Note:*** FPGA load mismatches that occur after the shelf processor software upgrade are detected only after a cold restart of the shelf processor.

—end—

Procedure 6-23
Upgrading the software load on a network processor

Use this procedure to upgrade the software load on a network processor from another network processor or an operations controller (OPC).

> ***Note 1:*** If the Loads Mismatch alarm is active, do not make any provisioning changes to the network processor until you complete this procedure.
>
> ***Note 2:*** If you are upgrading the software load on a network processor that is acting as a Time of Day server from Release 11.01, the network processor can raise a “TOD Server has not responded to a request” alarm during extreme system activity. This alarm can toggle at an interval consistent with the Network Timing Protocol polling period during a prolonged period of extreme system activity. This condition can be alleviated by increasing the Network Timing Protocol polling interval. This condition can also be cleared once the system returns to a normal level of activity.

CAUTION
Risk of reboot loop on the network processor
All network processors running a release prior to Release 11.02 must be upgraded to Release 11.02 before transferring the Release 12 software from the network processor or OPC. Failure to do so causes the network processor to enter into a reboot loop at the end of the software delivery.

Requirements

To perform this procedure you must:

- connect your computer to the network processor through an Ethernet connection
- use an account with a level 3 or higher user privilege code (UPC)

Step **Action**

1 Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.

2 Ensure that the network processor is selected in the Navigation Tree.

3 Select Upgrade Management from the Configuration drop-down menu to open the Upgrade Management window.

The ID of the target network processor appears at the top of the Upgrade Management window.

—continued—

Procedure 6-23 (continued)
Upgrading the software load on a network processor

Step	Action
4	Select network element from the Storage type drop-down list.
5	Do one of the following: • In the Source field, enter the TID of the network processor or OPC that contains the upgrade software release. • Click Find to open the Find Node dialog box. Select the TID of the network processor or OPC that contains the upgrade software release and click OK.
6	In the Upgrade to field, enter the release number to which the network processor will be upgraded.
7	Ensure that the Do not load if alarms exist on NE check box is selected. ***Note:*** If the network processor has a Loads Mismatch alarm or a SOC Software Version Mismatch Alarm, deselect the Do not load if alarms exist on NE check box.
8	Click Check. ***Note 1:*** Wait until the message, Checking upgrade... Done, is displayed in the Status area. If the check fails, use the appropriate trouble clearing procedure or contact your next level of support. ***Note 2:*** If the alarms listed in step 7 are present, you must continue to the next step.
9	Click Load.
10	Click OK in the confirmation dialog box that appears. ***Note 1:*** Wait until the message, Loading upgrade...Done, is displayed in the Status area. If the load fails, use the appropriate trouble clearing procedure or contact your next level of support. ***Note 2:*** After you see the message “Loading upgrade...Done,” you can cancel the software upgrade or proceed with the next step.
11	Click Invoke.
12	Click OK in the confirmation dialog box. The following message appears: “You are about to logout because the NE is rebooting, please wait 5 minutes then log back in.”
13	Click OK in the Connection Lost confirmation dialog box. The login session is closed. Wait for 5 minutes.
14	Log in to the target network processor again. See Procedures for logging in to a network processor on page 2-1.
15	Select Upgrade Management from the Configuration drop-down menu to open the Upgrade Management window.
16	Click Invoke.

—continued—

Procedure 6-23 (continued)

Upgrading the software load on a network processor

Step	**Action**
17	Click OK in the confirmation dialog box. ***Note 1:*** Wait until the message, Invoking upgrade... Done, is displayed in the Status area. If there is an error, use the appropriate trouble clearing procedure or contact your next level of support. ***Note 2:*** After you see the message “Invoking upgrade...Done,” you can cancel the software upgrade or proceed with the next step.
18	Click Commit.
19	Click OK in the confirmation dialog box that appears. ***Note:*** Wait until the message, Committing upgrade ... Done, is displayed in the Status area. If there is an error, use the appropriate trouble clearing procedure or contact your next level of support.

—end—

Procedure 6-24
Upgrading the software load on a network element from a local computer

Use this procedure to upgrade the software load on both the shelf processor and the transport circuit packs. You can get the upgrade load from a local computer directly connected to the shelf processor.

> ***Note:*** If the Load Mismatch alarm exists and the software release of the shelf processor is to be changed, a load install procedure should be used instead of an upgrade. This situation occurs after a shelf processor replacement when the shelf is running a different release than the shelf processor. See Installing a software load on a shelf processor from a local computer on page 6-49.

Requirements

To perform this procedure you must:

- connect the PC to the RS-232 interface on the target shelf processor
- use an account with a level 3 or higher user privilege code (UPC)

Step **Action**

1 Log in to the network element. See Procedures for logging in to a network element on page 2-1.

2 Ensure that the network element is selected in the Navigation Tree.

3 Select Upgrade Management from the Configuration drop-down menu to open the Upgrade Management window.

The ID of the target shelf processor appears at the top of the Upgrade Management window.

4 Select Local computer from the Storage type drop-down list.

5 Do one of the following:

- In the Directory field, enter the drive and directory that contain the upgrade software release.
- Click Browse, and search for the drive and directory. Select the directory and click OK.

6 In the Upgrade to field, enter the release number to which the shelf processor and the transport circuit packs will be upgraded.

—continued—

Procedure 6-24 (continued)
Upgrading the software load on a network element from a local computer

Step	Action
7	Ensure that the Do not load if alarms exist on NE check box is selected. ***Note:*** If Incomplete Load Lineup, Circuit Pack Unknown, or Transport Data Recovery Failed alarms exist, deselect the Do not load if alarms exist on NE check box.
8	Click Check. ***Note 1:*** Wait until the message, Checking upgrade... Done, is displayed in the Status area. If the check fails, use the appropriate trouble clearing procedure or contact your next level of support. ***Note 2:*** If an Incomplete Load Lineup alarm, Circuit Pack Unknown alarm, or Transport Data Recovery Failed alarm exists, the following message appears: “Checking upgrade... failed. Slot(s)....15 Passed.” Click OK in the Check failed confirmation dialog box and continue with the next step. If the check fails because of another reason, use the appropriate trouble clearing procedure or contact your next level of support.

CAUTION
Risk of losing Site Manager connection to the shelf processor
A network element that is connected with more than eight DSM DS1x84TM circuit packs (four protected DSM units or eight unprotected DSM units) is very busy during the load upgrade operation. During this period, it is highly recommended not to perform any operations, administration and maintenance (OAM) procedures or open any Site Manager applications except for Upgrade Management and Alarms and Events monitoring. Failure to do so can cause Site Manager to drop its connection to the shelf processor and prevent you from logging back in to the network element until the load upgrade operation is completed.

Step	Action
9	Click Load.
10	Click OK in the confirmation dialog box that appears. ***Note 1:*** Wait until the message, Loading upgrade...Done, is displayed in the Status area. If the load fails, use the appropriate trouble clearing procedure or contact your next level of support. ***Note 2:*** After you see the message Loading upgrade...Done, you can cancel the load installation or proceed with the next step. If you cancel the load installation, the Incomplete Load Lineup alarm appears.
11	Click Invoke.

—continued—

Procedure 6-24 (continued)

Upgrading the software load on a network element from a local computer

Step **Action**

12

If	**Then** go to
you are performing this procedure in order to clear the “Incomplete Load Lineup Alarm”	step 18
otherwise	step 13

13 Click OK in the confirmation dialog box.

The following message appears: “You are about to logout because the NE is rebooting, please wait 5 minutes then log back in.”

14 Click OK in the Session Dropped confirmation dialog box.

The login session is closed. Wait for 5 minutes.

15 Log in to the target network element again. See Procedures for logging in to a network element on page 2-1.

16 Select Upgrade Management from the Configuration drop-down menu to open the Upgrade Management window.

17 Click Invoke.

18 Click OK in the confirmation dialog box.

Note 1: Wait until the message, Invoking upgrade... Done, is displayed in the Status area. If there is an error, use the appropriate trouble clearing procedure or contact your next level of support.

Note 2: After you see the message “Invoking upgrade...Done,” you can cancel the load installation or proceed with the next step.

19 Click Commit.

20 Click OK in the confirmation dialog box that appears.

Note 1: Wait until the message, Committing upgrade... Done, is displayed in the Status area. If there is an error, use the appropriate trouble clearing procedure or contact your next level of support.

Note 2: If the “FPGA load mismatch” alarm is raised against a Packet Edge or 2x100BT-P2P circuit pack after the upgrade, you must download the latest FPGA load to the circuit pack. See Upgrading the FPGA load on a Packet Edge, 2x100BT-P2P, or 2xGigE/FC-P2P circuit pack on page 6-64.

—end—

Procedure 6-25
Upgrading the software load on a network element using an Ethernet connection

Use this procedure to upgrade the software load on both the shelf processor and the transport circuit packs. You can get the upgrade load from another shelf processor, a network processor, or an operations controller (OPC).

> ***Note:*** If the Load Mismatch alarm exists and the software release of the shelf processor is to be changed, a load install procedure should be used instead of an upgrade. This situation occurs after a shelf processor replacement when the shelf is running a different release than the shelf processor. See Installing a software load on a shelf processor using an Ethernet connection on page 6-52.

Requirements

To perform this procedure you must:

- connect your PC to the shelf processor through an Ethernet connection
- use an account with a level 3 or higher user privilege code (UPC)

Step	Action
1	Log in to the network element. See Procedures for logging in to a network element on page 2-1.
2	Ensure that the network element is selected in the Navigation Tree.
3	Select Upgrade Management from the Configuration drop-down menu to open the Upgrade Management window. The ID of the target shelf processor appears at the top of the Upgrade Management window.
4	Select Network element from the Storage type drop-down list.
5	Do one of the following: • In the Source field, enter the TID of the network element or OPC that contains the upgrade software release. • Click Find to open the Find Node dialog box. Select the TID of the network element or OPC that contains the upgrade software release and click OK.
6	In the Upgrade to field, enter the release number to which the shelf processor will be upgraded.
7	Ensure that the Do not load if alarms exist on NE check box is selected. ***Note:*** If a Load Mismatch or other software related alarms exist, deselect the Do not load if alarms exist on NE check box.

—continued—

Procedure 6-25 (continued)

Upgrading the software load on a network element using an Ethernet connection

Step **Action**

8 Click Check.

Note 1: Wait until the message, Checking upgrade... Done, is displayed in the Status area.

Note 2: If an Incomplete Load Lineup alarm, Circuit Pack Unknown alarm, or Transport Data Recovery Failed alarm exists, the following message appears: “Checking upgrade... failed. Slot(s)....15 Passed.” Click OK in the Check failed confirmation dialog box and continue with the next step. If the check fails because of another reason, use the appropriate trouble clearing procedure or contact your next level of support.

> **CAUTION**
>
> **Risk of losing Site Manager connection to the shelf processor**
>
> A network element that is connected with more than eight DSM DS1x84TM circuit packs (four protected DSM units or eight unprotected DSM units) is very busy during the load upgrade operation. During this period, it is highly recommended not to perform any operations, administration and maintenance (OAM) procedures or open any Site Manager applications except for Upgrade Management and Alarms and Events monitoring. Failure to do so can cause Site Manager to drop its connection to the shelf processor and prevent you from logging back in to the network element until the load upgrade operation is completed.

9 Click Load.

10 Click OK in the confirmation dialog that appears.

Note 1: Wait until the message, Loading upgrade...Done, is displayed in the Status area. If the load fails, use the appropriate trouble clearing procedure or contact your next level of support.

Note 2: After you see the message “Loading upgrade...Done,” you can cancel the software upgrade or proceed with the next step. If you cancel the upgrade, you’ll get an Incomplete Load Lineup alarm.

11 Click Invoke.

12

If	**Then** go to
you are performing this procedure in order to clear the “Incomplete Load Lineup Alarm”	step 18
otherwise	step 13

—continued—

Procedure 6-25 (continued)

Upgrading the software load on a network element using an Ethernet connection

Step	Action
13	Click OK in the confirmation dialog box. The following message appears: “You are about to logout because the network element is rebooting, please wait 5 minutes then log back in.” The network element reboots.
14	Click OK in the Session Dropped confirmation dialog box. The login session is closed. Wait for 5 minutes.
15	Log in to the target network element again. See Procedures for logging in to a network element on page 2-1.
16	Select Upgrade Management from the Configuration drop-down menu to open the Upgrade Management window.
17	Click Invoke.
18	Click Commit.
19	Click OK in the confirmation dialog box that appears. ***Note 1:*** Wait until the message, Committing upgrade... Done, is displayed in the Status area. If there is an error, use the appropriate trouble clearing procedure or contact your next level of support. ***Note 2:*** If the “FPGA load mismatch” alarm is raised against a Packet Edge or 2x100BT-P2P circuit pack after the upgrade, you must download the latest FPGA load to the circuit pack. See Upgrading the FPGA load on a Packet Edge, 2x100BT-P2P, or 2xGigE/FC-P2P circuit pack on page 6-64.

—end—

Procedure 6-26
Upgrading the FPGA load on a Packet Edge, 2x100BT-P2P, or 2xGigE/FC-P2P circuit pack

Use this procedure to upgrade the field programmable gate array (FPGA) load on a Packet Edge, 2x100BT-P2P or 2xGigE/FC-P2P circuit pack. Perform this procedure if the "FPGA load mismatch" alarm is raised against the circuit pack after an upgrade.

Requirements

To perform this procedure you must:

- save the provisioning data of the Packet Edge circuit pack
- use an account with a level 3 or higher user privilege code (UPC)

Step **Action**

1 Log in to the network element. See Procedures for logging in to a network element on page 2-1.

2 Ensure that the shelf processor is selected in the Navigation Tree.

3 Select FPGA Download from the Configuration menu to open the FPGA Download window.

4 Select the required circuit pack from the Type column.

Note: The FPGA Download window only displays provisioned and in-service circuit packs.

5 Click Load to open the Load FPGA dialog box.

Note: The Load button is only active if you are logged in to the network element with a user privilege code (UPC) level of 3 or higher and there are no circuit pack upgrades in progress.

6 Ensure that NP appears in the Storage type drop-down list.

7 Do one of the following:

- In the Source field, enter the target identifier (TID) of the network processor that contains the FPGA load to download to the circuit pack.
- Click Find to open the Find Node dialog box. Select the TID of the network processor that contains the FPGA load to download to the circuit pack, then click OK.

Note: The network processor must be in the shelf processor routing table but the shelf processor does not have to be within the network processor span of control.

—continued—

Procedure 6-26 (continued)

Upgrading the FPGA load on a Packet Edge, 2x100BT-P2P, or 2xGigE/FC-P2P circuit pack

Step **Action**

8 Click OK. The FPGA Download progress dialog box appears.

Note: You cannot perform an FPGA download and a network element software upgrade on the same shelf at the same time.

9 Wait until the FPGA Download progress dialog box closes.

10 Click OK in the FPGA Download confirmation dialog box.

11

> ⚠ **CAUTION**
> **Risk of traffic loss**
> A cold restart on a circuit pack that does not have equipment protection results in traffic loss. There is no equipment protection for Packet Edge and 2x100BT-P2P circuit packs.

Click Restart in the FPGA Download window to perform a cold restart of the selected circuit pack.

12 Click Yes in the Confirm Restart dialog box. The restart takes about 3 minutes.

—end—

Procedure 6-27
Transferring a software load from a Site Manager computer to a network processor over an Ethernet connection

Use this procedure to transfer a software load from a Site Manager computer to a network processor over an Ethernet connection.

> **CAUTION**
> **Risk of reboot loop on the network processor**
> All network processors running a release prior to Release 11.02 must be upgraded to Release 11.02 before transferring the Release 12 software from the Site Manager computer. Failure to do so causes the network processor to enter into a reboot loop at the end of the software delivery.

Requirements

To perform this procedure you must

- connect your PC to the network processor through an Ethernet connection
- use an account with a level 3 or higher user privilege code (UPC)

Step **Action**

1 Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.

2 Ensure that the network processor is selected in the Navigation Tree.

3 Select Release Management from the Configuration drop-down menu.

The ID of the target network processor appears at the top of the Release Management window.

4 Under Release loads, note the amount of space available on the NPx in the Space available field.

Note: You must have a minimum of 20,000 KB of space available on the NPx before you transfer a software load to it.

5 Click Add to open the Add Release Software dialog box.

6 Select Local computer from the Storage type drop-down list.

—continued—

Procedure 6-27 (continued)

Transferring a software load from a Site Manager computer to a network processor over an Ethernet connection

Step	Action
7	Do one of the following: • In the Directory field, enter the drive and directory that contains the software load to be transferred. • Click Browse, and search for the drive and directory that contains the software load to be transferred. Select the directory and click OK. The FTP Login dialog box opens.
8	Enter an ID in the User ID field.
9	Enter a password in the Password field.
10	Click Login. The FTP session starts and the file transfer is initiated. A Progress dialog box appears. ***Note 1:*** If there is a problem with the file transfer, a Resend Files warning dialog box appears. Click Yes to resend all software files from the Site Manager computer to the target network processor. ***Note 2:*** The network processor has limited file system space. When an attempt is made to transfer a new software load to the network processor, the software release management of the network processor may automatically delete the oldest software release load.
11	Wait until the Status area displays a message that the new release is successfully delivered.
12	Click Refresh to ensure that the new release is listed in the Release loads field.

—end—

Procedure 6-28
Transferring a software load from an OPC or network processor to a network processor using a network connection

Use this procedure to transfer a software load from an OPC or a network processor to a network processor using a network connection.

> **CAUTION**
> **Risk of reboot loop on the network processor**
> All network processors running a release prior to Release 11.02 must be upgraded to Release 11.02 before transferring the Release 12 software from the network processor or OPC. Failure to do so causes the network processor to enter into a reboot loop at the end of the software delivery.

Requirements

To perform this procedure you must use an account with a level 3 or higher user privilege code (UPC).

Step	Action
1	Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.
2	Ensure that the network processor is selected in the Navigation Tree.
3	Select Release Management from the Configuration drop-down menu to open the Release Management window. The ID of the target network processor appears at the top of the Release Management window.
4	Under Release loads, note the amount of space available on the NPx in the Space available field. ***Note:*** You must have a minimum of 20,000 KB of space available on the NPx before you transfer a software load to it.
5	Click Add to open the Add Release Software dialog box.
6	Select Network element from the Storage type drop-down list.

—continued—

Procedure 6-28 (continued)
Transferring a software load from an OPC or network processor to a network processor using a network connection

Step	Action
7	Do one of the following: • In the Source field, enter the ID of the network element that contains the software load to be transferred. • Click Find, select a network element ID in the Find Node dialog box, and click OK.
8	In the Release name field, enter the name of the new release to be transferred to the network processor.
9	Ensure that the Do not load if alarms exist on NE check box is selected.
10	Click OK.

—end—

Procedure 6-29
Transferring a software load from an OPC or network processor to a network processor using a direct cable connection

Use this procedure to transfer a software load from an OPC or a network processor to a network processor using a direct cable connection.

> **CAUTION**
> **Risk of reboot loop on the network processor**
> All network processors running a release prior to Release 11.02 must be upgraded to Release 11.02 before transferring the Release 12 software from the network processor or OPC. Failure to do so causes the network processor to enter into a reboot loop at the end of the software delivery.

Requirements

To perform this procedure you must

- connect the PC to the RS-232 interface on the target network element
- use an account with a level 3 or higher user privilege code (UPC)

Step **Action**

1 Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.

2 Ensure that the network processor is selected in the Navigation Tree.

3 Select Release Management from the Configuration drop-down menu to open the Release Management window.

The ID of the target network processor appears at the top of the Release Management window.

4 Under Release loads, note the amount of space available on the NPx in the Space available field.

Note: You must have a minimum of 20,000 KB of space available on the NPx before you transfer a software load to it.

5 Click Add to open the Add Release Software dialog box.

6 Select Network element from the Storage type drop-down list.

—continued—

Procedure 6-29 (continued)

Transferring a software load from an OPC or network processor to a network processor using a direct cable connection

Step	**Action**
7	Do one of the following: • In the Source field, enter the ID of the network element that contains the software load to be transferred. • Click Find, select a network element ID from the routing table, and click OK.
8	In the Release name field, enter the name of the new release to be transferred to the network processor.
9	Ensure that the Do not load if alarms exist on NE check box is selected.
10	Click OK.

—end—

Procedure 6-30
Retrieving a list of the software releases on the network processor

Use this procedure to retrieve a list of the software releases on the network processor. Software releases are stored on the network processor file system for shelf upgrades.

Requirements

To perform this procedure you must use an account with a level 3 or higher user privilege code (UPC).

Step	Action
1	Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.
2	Ensure that the network processor is selected in the Navigation Tree.
3	Select Release Management from the Configuration drop-down menu to open the Release Management window. The ID of the target network processor appears at the top of the Release Management window.
4	Click Refresh to retrieve the list of current software releases in the Release loads area.

—end—

Procedure 6-31
Deleting a software load from a network processor

Use this procedure to delete a software load from a network processor.

Requirements

To perform this procedure you must use an account with a level 3 or higher user privilege code (UPC).

Step	Action
1	Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.
2	Ensure that the network processor is selected in the Navigation Tree.
3	Select Release Management from the Configuration drop-down menu to open the Release Management window. The ID of the target network processor appears at the top of the Release Management window.
4	In the Release loads list, select the software load to be deleted.
5	Click Delete.
6	Click Yes in the Delete a Software Load warning dialog box.
7	Wait until the Status area displays a message that the new release is successfully deleted.
8	Click Refresh to ensure that the new release is no longer listed in the Release loads field.

—end—

Procedure 6-32
Verifying the current network processor software version

Use this procedure to verify the current version of the network processor software load.

Requirements

To perform this procedure you must use an account with a level 3 or higher user privilege code (UPC).

Step	Action
1	Log in to the network processor. See Procedures for logging in to a network processor on page 2-1.
2	Ensure that the network processor is selected in the Navigation Tree.
3	Select Node Information from the Configuration drop-down menu to open the Node Information window. The current release is displayed in the Software version field.

—end—

Procedure 6-33
Verifying the current shelf processor software version

Use this procedure to verify the current version of the shelf processor software load.

Requirements

To perform this procedure you must use an account with a level 3 or higher user privilege code (UPC).

Step	Action
1	Log in to the shelf processor. See Procedures for logging in to a network element on page 2-1.
2	Select Node Information from the Configuration drop-down menu to open the Node Information window. The current release is displayed in the Software version field.

—end—

TL1 Command Builder

Procedures for using the TL1 Command Builder

Procedure 7-1
Starting the TL1 Command Builder

Use this procedure to open the TL1 Command Builder.

Step	Action
1	Select TL1 Command Builder from the Tools sub-menu of the File drop-down menu. ***Note:*** The network element verifies your user privilege code (UPC) against each command, and will not permit access to commands or scripts for which your UPC is too low. TL1 Command Builder is fully functional for all UPCs, the network element ensures the validation.

—end—

Procedure 7-2
Closing the TL1 Command Builder

Step	Action

1 From the TL1 Command Builder window, do one of the following:

- Select Close from the File drop-down menu.
- Click the X button in the top right corner of the window.
- Right-click the window title bar, and select Close from the pop-up menu.

Note 1: If you have not saved changes to a script file, a warning dialog appears asking you whether you want to save the changes.

Note 2: If there is a script in progress, closing the TL1 Command Builder stops the execution of the script.

—end—

Procedure 7-3
Editing and running a TL1 command

The TL1 command Builder lets you edit and run one command at a time using the Immediate mode of operation. In the Immediate mode, you cannot save any changes to a TL1 command or record it to a script.

You can save an edited TL1 command and add it to a script while building a script. For more information, see Building a script on page 7-6.

Step **Action**

1 Ensure that you are logged in to the network element. See Procedures for logging in to a network element on page 2-1.

2 Start the TL1 Command Builder. See Starting the TL1 Command Builder on page 7-2.

3 Select the network element from the NE drop-down list.

Note 1: The network element to which you are logged in and have selected in the Site Manager navigation tree appears by default in the NE drop-down list.

Note 2: The type and release for the network element you have selected appears by default in the NE type and the Release drop-down lists.

4 Select Immediate from the Mode drop-down list.

5 Select the required option for filtering the TL1 commands displayed in the Command list.

If you want to display the following TL1 commands in the Command list	**Then** from the Filter drop-down list, select the
all supported TL1 commands (no filtering options)	All option, then go to step 9
TL1 commands of a specific group	By Group option, then go to step 6
TL1 commands that have a specific verb	By Verb option, then go to step 7
TL1 commands that contain a specific string	By String option, then go to step 8

6 From the Category drop-down list, select the group of TL1 commands you want to display in the Command list.

Go to step 9.

—continued—

Procedure 7-3 (continued)

Editing and running a TL1 command

Step	Action
7	From the Category drop-down list, select the verb for the TL1 commands you want to display in the Command list. ***Note:*** A TL1 command always begins with a verb as shown in the TL1 command structure: VERB-MODIFIER:TID:AID:CTAG::parameter-list;. Go to step 9.
8	In the Category drop-down list, type the string that you want to use to filter the TL1 commands displayed in the Command list.
9	Select a command name from the Command list. ***Note 1:*** All of the command parameter and value options that are available in the Parameter table are valid for the network element you have selected. ***Note 2:*** The selected command and its parameters appear in the text field above the Run Command button.
10	Specify the value for each parameter listed in the Parameter table: • If the parameter supports a fixed set of values, click on the corresponding Value field to activate a drop-down list of supported values, then select the required value. • If the Value field displays <String> or <Number>, then you can type the required value. The TL1 command field (the text field above the Run Command) is updated with the parameter values you selected in the Parameter table. ***Note 1:*** The Value drop-down list contains the entire domain for the selected parameter. ***Note 2:*** If a TL1 command includes a password parameter, then you must select a generic password in the password identifier (PID) value field of the Parameter table. You cannot type the actual password in the Parameter table when you edit TL1 commands in the TL1 Command Builder window. You can map the generic password to an actual password during command execution. ***Note 3:*** The text field above the Run Command button is editable and you can further modify the command text if you wish. However, you have full responsibility for the syntax and parameter values you enter.
11	When you finalize the TL1 command, click Run Command to test it. The command is sent to the network element and the command response message appears in the Results area.

—end—

Procedure 7-4
Building a script

Use this procedure to record a series of TL1 commands and save them in a script.

Step	Action
1	Start the TL1 Command Builder. See Starting the TL1 Command Builder on page 7-2.
2	Select New from the File drop-down menu in the TL1 Command Builder to create a new script file.
3	Select Batch from the Mode drop-down list.
4	

If you want to build a script for a	**Then** go to
specific network element	step 5
network element type	step 8

Building a script for a network element type

5 Select a generic TID from the NE drop-down list.

Note: You can map the generic network element name (GenTID#) to a network element at the time of script execution.

6 Select a network element type from the NE Type drop-down list.

7 Select a release number for the network element type from the Release drop-down list.

Go to step 10.

Building a script for a specific network element

8 Ensure that you are logged in to the network element. See Procedures for logging in to a network element on page 2-1.

9 Select the network element from the NE drop-down list.

Note 1: If you are logged in to a network element and have selected it in the navigation tree, its name appears automatically in the NE drop-down list.

Note 2: If you are logged in to a network element and have selected it in the navigation tree, the NE Type and Release drop-down lists display the network element type and release number and are not editable.

—continued—

Procedure 7-4 (continued)
Building a script

Step **Action**

Adding commands to the script

10 Select the required option for filtering the TL1 commands displayed in the Command list.

If you want to display the following TL1 commands in the Command list	**Then** from the Filter drop-down list, select the
all supported TL1 commands (no filtering options)	All option, then go to step 14
TL1 commands of a specific group	By Group option, then go to step 11
TL1 commands that have a specific verb	By Verb option, then go to step 12
TL1 commands that contain a specific string	By String option, then go to step 13

11 From the Category drop-down list, select the group of TL1 commands you want to display in the Command list.

Go to step 14.

12 From the Category drop-down list, select the verb for the TL1 commands you want to display in the Command list.

Note: A TL1 command always begins with a verb as shown in the TL1 command structure: VERB-MODIFIER:TID:AID:CTAG::parameter-list;.

Go to step 14.

13 From the Category drop-down list, type the string that you want to use to filter the TL1 commands displayed in the Command list.

14 Select a command name from the Command list.

Note 1: All of the command parameter and value options that are available in the Parameter table are valid for the network element you have selected.

Note 2: The selected command and its parameters appear in the text field above the Run Command button.

—continued—

Procedure 7-4 (continued)
Building a script

Step	**Action**
15	Specify the value for each parameter listed in the Parameter table:

- If the parameter supports a fixed set of values, click on the corresponding Value field to activate a drop-down list of supported values, then select the required value.
- If the Value field displays <String> or <Number>, then you can type the required value.

The TL1 command field (the text field above the Run Command) is updated with the parameter values you selected in the Parameter table.

Note 1: The Value drop-down list contains the entire domain for the selected parameter.

Note 2: If a TL1 command includes a password parameter, then you must select a generic password in the password identifier (PID) value field of the Parameter table. You cannot type the actual password in the Parameter table when you edit TL1 commands in the TL1 Command Builder window. You can map the generic password to an actual password during script execution.

Note 3: The text field above the Run Command button is editable and you can further modify the command text if you wish. However, you have full responsibility for the syntax and parameter values you enter.

16 Click Add to Script to record the command to the script.

17 Repeat step 10 through step 16 to add more commands to the script.

Inserting comments, prompts, and delay commands to the script

18

If you want to	**Then** go to
insert a comment	step 19
insert a prompt command	step 21
insert a delay command	step 23
save the script	step 25

19 Select COMMENT from the Insert drop-down list, enter the text in the Value field, then press Enter to add the comment to the TL1 command field (the text field above the Run Command).

20 Click Add to Script to add the comment to the script.

Go to step 18.

21 Select PROMPT from the Insert drop-down list, enter the text in the Value field, then press Enter to add the prompt command to the TL1 command field (the text field above the Run Command).

22 Click Add to Script to add the prompt command to the script.

Go to step 18.

—continued—

Procedure 7-4 (continued)
Building a script

Step	Action
23	Select Delay Time (seconds) from the Insert drop-down list, enter the delay time in the Value field, then press Enter to add the delay command to the TL1 command field (the text field above the Run Command). ***Note:*** The delay value is the length of the pause before the next command in the script is executed. When the script runs and a delay line occurs, a progress dialog box will appear, informing the user about the delay period.
24	Click Add to Script to add the delay command to the script. Go to step 18.

Saving the script

Step	Action
25	Select Save As from the File drop-down menu in the TL1 Command Builder to open the Save As dialog box.
26	From the Look in drop-down list, select a folder location for the script file.
27	Type a file name for the script in the File name field.
28	Click Save.
29	Select Close from the File drop-down menu to close the script file. ***Note:*** If you want to run the script instead of closing it, you must be logged in to a network element. See Running a script on page 7-14.

—end—

Procedure 7-5
Loading a script

Use this procedure to display a previously saved script in the TL1 Command Builder.

Step	Action
1	Start the TL1 Command Builder. See Starting the TL1 Command Builder on page 7-2.
2	Select Open from the File drop-down menu in the TL1 Command Builder.
3	Find the location of the script file from the Look In drop-down list in the Open dialog box.
4	Select the file in the Look In area, and click Load to display the script in the Script area of the TL1 Command Builder.

—end—

Procedure 7-6
Editing a script

Use this procedure to edit a script.

Step	Action
1	Start the TL1 Command Builder. See Starting the TL1 Command Builder on page 7-2.
2	Select Batch from the Mode drop-down list. ***Note:*** If you are not logged in to a network element, Batch automatically appears in the Mode drop-down list and the Immediate option is not available.
3	If the script is not loaded, load the script. See Loading a script on page 7-10.
4	Click on the line in the script that you want to edit or copy by selecting it in the Script area.

—continued—

Procedure 7-6 (continued)

Editing a script

Step	Action	
5	**If** you want to	**Then**
	edit the selected line	click the Edit button. In the Edit Script Line dialog box, make the required changes to the script line, then click OK.
	delete the selected line	click the Delete button.
	move the selected line up or down one line in the script	click the Move Up or Move Down button, as required.
	cut the selected line and store it on the clipboard	select Cut Script from the Edit drop-down menu. To paste the line that you just cut above another line in the script, click on a line in the script, then select Insert Script from the Edit menu.
	copy the selected line to the clipboard	select Copy Script from the Edit drop-down menu. To paste the line that you just copied above another line in the script, click on a line in the script, then select Insert Script from the Edit drop-down menu.

Note: If you want to add commands to the script, or insert comments, prompt and delay commands, see Adding commands to the script or Inserting comments, prompts, and delay commands to the script in Building a script on page 7-6.

—continued—

Procedure 7-6 (continued)
Editing a script

Step	Action
6	Select Save from the File drop-down menu in the TL1 Command Builder to save the changes to the script. ***Note:*** If you want to save the edited script with a new name, select Save As from the File drop-down menu, and enter a new name for the script in the Save as dialog box.
7	Select Close from the File drop-down menu to close the TL1 Command Builder window. ***Note:*** If you want to run the script instead of closing it, you must be logged in to a network element. See Running a script on page 7-14.

—end—

Procedure 7-7
Running a script

Use this procedure to run a script using the TL1 Command Builder.

> ***Note:*** If you want to run a script across multiple network elements, they all must be within the network processor span of control.

Requirements

Before you perform this procedure, ensure that you use an account with the required user privilege code (UPC).

Step	Action
1	Ensure that you are logged in to the network element the script is referring to or to the network elements within the span of control. See Procedures for logging in to a network element on page 2-1.
2	Start the TL1 Command Builder. See Starting the TL1 Command Builder on page 7-2.
3	Select Batch from the Mode drop-down list.
4	Load the script. See Loading a script on page 7-10. ***Note:*** Ensure that the script does not refer to unsupported releases and is not in conflict with the software load of the network element. If the script contains unsupported commands, the network element will respond with an error.
5	Select a Script Mode: • Select Sequential to run the commands in the script one at a time. The next command is executed only when a response for the current command is received. • Select Continuous to run all the commands in the script without pauses between the commands. The next command is executed even if a response is not received for the previous command.
6	If you set the Script Mode to Sequential: • Select the Halt on Error check box, if you want the execution of the script to stop after the first command that fails. • Leave the Halt on Error check box unselected, if you want the script to continue even when more that one commands have failed.
7	Click Run Script. ***Note:*** The Results area displays the response message.

—continued—

Procedure 7-7 (continued)
Running a script

Step	Action
8	If there are generic TID (GenTID#), generic AID (GenAID#), or generic password (PASSWORD#) parameters in the script, you are prompted to map the generic parameters to actual values. ***Note 1:*** The Actual drop-down list in the Assign Generic TID dialog box contains the TIDs of the network elements to which you are logged in. ***Note 2:*** The Actual drop-down list in the Assign Generic AID dialog box contains valid AIDs for the selected command-parameter combinations. ***Note 3:*** Passwords are masked in the Assign Generic Passwords dialog box using asterisks (*). Passwords are not stored in scripts. Also, passwords are not displayed in the TL1 Command Builder window when you build or execute a script.
9	If you want to save the results of the script, click Save Result, then specify a folder location and file name for the results file.

—end—

Time of day synchronization

Procedures for time of day synchronization

Note: For an overview of time of day synchronization, see *Planning and Ordering Guide,* NTRN10AM.

Procedure 8-1
Editing time of day synchronization parameters on the network processor or network element

Use this procedure to edit the following time of day parameters on the network processor of network element:

- Status (network processor and network element)
- Offset threshold (network processor and network element)
- Minimum polling interval (network processor only)
- Maximum polling interval (network processor only)

Requirements

To perform this procedure, you must use an account with a level of 3 or higher.

Step **Action**

1 Login to the network processor or the network element. See Procedures for interface login and logout on page 2-1.

2 Ensure that the network processor or network element is selected in the navigation tree.

3 Select Node Information from the Configuration drop-down menu to open the Node Information window.

4 Select the Time of Day tab.

5 Click Edit (in the Settings area of the window) to open the Edit Time of Day settings dialog box.

6 Select the On radio button to activate time of day synchronization. Select the Off button to deactivate time of day synchronization.

Note: If the time of day synchronization feature is deactivated on the network processor, and the network processor has a provisioned time offset value, the network processor will take its reference time from its collocated shelf processor. As a result, the time reported on the network processor will be the reference time of the shelf processor, plus or minus the provisioned time offset. This will also result in the system generating events every 30 seconds to indicate that it cannot change the time of the network processor to that of the collocated shelf processor because of the time offset value. It is recommended that you change the time offset value of the network processor to 0 before deactivating the time of day synchronization feature. For more information on setting the time offset value, see Setting time offset and daylight savings offset on page 8-8.

—continued—

Procedure 8-1 (continued)
Editing time of day synchronization parameters on the network processor or network element

Step	Action

7

If you are editing time of day parameters on a	**Then** go to
network processor	step 8
network element	step 10

8 Select the number of seconds from the Minimum polling interval drop-down list.

9 Select the number of seconds from the Maximum polling interval drop-down list.

10 Select the number of seconds from the Offset threshold drop-down list.

11 Click OK to save the time of day parameters.

—end—

Procedure 8-2
Setting time of day servers on the network processors or network element

Use this procedure to:

- add, edit or delete up to five time of day timing servers (NTP servers) on the network processor
- add, edit or delete up to two network processor timing references on a network element shelf processor

Note 1: The shelf processor must be in the span of control of the network processor for the network processor to act as the shelf processors time of day- timing server.

Note 2: When the state of the server is unstable or displayed as “Unknown” then the network processor or shelf processor switches to another provisioned timing server.

Note 3: A “*” next to the timing source in Site Manager, indicates that it is the timing source being queried.

Requirements

To perform this procedure, you must

- use an account with a level of 3 or higher
- ensure you have the IP address of a network timing protocol (NTP) server, if you are provisioning the timing source for a network processor.

Step **Action**

1 Login to the network processor or the network element. See Procedures for interface login and logout on page 2-1.

2 Ensure that the network processor or network element is selected in the navigation tree.

3 Select Node Information from the Configuration drop-down menu to open the Node Information window.

4 Select the Time of Day tab.

5 Select an option:

If you are	**Then** go to
adding a timing server	step 6
editing a timing server	step 9
deleting a timing server	step 12

—continued—

Procedure 8-2 (continued)
Setting time of day servers on the network processors or network element

Step	Action
6	Click Add (in the Servers area of the window) to open the Add Time of Day servers dialog box.
	Note: If maximum number of timing servers are provisioned (five for network processor and two for SP), the Add button is disabled.
7	Select a Source value from the Source drop-down list.
	Note: If a source value is already provisioned it does not appear in the drop down list.
8	Select an option:

If you are adding a server to a	**Then** enter the
network processor	IP address of the timing server and go to step 15
network element	the ID of the network processor that will be the master timing source for this network element. ***Note:*** Use the Find button to view available network processors in the network. Go to step 15.

Step	Action
9	Click Edit (in the Servers area of the window) to open the Edit Time of Day servers dialog box.
10	Select a Source from the Source drop-down list.
11	Edit the IP address of the timing server on the network processor or edit the network processor TID on the network element. Go to step 15.
12	Select a server source from the Node Information window (in the Servers area).
13	Click Delete (in the Servers area of the window) to delete the selected server.
14	Click OK to confirm the delete. This procedure is complete.
15	Do one of the following: • Click Apply to save the server details and keep the dialog box open for additional changes. • Click OK to save the server details and return to the Node Information window (Time of Day tab).

—end—

Procedure 8-3
Operating a time of day synchronization on the network processors or network element

Use this procedure to:

- force the network processor to attempt to reference its internal clock to one of its provisioned external timing servers
- force the shelf processor to attempt to reference its internal clock to one of its provisioned network processor timing servers

Requirements

To perform this procedure, you must use an account with a level of 3 or higher

Step	Action
1	Ensure the status parameter is on, see Editing time of day synchronization parameters on the network processor or network element on page 8-2.
2	Ensure the time of day timing source is provisioned, see Setting time of day servers on the network processors or network element on page 8-4.
3	Login to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
4	Ensure that the network processor or network element is selected in the navigation tree.
5	Select Node Information from the Configuration drop-down menu to open the Node Information window.
6	Select the Time of Day tab.
7	Click Synchronize (in the Servers area of the window) to initiate a time of day synchronization.

—end—

Procedure 8-4
Displaying time of day server details and parameters

Use this procedure to display the following server details and parameters on the network processor and or network element:

- Status (network processor and network element)
- Offset threshold (network processor and network element)
- Server source, address, and status (network processor and network element)
- Minimum polling interval (network processor only)
- Maximum polling interval (network processor only)
- Time of Day (network processor only)
- Detected offset (network processor only)
- Polling interval (network processor only)
- Next synchronization (network processor only)
- Last synchronization (network processor only)

Note: For a description of all time of day parameters, refer to the *Planning and Ordering Guide,* NTRN10AM.

Step	Action
1	Login to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the network processor or network element is selected in the navigation tree.
3	Select Node Information from the Configuration drop-down menu to open the Node Information window.
4	Select the Time of Day tab to display the time of day server details and parameters.

—end—

Procedure 8-5
Setting time offset and daylight savings offset

Use this procedure to set the following time of day synchronization parameters: time offset and daylight savings offset.

Time offset is the difference between the network elements real time clock and the reference time of the time of day synchronization source (the master clock). For example, if reference time is GMT, (most NTP servers use GMT as reference), you will need to set a -3 hour offset (-180 minutes) if the real time clock on the element is to report its time as GMT -3 hours.

Daylight savings offset is the difference between the network elements real time clock and the time offset during daylight saving periods. For example, if reference time is GMT, and the time offset is -3 hours, and the daylight savings period adjustment is 1 hour (report time on the element as GMT -2 hour during daylight savings periods), you will need to set a 60 minute daylight savings offset.

In Site Manager, time offset can have a positive or negative value ranging from 0 to 720 minutes. See Time offset values for each time zone on page 8-11.

> ***Note 1:*** The following web site provides time zone and daylight savings time data: http//www.timeanddate.com/worldclock/full.html?sort=2
>
> ***Note 2:*** To provision a geographic time zone label, see Changing the network element or network processor date, time, and time zone on page 3-40.

Step	Action
1	Login to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the network processor or network element is selected in the navigation tree.
3	Select Node Information from the Configuration drop-down menu.
4	Select the General tab.
5	Click Edit (under General) to open the Edit General dialog box.
6	Select Time Zone from the Parameter drop-down list.
7	Indicate using the radio buttons, if the time offset is positive or negative.

—continued—

Procedure 8-5 (continued)

Setting time offset and daylight savings offset

Step	Action
8	Enter a value between 0 and 720 minutes in the Time offset field. See Time offset values for each time zone on page 8-11 for more information. ***Note:*** If the time of day synchronization feature is deactivated on the network processor, and the network processor has a provisioned time offset value, the network processor will take its reference time from its collocated shelf processor. As a result, the time reported on the network processor will be the reference time of the shelf processor, plus or minus the provisioned time offset. This will also result in the system generating events every 30 seconds to indicate that it cannot change the time of the network processor to that of the collocated shelf processor because of the time offset value. It is recommended that you change the time offset value of the network processor to 0 before deactivating the time of day synchronization feature.
9	See the If/Then table below.

Step 9:

If	**Then**
you are using daylight savings time	select the Yes radio button and then go to step 10
otherwise	select the No radio button and then go to step 26

10 Enter the daylight saving time offset (reference time offset value) from 0 to 120 minutes (up to 2 hours) that will occur when daylight savings time takes effect.

11 Select an option for when the daylight savings time starts:

If you want to set the start date with	**Then** go to
an exact date in a given month	step 12
a particular day of a particular week	step 15

12 Enter 0 in the start date week field.

13 Enter the exact date in the day field (value from 1 to 31, depending on the month).

14 Enter the month and start time.

Go to step 18.

15 Enter a value between 1 and 5 in the start date field (for example, “1” represents the first week of the month).

16 Enter a day in the day field.

17 Enter the month and start time.

—continued—

Procedure 8-5 (continued)
Setting time offset and daylight savings offset

Step	Action
18	Select an option for when the daylight savings time ends:

If you want to set the end date with	**Then** go to
an exact date in a given month	step 19
a particular day of a particular week	step 22

Step	Action
19	Enter 0 in the end date week field.
20	Enter the exact date in the day field (value from 1 to 31, depending on the month).
21	Enter the month and end time. Go to step 25.
22	Enter a value between 1 and 5 in the end date field (for example, “1” represents the first week of the month).
23	Enter a day in the day field.
24	Enter the month and end time.
25	Select the Yes radio button to have the next day light savings period automatically calculated or No, if the next daylight savings time period will be entered.
26	Do one of the following: • Click Apply to save the offset and daylight savings time details and keep the dialog box open for additional changes. • Click OK to save the offset and daylight savings time details and return to the Node Information window (General tab).

—end—

Time offset values for each time zone

Standard time zones	**Time offset (in minutes)**
GMT -10:00: Hawaiian Standard Time	-600 minutes
GMT -10:00: Aleutian standard/daylight time	-600 minutes
GMT -9:00: Yukon Standard Time	-540 minutes
GMT -9:00: Yukon Standard time/daylight Time	-540 minutes
GMT -8:00: Pacific Standard time	-480 minutes
GMT -8:00: Pacific Standard/daylight time	-480 minutes
GMT -7:00: Mountain standard time	-420 minutes
GMT -7:00: Mountain standard/daylight time	-420 minutes
GMT -6:00: Central standard time	-360 minutes
GMT -6:00: Central standard/daylight time	-360 minutes
GMT -5:00: Eastern standard time	-300 minutes
GMT -5:00: Eastern standard/central daylight time	-300 minutes
GMT -5:00: Eastern standard/daylight time	-300 minutes
GMT -4:00: Atlantic standard time	-240 minutes
GMT -4:00: Atlantic standard/daylight time	-240 minutes
GMT -3:30: Newfoundland standard/daylight time	-210 minutes
GMT -3:00: Argentina standard time	-180 minutes
GMT 0:00: Greenwich Mean time	0 minutes
GMT 0:00: Greenwich Mean time/British summer time	0 minutes
GMT 0:00: Portuguese winter/summer time	0 minutes
GMT 0:00: Western European/daylight savings time	0 minutes
GMT +1:00: Middle European time	+60 minutes
GMT +1:00: Middle European standard/daylight time	+60 minutes
GMT +2:00: Middle European time	+120 minutes
GMT +3:00: Eastern European time	+180 minutes
GMT +3:00: South African standard/daylight time	+180 minutes
GMT +4:00: Western Asian time	+240 minutes

Standard time zones	**Time offset (in minutes)**
GMT +5:00: Western Asian time	+300 minutes
GMT +6:00: Middle Asian time	+360 minutes
GMT +7:00: Middle Asian time	+420 minutes
GMT +8:00: Australian western standard time	+480 minutes
GMT +9:00: Japan standard time	+540 minutes
GMT +9:00: Korean standard time	+540 minutes
GMT +9:30: Australian central standard time	+570 minutes
GMT +9:30: Australian central standard/daylight time	+570 minutes
GMT +10:00: Australian eastern standard time	+600 minutes
GMT +10:00: Australian eastern standard/daylight time	+600 minutes
GMT +12:00: New Zealand standard/daylight time	+720 minutes

Login banner and general broadcast message tool

Procedures for the login banner

Procedures for the general broadcast message tool

Note: For an overview of the login banner and general broadcast tool, see *Planning and Ordering Guide,* NTRN10AM.

Procedure 9-1
Editing or replacing the login banner

Use this procedure to:

- edit the login banner text manually
- replace the current login banner text with the default login banner
- replace the current login banner text with the backup login banner saved to a file

Requirements

To perform this procedure, you must use an account with a level of 4 or higher.

Step	Action
1	Login to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the network processor or network element is selected in the navigation tree.
3	Select Node Information from the Configuration drop-down menu to open the Node Information window. ***Note:*** The Node Information window is automatically displayed after you log in to a network element or network processor.
4	Ensure the Login Banner tab is displayed.
5	See the table below.

If you want to	**Then** go to
edit the login banner text manually	step 6
replace the current login banner with the default login banner	step 11
replace the current login banner with the backup login banner saved to a file	step 13

Edit the login banner text manually

Step	Action
6	Click Edit (under Login Banner) to open the Edit Login Banner dialog box.
7	Select the current text and modify it as required.
8	Click Apply to save the modified text.
9	Click OK to close the Edit Login Banner dialog box closes and return to the Node Information window (Login Banner tab). The modified text appears in the login banner.
10	You have completed this procedure.

—continued—

Procedure 9-1 (continued)
Editing or replacing the login banner

Step	Action

Replace the current login banner with the default login banner

11 Click Replace with Default (under Login Banner) to display the default login banner text.

12 You have completed this procedure.

Replace the current login banner with the backup login banner

13 Click Replace with Backup (under Login Banner) to display the backup login banner text.

—end—

Procedure 9-2
Saving the login banner to a backup file

Use this procedure to save the current login banner to a file.

Requirements

To perform this procedure, you must use an account with a level of 4 or higher.

Step	Action
1	Login to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the network processor or network element is selected in the navigation tree.
3	Select Node Information from the Configuration drop-down menu to open the Node Information window. ***Note:*** The Node Information window is automatically displayed after you log in to a network element or network processor.
4	Ensure the Login Banner tab is displayed.
5	Click Set as Backup (under Login Banner) to save this login banner to a file on the network element.

—end—

Procedure 9-3
Refreshing the login banner

Use this procedure to display the latest login banner text.

Step	Action
1	Login to the network processor or the network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the network processor or network element is selected in the navigation tree.
3	Select Node Information from the Configuration drop-down menu to open the Node Information window. ***Note:*** The Node Information window is automatically displayed after you log in to a network element or network processor.
4	Ensure the Login Banner tab is displayed.
5	Click Refresh (under Login Banner) to display the latest login banner text The system displays the message “Retrieving login banner...Done”. The system also updates the “Last refresh:” label with the time when you retrieved this login banner text.

—end—

Procedure 9-4
Sending and viewing messages with the general broadcast tool

Use this procedure to send messages to other network elements with the general broadcast tool.

> ***Note:*** The general broadcast tool is only available on OPTera Metro 3500 network elements running Release 12 or later.

Requirements

Both you and the user you want to communicate with must be logged in to the same network element. This allows you to send messages to and receive messages from this user through this network element.

Step	Action
1	Login to the network processor or network element. See Procedures for interface login and logout on page 2-1.
2	Ensure that the network processor or network element is selected in the navigation tree.
3	Select General Broadcast from the Tools submenu of the File drop-down menu. The General Broadcast window opens.
4	

If you want to	**Then** go to
send a message	step 5
view a received message	step 9
close the general broadcast tool	step 10

Sending a message

Step	Action
5	In the General Broadcast window, select the network element to which you want to send a message from the To drop-down list. Select All to send your message to all network elements. ***Note:*** The network elements listed in the To drop-down list are the network elements you are currently logged in to. The All option represents all of the network elements you are logged in to (all of the network elements in the To drop-down list).
6	In the General Broadcast window, place the cursor in the open text box.

—continued—

Procedure 9-4 (continued)
Sending and viewing messages with the general broadcast tool

Step	Action
7	Type your message in this text box. Your message can have up to 124 characters.
	Note: If you want to copy and send text from a received message, you can only copy and paste one line of text at a time from the received message into the open text box.
8	Click Send to send your message to the selected network element.

Viewing a received message

9 Ensure the “Show when messages received” option is selected in the General Broadcast window.

If this option is selected and you bring other Site Manager windows to the foreground, the General Broadcast window reappears when you receive a message.

If this option is not selected, the General Broadcast window remains in the background (behind other windows) even if you receive a message.

Received messages appear in the status area of the General Broadcast window, above the open text box.

Closing the general broadcast tool

10 In the General Broadcast window, select Close from the File drop-down menu to close the General Broadcast window.

—end—

Terms and conditions

Completion of a purchase agreement is required prior to purchasing OPTera Metro 3500 products and/or services. Contact one of the following:

- your Nortel Networks sales person
- telephone: Suzanne Calton (972) 685-2888
- email CONTMGNT@nortelnetworks.com

Statement of Conditions

Portions of the code in this software may be Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994 The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3 All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4 Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of the code in this software may be Copyright © 1988 Juniper Networks, Inc. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of the code in this software may be Copyright © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the “RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as “derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided “as is” without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software. $FreeBSD: src/lib/libmd/md5c.c,v 1.11 1999/12/29 05:04:20 peter Exp $This code is the same as the code published by RSA Inc. It has been edited for clarity and style only.

Nortel Networks

OPTera Metro 3500 Multiservice Platform

Security and Administration

The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose the information only to its employees with a need to know, and shall protect the information, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

323-1059-302
Standard   Issue 1   Release 12.0
November 2003
Printed in Canada

NORTEL
NETWORKS™