NT0H65AM 323-1701-310

Nortel

Optical Metro 5100/5200

Provisioning and Operating Procedures, Part 1 of 2

Standard Release 8.0 Issue 1 April 2005

What's inside...

Using the System Manager
Managing security and user accounts

See Part 2 for the following:

Provisioning circuit packs and managing traffic
Shelf management procedures
Upgrading Optical Metro 5100/5200 software
Optical Trunk Switch OAM&P
Performance monitoring procedures
Enhanced Trunk Switch OAM&P

NORTEL

Printed in Canada and the United Kingdom

Contents

About this document v

Audience for this document v
Optical Metro 5100/5200 library vi
Technical assistance service telephone numbers viii

Using the System Manager 1-1

User levels and access privileges 1-2
Access to the System Manager through IP addresses 1-3

List of procedures

1-1 Logging into the network 1-7
1-2 Editing the naming, timing, and basic communications settings 1-12
1-3 Setting the DCN gateway and editing the DCN gateway function settings 1-17
1-4 Viewing detailed event history 1-20
1-5 Viewing the event console 1-21
1-6 Saving event logs 1-22
1-7 Printing event lists 1-24
1-8 Clearing the event console 1-25
1-9 Configuring telemetry ports and alarms 1-27
1-10 Provisioning alarm severity on a shelf 1-31
1-11 Restoring the severity of an alarm to its default on a shelf 1-33
1-12 Saving the alarm list 1-34
1-13 Printing the alarm list 1-35
1-14 Acknowledging visual alarms 1-36
1-15 Selecting shelves 1-38
1-16 Sorting shelves 1-40
1-17 Sorting information 1-42
1-18 Saving information 1-44
1-19 Printing information 1-45
1-20 Modifying, adding, deleting, and viewing details 1-46
1-21 Querying the inventory list 1-47
1-22 Querying facilities 1-48
1-23 Querying channel assignments 1-49
1-24 Changing the date and time on a shelf 1-50
1-25 Provisioning Ethernet port alarms 1-51
1-26 Provisioning Ethernet and serial ports 1-53
1-27 Provisioning Ethernet port 2 access control 1-55
1-28 Provisioning IP forwarding on Ethernet port 1 1-58

1-29 Defining or changing advanced communications settings for the network 1-59
1-30 Assigning IP addresses for Ethernet port 2 and Serial port 1 1-62
1-31 Enabling or disabling the DNS proxy service 1-65
1-32 Setting up the DNS proxy service 1-67
1-33 Converting from private IP addressing to public IP addressing 1-70
1-34 Converting from public IP addressing to private IP addressing 1-81
1-35 Changing the target identifier (TID) properties 1-93
1-36 Backing up shelf configuration data 1-95
1-37 Restoring shelf configuration data 1-98
1-38 Changing clock reference settings for the OCI SRM SONET/SDH 1310 nm 1-102
1-39 Performing a health check 1-104
1-40 Saving a health check report 1-107
1-41 Displaying shelf level graphics 1-109
1-42 Displaying shelf level graphic details for a shelf circuit pack 1-111
1-43 Enabling or disabling automatic laser shutdown 1-112
1-44 Enabling or disabling automatic laser recovery 1-113
1-45 Enabling manual laser recovery 1-115
1-46 Enabling or disabling remote fault notification 1-116
1-47 Enabling or disabling passive slot numbering 1-117
1-48 Exiting the System Manager 1-118

Managing security and user accounts 2-1

List of procedures

2-1 Viewing user account details for a shelf 2-3
2-2 Adding a user account 2-4
2-3 Changing a user account 2-6
2-4 Deleting a user account 2-10
2-5 Viewing the login user list 2-12
2-6 Changing your password 2-13
2-7 Changing the community name 2-15
2-8 Setting the centralized security administration attributes 2-18
2-9 Setting intrusion attempts handling 2-21
2-10 Setting the primary or secondary RADIUS server attributes 2-22
2-11 Changing the challenge/response shared secret for a shelf 2-24
2-12 Changing the shared secret for the primary or secondary RADIUS server 2-25
2-13 Clearing security alarms 2-26

About this document

ATTENTION

This document is presented in two parts: Part 1 and Part 2. Each part has its own table of contents. The table of contents in Part 1 contains topics found in Part 1 only. The table of contents in Part 2 contains topics found in Part 2 only.

You are reading Part 1 of the *Provisioning and Operating Procedures*, 323-1701-310.

This document provides information about using the System Manager interface to provision and operate the Nortel Optical Metro 5100/5200 (identified prior to Release 7 as Nortel Networks OPTera Metro 5000-series Multiservice Platform).

Part 1 of the *Provisioning and Operating Procedures* covers the following:

- using the System Manager
- managing security and user accounts

Part 2 of the *Provisioning and Operating Procedures* covers the following:

- provisioning circuit packs and managing traffic
- shelf management procedures
- upgrading the software
- operating the Optical Trunk Switch
- procedures for performance monitoring
- operating the Enhanced Trunk Switch

Audience for this document

This document is intended for the following audience:

- strategic and current planners
- provisioners
- installers
- transmission standards engineers

- field maintenance engineers
- system line-up and testing (SLAT) personnel
- maintenance technicians
- network administrators

Optical Metro 5100/5200 library

The Optical Metro 5100/5200 library consists of the *Nortel Optical Metro 5100/5200 Technical Publications*, NT0H65AM.

Technical Publications

The *Optical Metro 5100/5200 Nortel Technical Publications* (NTP) consist of descriptive information and procedures.

Descriptive information

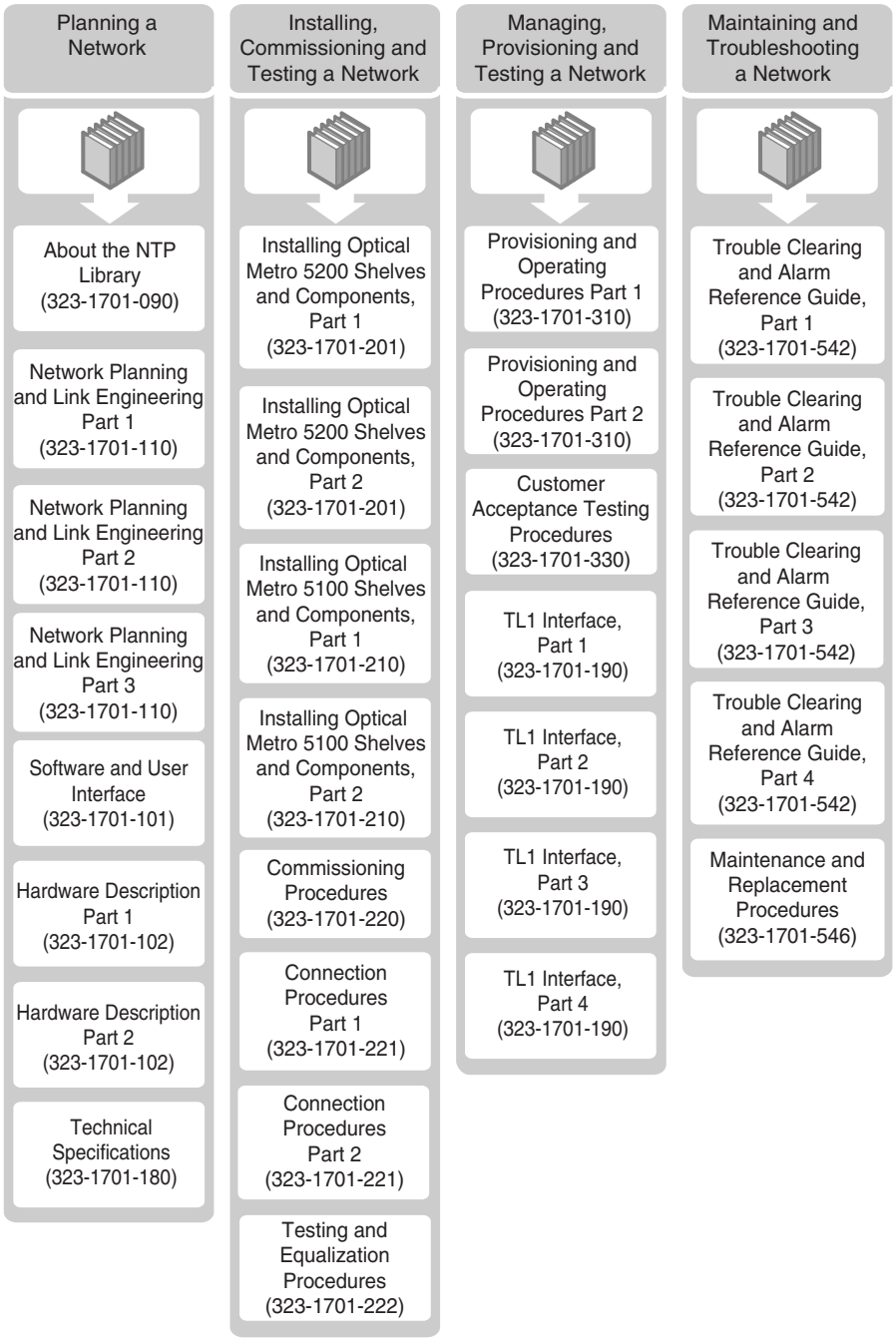
These NTPs provide detailed descriptive information about the Optical Metro 5100/5200, including system software and hardware descriptions, technical specifications, ordering information, and TL1 user information.

Procedures

These NTPs contain all procedures required to install, provision, and maintain the Optical Metro 5100/5200.

The following roadmap lists the documents in the Optical Metro 5100/5200 library.

OM2805p



Technical assistance service telephone numbers

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.nortel.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.nortel.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.nortel.com. Click on the Contact Us link.

Using the System Manager

Follow the procedures in this chapter to use the System Manager.

The System Manager is accessible by connecting:

- remotely to a commissioned shelf through a LAN (see Procedure 1-1, "Logging into the network" in this book)
- locally to a commissioned shelf using Ethernet port 1 or port 2 (see Procedure 1-8, "Connecting locally to a commissioned shelf using Ethernet port 1 or port 2 and configuring DHCP (Windows 2000/NT/XP)" in *Commissioning Procedures*, 323-1701-220
- locally to a commissioned GNE shelf using Ethernet port 1 (see Procedure 1-9, "Connecting locally to a commissioned GNE shelf using Ethernet port 1 and configuring a static IP address (Windows 2000/NT/XP)" in *Commissioning Procedures*, 323-1701-220

  Note: For detailed information about System Manager windows, refer to the "Appendix—System Manager windows and fields" chapter in *Software and User Interface*, 323-1701-101.

Before you begin

Before you begin the procedures in this chapter, make sure you have

- read about the System Manager and its functions in the "System Manager" chapter of *Software and User Interface*, 323-1701-101
- completed the installation of the System Manager and the Web browser using the procedures in the "Installing the System Manager" chapter in *Commissioning Procedures,* 323-1701-220
- correctly configured a remote connection between the System Manager computer and the Optical Metro 5100/5200 network, if required, according to the procedures in the "Configuring a remote connection to the System Manager" chapter in *Commissioning Procedures,* 323-1701-220

- some of the procedures in this section are specific to a shelf. Follow Procedure 1-15 "Selecting shelves" to select the shelf you need to perform the procedure on.

ATTENTION

If the "Software Library Missing" alarm is raised on a shelf, the System Manager may not correctly display information about the shelf, or the circuit packs that are seated in the shelf. To clear the alarm, follow Procedure 13-13 "Shelf—Software Library Missing" in *Trouble Clearing and Alarm Reference Guide*, 323-1701-542.

ATTENTION

Nortel Networks recommends the following background color settings for platforms running System Manager:
for Unix: Default
for Windows: Windows Standard

User levels and access privileges

There are different levels of user access and privilege. Table 1-1 lists descriptions of the different user privileges.

Table 1-1
System Manager user levels and privileges

User level	Description
Admin	The system administrator • has read and write access to all of the system • can change user profile attributes • can commission and decommission shelves • can view and clear security events and alarms • can provision the severity of any alarm using System Manager
Operator	The typical user class • has read and write access to most of the system • can change user's own password • cannot commission or decommission shelves • cannot perform software upgrade • cannot view or clear security events and alarms
Observer	This user has read-only access; however, can change user's own password.

Table 1-1 (continued)
System Manager user levels and privileges

User level	Description
Customer1 (see Note)	The Customer1 user • can access PM data • has read-only access to their customer owned network (equipment, facility and channel assignments) • can change own password • only sees service affecting alarms plus AIS, LOS, RDI, Optical Power, Far End Client Rx Signal Fail and PM alarms, that concern their operation. All other events, user requests, and non-service affecting alarms are filtered. • can access PM data • cannot log into an Optical Metro 5100/5200 shelves using TL1 interfaces, although this user class can be provisioned through TL1 commands
Customer2 (see Note)	The Customer2 user has the same access and privileges Customer1 except, Customer 2 cannot access PM data and AIS, LOS, RDI, Optical Power, Far End Client Rx Signal Fail and PM alarms are not displayed.
Note: For a listing of the tabs and menu items that are enabled and disabled in SMI for this user class, see "System Manager access privileges for the customer user classes" in *Software and User Interface,* 323-1701-101.	

Note: Make sure to protect your passwords to the System Manager. If you do not remember your password, you must contact the Nortel Networks Technical support to access the shelves.

Access to the System Manager through IP addresses

By default, you access Optical Metro 5100/5200 shelves using uniform resource locator (URL) IP addresses. Your network administrator can configure your system to use shelf names or IP addresses, such as DNS entries that map user defined shelf names to their related IP address. If your network environment does not use DNS, your network administrator can create entries in the example files listed below to map shelf names to IP addresses.

- /etc/hosts (for Unix)
- C:\winnt\system32\drivers\etc\Hosts (for Windows NT, Windows 2000, Windows XP)
- C:\windows\Hosts (for Windows 98)

Optical Metro 5100/5200 network elements managed by OMEA

When Optical Metro 5100/5200 network elements are managed by OMEA, there are some cases, when rediscovery is insufficient to recover from a network configuration change.

If you must change any of the following items for Optical Metro 5100/5200 network elements, do not make the change and then attempt to rediscover the NE. The correct procedure is as follows: first delete the NE from OMEA and then make the change, and finally manage the NE again.

- change the Site ID (this change will affect the default NE TID)
- change the security authentication mode (Local/Centralized) for the NE (relevant for all configurations—private or public IP configurations)
- change the NE configuration (for example, change the NE TID or NE IP address) (relevant for all configurations—private or public IP configurations)
- change the configuration of either the principal or standby gateway so that it is no longer functioning as a gateway for the ring (relevant for private IP configurations only)

See *Optical Manager Element Adapter, Standard Operations Guide,* 450-3121-301, for procedures on deleting a network element and managing a network element.

Procedure list

Table 1-2 lists the procedures in this chapter.

Table 1-2
System Manager operation procedures

Procedure	Page	Comments
1-1 Logging into the network	1-7	Required to perform most commissioning, provisioning, operating, and test procedures.
1-2 Editing the naming, timing, and basic communications settings	1-12	Optional. Always perform a backup after editing shelf configurations.
1-3 Setting the DCN gateway and editing the DCN gateway function settings	1-17	Optional.
1-4 Viewing detailed event history	1-20	Optional.
1-5 Viewing the event console	1-21	Optional.
1-6 Saving event logs	1-22	Perform this procedure before replacing an SP circuit pack.
1-7 Printing event lists	1-24	Optional.
1-8 Clearing the event console	1-25	Optional.

Table 1-2 (continued)
System Manager operation procedures

Procedure	Page	Comments
1-9 Configuring telemetry ports and alarms	1-27	Optional.
1-10 Provisioning alarm severity on a shelf	1-31	Optional.
1-11 Restoring the severity of an alarm to its default on a shelf	1-33	Optional.
1-12 Saving the alarm list	1-34	Optional.
1-13 Printing the alarm list	1-35	Optional.
1-14 Acknowledging visual alarms	1-36	Optional.
1-15 Selecting shelves	1-38	Optional.
1-16 Sorting shelves	1-40	Optional.
1-17 Sorting information	1-42	Optional.
1-18 Saving information	1-44	Optional.
1-19 Printing information	1-45	Optional.
1-20 Modifying, adding, deleting, and viewing details	1-46	Optional.
1-21 Querying the inventory list	1-47	Optional.
1-22 Querying facilities	1-48	Optional.
1-23 Querying channel assignments	1-49	Optional.
1-24 Changing the date and time on a shelf	1-50	Optional.
1-25 Provisioning Ethernet port alarms	1-51	Optional.
1-26 Provisioning Ethernet and serial ports	1-53	Optional.
1-27 Provisioning Ethernet port 2 access control	1-55	Optional.
1-28 Provisioning IP forwarding on Ethernet port 1	1-58	Optional.
1-29 Defining or changing advanced communications settings for the network	1-59	Optional. Always perform a backup of the affected shelves after changing IP addresses and communication settings.
1-30 Assigning IP addresses for Ethernet port 2 and Serial port 1	1-62	Optional.
1-31 Enabling or disabling the DNS proxy service	1-65	Optional.

Table 1-2 (continued)
System Manager operation procedures

Procedure	Page	Comments
1-32 Setting up the DNS proxy service	1-67	Optional.
1-33 Converting from private IP addressing to public IP addressing	1-70	Optional.
1-34 Converting from public IP addressing to private IP addressing	1-81	Optional.
1-35 Changing the target identifier (TID) properties	1-93	Optional.
1-36 Backing up shelf configuration data	1-95	Strongly recommended after commissioning a new shelf, or changes to shelf configurations, shelf passwords or IP addresses.
1-37 Restoring shelf configuration data	1-98	Required in the event of shelf failure.
1-38 Changing clock reference settings for the OCI SRM SONET/SDH 1310 nm	1-102	Optional.
1-39 Performing a health check	1-104	Recommended for each shelf after a software upgrade to review the results.
1-40 Saving a health check report	1-107	Optional.
1-41 Displaying shelf level graphics	1-109	Optional.
1-42 Displaying shelf level graphic details for a shelf circuit pack	1-111	Optional.
1-43 Enabling or disabling automatic laser shutdown	1-112	Optional.
1-44 Enabling or disabling automatic laser recovery	1-113	Optional.
1-45 Enabling manual laser recovery	1-115	Optional.
1-46 Enabling or disabling remote fault notification	1-116	Optional.
1-47 Enabling or disabling passive slot numbering	1-117	Optional.
1-48 Exiting the System Manager	1-118	Optional.

Procedure 1-1
Logging into the network

Use this procedure to log into the Optical Metro 5100/5200 network through the System Manager.

This procedure is required to commission, provision, operate, and test the Optical Metro 5100/5200 network.

Note: You can launch System Manager using Exceed version 9.0. This can be done using the following methods:

— Start an Exceed session against a Solaris workstation and then use Netscape on the Solaris workstation to launch a System Manager session

— Start an Exceed session against a Optical Network Manager workstation and then use the Graphical Network Browser to launch a System Manager session.

Requirements

Before you begin this procedure, make sure that you

- have a PC, a Solaris workstation, or a Optical Network Manager workstation to log into the Optical Metro 5100/5200 network
- know your user ID and password to log on to the primary shelf of your network

  Note 1: If Centralized authentication mode is used, the RADIUS server is not reachable and the alternate login method is set to Local User, you need to know the user ID and password of a local user provisioned at the primary shelf.

  Note 2: If Centralized authentication mode is used, the RADIUS server is not reachable and the alternate login method is set to Challenge/Response, you need to contact your administrator to get the Challenge Response code.
- have the System Manager installed and configured for running on an Internet Explorer or Netscape Communicator Web browser. (Follow procedures in "Installing the System Manager" chapter in *Commissioning Procedures*, 323-1701-220)
- correctly configured a remote connection between the System Manager computer and the Optical Metro 5100/5200 network, if required, according to the procedures in the "Configuring a remote connection to the System Manager" chapter in *Commissioning Procedures,* 323-1701-220

—continued—

Procedure 1-1 (continued)
Logging into the network

Action

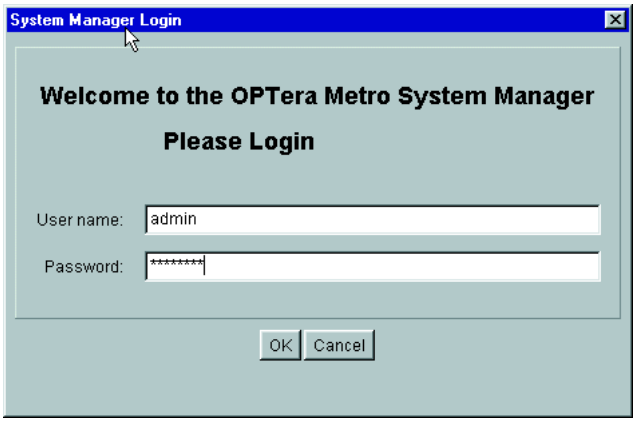
Step	Action
1	Determine your access strategy. You can use a PC, a Solaris workstation, or a Optical Network Manager workstation to log into the Optical Metro 5100/5200 network.
2	**If** / **Then** go to you are using the Optical Network Manager Graphical Network Browser (GNB) — step 3 otherwise — step 4
3	In the Optical Network Manager GNB: **a.** find the primary shelf for your network **b.** double-click on the shelf After up to 15 seconds, the System Manager Login dialog opens. Go to step 9.
4	Open the Web browser.
5	In the Address (URL) field of the Web browser, enter the IP address of the primary shelf. *The Optical Metro–Nortel Networks page appears.* ***Note:*** If your Web browser shows the status message “detecting proxy settings...” for more than 30 seconds, contact your LAN administrator.
6	In the Optical Metro window, click **Start the System Manager**. *The Optical Metro—System Manager Web page appears, the system checks for the required security certificate and downloads the required Java applet.*
7	**If** / **Then** go to the System Manager Login dialog appears — step 9 the Warning - Security dialog appears — step 8

—continued—

Procedure 1-1 (continued)
Logging into the network

Step	Action
8	Click on the **Always** button to indicate that you trust the signed applet. *The System Manager Login dialog box appears.*

OM0864t



9 In the System Manager Login dialog box

a. enter your user ID in the “User name” field

b. enter your user password in the “Password” field

c. click **OK**

Note 1: The System Manager password is case sensitive.

Note 2: If you click **Cancel** or if the number of login failures equal the provisioned Failed Login Attempt Threshold, the System Manager Login dialog box and the System Manager automatically close.

A Warning Notice dialog box appears if Local authentication mode is provisioned, if Centralized authentication mode is provisioned and the Radius server is reachable, or if Centralized authentication mode is provisioned, the Radius server is not reachable, the alternate login method is set to Local User, and the User name and password is provisioned at the network element as a Local user.

The Challenge Response dialog is displayed if Centralized authentication mode is provisioned, the Radius server is not reachable, and the alternate login method is set to Challenge Response.

The Login failed dialog with message “Centralized authentication is unavailable, please use local user authentication” is displayed if Centralized authentication mode is provisioned, the Radius server is not reachable, the alternate login method is set to Local User, and the User name and password is not provisioned at the network element as a Local user.

—continued—

Procedure 1-1 (continued)
Logging into the network

Step	Action

10

If	Then go to
the Warning Notice dialog appears	step 17
the Challenge Response dialog appears	step 13
the Login failed dialog with message “Centralized authentication is unavailable, please use local user authentication” appears	step 11

11 In the Login failed dialog, click **Close**.

The System Manager Login dialog box appears.

12 Go to step 9 and enter a User name and password that is provisioned as a local user at the network element.

13 Obtain the Challenge Response code. Contact your administrator to get the Challenge Response code. The Challenge Response code can be obtained using the Challenge Response Tool. The Challenge Response Tool is available as part of the Optical Manager Element Adaptor or as a standalone application, which can be installed and executed on a computer. Refer to the *Challenge Response Tool User Guide* for more information.

14 Enter the Challenge Response code in the Response field of the Challenge Response dialog and then click **OK**.

A Warning Notice dialog box appears.

15 In the Warning Notice dialog box, click **OK**.

The main window of the System Manager appears.

16 Go to step 24.

17 In the Warning Notice dialog box, click **OK**.

The main window of the System Manager appears, the Login Information dialog appears, the Password Expiry Warning dialog appears or the Login Warning dialog appears. The Login Information dialog appears if Centralized authentication mode is provisioned and the Radius server is reachable. The Login Warning dialog appears if Centralized authentication mode is provisioned, the Radius server is not reachable and the alternate login method is set to Local User.

18

If	Then go to
the Password Expiry Warning dialog appears	step 19
the Login Warning dialog appears	step 21
the Login Information dialog appears	step 23
otherwise	step 24

—continued—

Procedure 1-1 (continued)
Logging into the network

Step	Action
19	In the Password Expiry Warning dialog, click **Close**. *The Login Information dialog appears.*
20	Go to step 23.
21	In the Login Warning dialog, click **Close**. *The main window of the System Manager appears.*
22	Go to step 24.
23	In the Login Information dialog, click **Close**. *The main window of the System Manager appears.*
24	In the System Manager main window **a.** click the maximize button **b.** click on the **Selected Shelves** drop-down list to display the network tree

—end—

Procedure 1-2
Editing the naming, timing, and basic communications settings

Use this procedure to edit the naming, timing and basic communications settings.

See Procedure 1-3 "Setting the DCN gateway and editing the DCN gateway function settings" for information on editing the DCN gateway function settings. See Procedure 1-29 "Defining or changing advanced communications settings for the network" for information on editing advanced communications settings and IP addressing.

When you change shelf configuration data, System Manager may initiate a shelf restart. Table 1-3 on page 1-15, Table 1-4 on page 1-15, and Table 1-5 on page 1-16 list the fields that initiate a shelf restart following configuration changes.

Requirements

You must be an Admin level user to edit configuration information on the shelf.

Precautions

CAUTION
Risk of loss of access to one or more shelves
If you provision incorrect information in the Configuration window, you can lose access to one or more shelves and impact intershelf communication.

CAUTION
Risk of incorrect backup file
After you edit shelf configuration data, backup the configuration data of all affected shelves. See Procedure 1-36 "Backing up shelf configuration data" for details.

—continued—

Procedure 1-2 (continued)
Editing the naming, timing, and basic communications settings

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Configuration tab.
3	Select the Naming or Communications tab.
4	Double-click on the line that you want to modify, or right-click the line and then select Modify. *The Shelf Configuration dialog box appears.*
5	**If** you want to edit — **Then** go to naming information — step 6 basic communication information — step 7 time information — step 8
6	Select the Naming tab to change name information. See Table 1-3 on page 1-15 for information on the naming information that can be changed from this window and indicates if changing a particular name parameter initiates a shelf restart. Go to step 9. ***Note 1:*** To change the target identifier (TID) properties, see Procedure 1-35 "Changing the target identifier (TID) properties" on page 1-93. ***Note 2:*** To change the optical system identifier (OSID), see Procedure 3-36 "Provisioning the optical system identifier (OSID)" on page 3-117.

—continued—

Procedure 1-2 (continued)
Editing the naming, timing, and basic communications settings

Step	Action

7

CAUTION
Risk of a loss of contact
Before you change the primary shelf address in any of the shelves in a in-service Optical Metro 5100/5200 network, make sure that the OSPF Area ID is set to a value other than 0.0.0.0. Failure to do so results in a loss of IP routing capability between some of the shelves which is turn causes a loss of contact with those shelves.

Select the Communications tab to change basic communication information. Table 1-4 on page 1-15 identifies the communication information that can be changed from this window and indicates if changing a particular parameter initiates a shelf restart.

Go to step 9.

Note 1: To edit the DCN gateway function settings, see Procedure 1-3 "Setting the DCN gateway and editing the DCN gateway function settings".

Note 2: To edit advanced communications settings including the OSPF Area ID, see Procedure 1-29 "Defining or changing advanced communications settings for the network".

Note 3: To edit port control settings, or IP addressing for Ethernet ports, see Procedure 1-25 "Provisioning Ethernet port alarms", Procedure 1-26 "Provisioning Ethernet and serial ports", and Procedure 1-30 "Assigning IP addresses for Ethernet port 2 and Serial port 1".

8 Select the Time tab to change time information. Table 1-5 on page 1-16 indicates if changing the time or date parameter initiates a shelf restart.

9 Click the **OK** button to exit the dialog.

Note 1: If you edit any fields that initiate a shelf restart, System Manager displays a restart message.

Note 2: Depending on the size of the system, System Manager can take several minutes to update the information on the screen.

10

If	Then
a restart dialog appears	you have edited a parameter that initiates a shelf restart. Go to step 11.
otherwise	you have completed this procedure

11 Click the **Yes** button.

The shelf restarts with the new configuration data.

—end—

Table 1-3
Editing name information

Field name	Reboot required?	Result	Result of incorrect value
Network Name	N	The field is changed.	None
Site Name	N	The field is changed.	None
Shelf Name	N	The field is changed. (See Note 1)	None
Shelf Description	N	The field is changed. (See Note 2 and Note 3)	None
Site Identifier	Y	This field groups shelves together in the System Manager display.	Incorrect grouping in the System Manager shelf selector panel.
Shelf Identifier	Y	The field is changed.	The shelf ID will be incorrect in the shelf list. A duplicate value within the ring makes a shelf inaccessible.

Note 1: Do not use brackets in a shelf name.

Note 2: The Shelf Description field cannot contain leading zeros.

Note 3: If you are changing the Shelf Description, and you are managing the network element through Optical Manager Element Adaptor Rel 2.0, refer to the *OMEA User and Installation Guide* to make sure that the network element re-appears on the Optical Network Manager after the change.

Note 4: You may need to do a View/Rediscover Network after the manual edit to see the changes.

Note 5: To change the target identifier (TID) properties, see Procedure 1-35 “Changing the target identifier (TID) properties” on page 1-93.

Note 6: To change the optical system identifier (OSID), see Procedure 3-36 “Provisioning the optical system identifier (OSID)” on page 3-117.

Table 1-4
Editing communication information

Field name	Reboot required?	Result	Result of incorrect value
Shelf Address	Y	This field changes the IP network address of the shelf.	An invalid value can make the shelf unreachable on the network. Visibility of the shelf may be lost.
Primary Shelf Address	Y	This field changes the primary shelf IP address.	The shelf with the incorrect value will not appear in the System Manager. Visibility of the shelf will be lost.
Subnet Mask	Y	This field changes the range of IP addresses associated with the 10Base-T 1X interface.	May cause IP routing within the ring to become non-functional.

Table 1-4 (continued)
Editing communication information

Field name	Reboot required?	Result	Result of incorrect value
DHCP Address	Y	This field changes the IP address that will be assigned to the System Manager connected by way of 10Base-T 1X.	May cause a locally attached System Manager to not operate.
Default Gateway Address	Y	This field changes the IP address of the router to which IP packets are forwarded for routing to the DCN.	May cause IP routing within the ring or to the DCN to become non-functional.
Shelf Type	Y	This field changes the type of shelf.	Would cause provisioning mismatch alarms and loss of traffic.
Ethernet Hubbing Group	Y	This field algorithmically changes the IP address used for 10Base-T 2X communications.	All shelves hubbed together by way of 10Base-T 2X must have the same Ethernet hubbing group value or they cannot communicate.
Note: To edit the DCN gateway function settings in the DCN Gateway Function area of the screen, see Procedure 1-3 “Setting the DCN gateway and editing the DCN gateway function settings”.			

Table 1-5
Editing time information

Field name	Reboot required?	Result	Result of incorrect value
Time Fields	N	Editing on the primary shelf causes all shelves to be synchronized to the new time. Editing on a non-primary will be overwritten after the time server on the Primary establishes communication with the shelf.	Events/alarms will have incorrect time stamps.

Procedure 1-3
Setting the DCN gateway and editing the DCN gateway function settings

Use this procedure to edit the DCN gateway function settings.

See Procedure 1-2 "Editing the naming, timing, and basic communications settings" for information on editing other basic communications settings. See Procedure 1-29 "Defining or changing advanced communications settings for the network" for information on editing advanced communications settings and IP addressing.

When you change shelf configuration data, System Manager may initiate a shelf restart.

Requirements

You must be an Admin level user to edit configuration information on the shelf.

Precautions

CAUTION
Risk of loss of access to one or more shelves
If you provision incorrect information in the Configuration window, you can lose access to one or more shelves and impact intershelf communication.

CAUTION
Risk of incorrect backup file
After you edit shelf configuration data, backup the configuration data of all affected shelves. See Procedure 1-36 "Backing up shelf configuration data" for details.

—continued—

Procedure 1-3 (continued)
Setting the DCN gateway and editing the DCN gateway function settings

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Configuration tab.
3	Select the Communications tab.
4	Double-click on the line that you want to modify, or right-click the line and then select Modify. *The Shelf Configuration dialog box appears.*
5	In the DCN Gateway Function setting area, make sure that the Shelf is DCN Gateway check box is selected.
6	In the DCN Gateway Function setting area, select NONE, Proxy ARP, OSPF, or BGP from the External Routing mode drop-down list. ***Note 1:*** If the shelf is a DCN gateway, and the External Routing mode is set to None, the DCN gateway shelf is used in a system configured with private IP addresses. If the shelf is not selected as a DCN gateway, the External Routing mode is automatically set to None and is greyed out. ***Note 2:*** When Proxy ARP is used, GNE shelves in the network must have the External Routing mode set to Proxy ARP. The Default Gateway Address for the GNE shelf is set to the IP address of the GNE shelf when the System Manager computer is on the same subnet as the GNE shelf. When the System Manager computer is on a different subnet than the GNE shelf, the Default Gateway Address for the GNE shelf is set to the IP address of the IP router residing between the DCN and the GNE shelf. For all other shelves, the Default Gateway Address is set to 0.0.0.0. All non-GNE shelves must be in the same subnet as the GNE shelf. ***Note 3:*** When OSPF is used, GNE shelves in the network must have the External Routing mode set to OSPF and all other shelves must have the External Routing mode set to None. All shelves in the network must have the Default Gateway Address set to 0.0.0.0. The non-GNE shelves can be, but do not have to be, in the same subnet as the GNE shelves. ***Note 4:*** When BGP is used, GNE shelves in the network must have the External Routing mode set to BGP and all other shelves must have the External Routing mode set to None. All shelves in the network must have the Default Gateway Address set to 0.0.0.0. Non-GNE shelves cannot be in the same subnet as the GNE shelves. Each GNE shelf must be in a different subnet.

—continued—

Procedure 1-3 (continued)
Setting the DCN gateway and editing the DCN gateway function settings

Step	Action	
7	**If**	**Then** go to
	the external routing mode is OSPF or BGP	step 8
	otherwise	step 10
8	If you want to change the default values of the selected external routing mode, click the **Set** button. *The OSPF Settings or BGP Settings dialog box appears.*	
9	Change the default values and click the **OK** button.	
10	Click the **OK** button on the Shelf Configuration dialog box. *A Confirm commissioning data modification dialog box appears.*	
11	Click the **Yes** button.	
12	Click the **OK** button to restart the shelf. *The shelf restarts with the new configuration data.*	

—end—

Procedure 1-4
Viewing detailed event history

Use this procedure to view up to 400 events in the Event History display.

The System Manager event buffer records up to 400 events from the shelves in the Optical Metro 5100/5200 network. When the System Manager event buffer has over 400 events, the System Manager overwrites the oldest events with the newer events. If you want to keep an event log you can save it to a file before the System Manager overwrites it. See Procedure 1-6 "Saving event logs" on page 1-22.

For more information about Event History buffers, refer to "Event history review" on page 1-5 in the "System Manager" chapter of *Software and User Interface,* 323-1701-101.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Fault tab.
3	Select the Event History tab.
4	Click on the **Refresh** button. *The Event History window updates with the latest 400 events for the site that you selected.* ***Note:*** To sort information in the Event History, follow Procedure 1-17 "Sorting information".

—end—

Procedure 1-5
Viewing the event console

Use this procedure to view events for all shelves in the network.

ATTENTION
In the case of Windows XP, the System Manager Event Console does not receive events generated by the network element when the Windows XP firewall is enabled. This firewall must be disabled in order to allow autonomous alarms and events to be displayed in the Event Console. Contact your network administrator before disabling the Windows XP firewall.

The System Manager event buffer records up to 400 events from the shelves in the Optical Metro 5100/5200 network. When the System Manager event buffer has over 400 events, the System Manager overwrites the oldest events with the newer events. If you want to keep an event log you can save it to a file before the System Manager overwrites it. See Procedure 1-6 “Saving event logs” on page 1-22.

For more information about Event History buffers, refer to “Event history review” on page 1-5 in the “System Manager” chapter of *Software and User Interface,* 323-1701-101.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, “Logging into the network” on page 1-7.
2	Select the Fault tab.
3	Select the Event Console tab. *The Event Console window displays information for the entire network.* ***Note:*** The System Manager may display an “Overhead Invalid Code” error in the Event Console. This error is monitored for diagnostic purposes and does not affect the performance of your system.

—end—

Procedure 1-6
Saving event logs

Use this procedure to save events from the Event Console or the Event History.

> ***Note:*** You must save the event logs before replacing an SP circuit pack on the shelf. Refer to Procedure 3-13, "Replacing an SP circuit pack" in *Maintenance and Replacement Procedures*, 323-1701-546.

The System Manager event buffer records up to 400 events from the shelves in the Optical Metro 5100/5200 network. When the System Manager event buffer has over 400 events, the System Manager overwrites the oldest events with the newer events. If you want to keep an event log you can save it to a file before the System Manager overwrites it. You can save events in the Event Console window and the Event History window.

For more information about Event History buffers, refer to "Event history review" on page 1-5 in the "System Manager" chapter of *Software and User Interface,* 323-1701-101.

Precautions

CAUTION
Risk of information loss
If your computer has a Windows operating system, do not use any of the following characters in your file names: / : " < | > * ?. In most cases, an error message indicates that the file will not save properly. If you use * or ? in the file name, Windows does not save the file, and fails to provide any error message or warning that information will be lost.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Fault tab.
3	Select the Event Console or the Event History.
4	From the File menu, select Save As. *The Save As dialog box appears.*

—continued—

Procedure 1-6 (continued)
Saving event logs

Step	Action
5	Name the event log file using the .csv extension and select a location for it. ***Note:*** Save your event log with a .csv (comma separated value) extension so that you can open it easily in spreadsheet programs.
6	Click **Save**.

—end—

Procedure 1-7
Printing event lists

Use this procedure to print events lists.

You can print both the Event Console and the Event History.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Fault tab.
3	Select the Event Console or Event History.
4	From the File menu, select Print. *The Print dialog box appears.*
5	Click **OK** in the Print dialog box to confirm printing. *The file prints to your default printer.*

—end—

Procedure 1-8
Clearing the event console

Use this procedure to clear the Event Console.

You can clear the events in the Event Console of a shelf. When you complete this procedure, the System Manager clears all the entries in the Event Console. Entries include events on shelves that you have not selected.

You cannot clear the Event History buffer. For every shelf, the System Manager uses the information in this buffer to provide an event history. You can use the information for troubleshooting.

Precautions

CAUTION
Risk of erasing information for all shelves
Clearing the Event Console erases information for all shelves in the network including shelves that are not selected with the network shelf selector.

Action

Step	Action	
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.	
2	Select the Fault tab.	
3	Select the Event Console tab.	
4	From the Fault menu, select the Clear Event Console option, or click the **Clear** button on the upper right side of the Event Console Display window. *The Confirm Save Log dialog box appears.*	
5	**If**	**Then**
	you want to save a copy of the current log	click **Yes** in the Confirm Save Log dialog box, and go to step 6
	otherwise	click **No** in the Confirm Save Log dialog box, and go to step 8
6	Type the name of the event log file using a .csv extension and select a location. ***Note:*** Save your event log with a .csv (comma separated value) extension so that you can open it easily in spreadsheet programs.	

—continued—

Procedure 1-8 (continued)
Clearing the event console

Step	Action
7	Click **Save**. *The Confirm Clear Log dialog box appears.*
8	Click **Yes** to clear the log.

—end—

Procedure 1-9
Configuring telemetry ports and alarms

Use this procedure to configure telemetry ports and alarms.

The central office telemetry (COTEL) card in the maintenance panel allows you to connect external devices to control and respond to environmental conditions at the equipment site. For example, you can connect a water sensor to the input and a water pump to an output. When the sensor detects water at the equipment site, the System Manager displays an alarm. You can then manually activate the pump, and the alarm clears when the water level returns to normal. The System Manager allows you to indicate the severity of the alarm for every input and alarm text.

After you configure the severity and the text for the telemetry alarms, you can place the alarms in-service or out-of-service. When you place the alarm out-of-service, the alarm remains configured but is disabled. You cannot configure telemetry alarms if they are in-service.

The Optical Metro 5200 has four inputs and four outputs for telemetry equipment. The Optical Metro 5100 has eight inputs and four outputs for telemetry equipment. The configuration for each input and output is the same, with one exception: Output Device 1 allows you to reflect whether the hardware is connected to the port that is normally open or normally closed.

The normally closed option enables you to monitor your system for a power failure. If you connect the hardware to normally closed, the relay is energized and a loss of power triggers an alarm in the central office. The relay controls the alarm equipment in the central office.

The configuration setting on Output Device 1 to normally open or normally closed has no impact on the hardware behavior. It is a reflection of the port to which the external hardware device is connected. Refer to "Central office alarm and telemetry interface" in Chapter 1 of *Technical Specifications*, 323-1701-180 for more details.

The System Manager lists virtual slot 27 as the location of telemetry alarms for the Optical Metro 5100/5200 products.

—continued—

Procedure 1-9 (continued)
Configuring telemetry ports and alarms

Requirements

You must be an Admin level user to configure telemetry alarms on a shelf.

You must connect shelf alarms and telemetry equipment to the central office alarm system before you can configure COTEL alarms. For more information, refer to Procedure 6-1 "Connecting shelf alarms and telemetry equipment to the central office alarm system" in *Installing Optical Metro 5200 Shelves and Components,* 323-1701-201, or Procedure 6-1 "Connecting Optical Metro 5100 shelf alarms and telemetry equipment to the central office alarm system" in *Installing Optical Metro 5100 Shelves and Components,* 323-1701-210.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Equipment tab.
3	Select the Telemetry tab. *The System Manager lists the shelves that have telemetry connections and their state.*

Configuring the input port

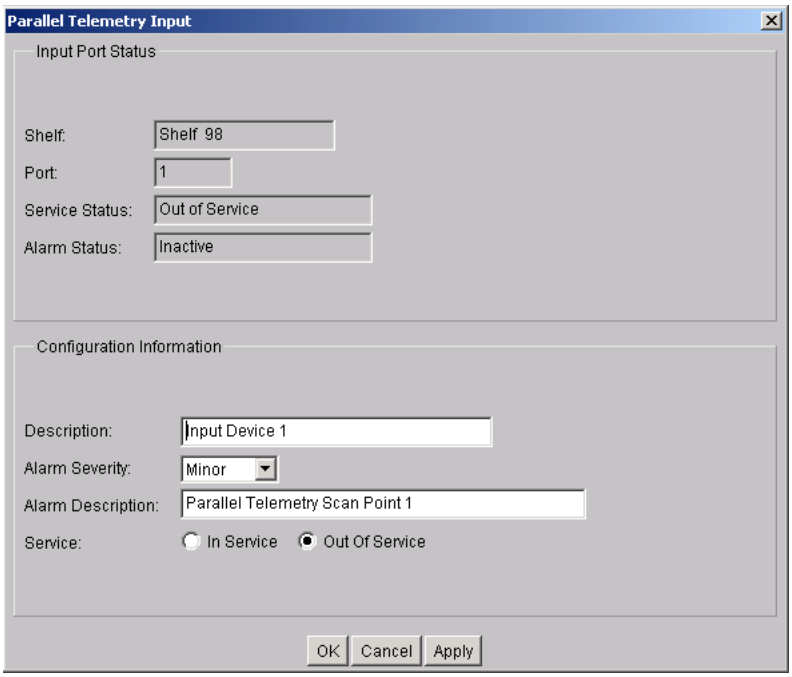
4	Select the shelf for the input (Type field shows "In") that you want to configure. *The information in the Parallel Telemetry window is specific to each shelf.*
5	Select the input device number that you want to configure.
6	Double-click on the input device to view input configuration information. *The Parallel Telemetry Input window appears.*

—continued—

Procedure 1-9 (continued)
Configuring telemetry ports and alarms

Step	Action

OM0237t



7 Enter a description for the telemetry input port.

8 From the Alarm Severity menu, select an option to indicate the severity of the alarm.

9 In the Alarm Description field, enter the text that you want the System Manager to display when it raises an alarm for this input port.

10 Place the input port in-service by clicking on the radio button.

11 Click **OK**.

—continued—

Procedure 1-9 (continued)
Configuring telemetry ports and alarms

Step	Action

Configuring the output port

12 Select the shelf for the output (Type field shows “Out”) that you want to configure.

13 Select the output device number that you want to configure.

14 Double-click on the output device to view output configuration information.

The Parallel Telemetry Output window appears.

15 Enter a description for the output port.

Note: For Output Device 1, you can configure the hardware to be normally open or normally closed. This option is available for Output Device 1 only.

16 Place the output port in-service by clicking on the radio button.

17 Click **Apply**.

18 Click the radio button to place the device in a Released or Operated state.

Note: You must activate or deactivate an output device in response to an alarm by selecting Released or Operated. If the output port is powered on, choosing Operated activates the output port. Choosing Released deactivates the output port.

19 Click **OK**.

—end—

Procedure 1-10
Provisioning alarm severity on a shelf

Use this procedure to provision the severity of an alarm as critical, major, minor or warning using System Manager on a shelf.

> ***Note:*** Alarm severity provisioning changes are applied only to the shelf on which the provisioning changes are completed.

Once the alarm severity is provisioned, alarms are raised with the provisioned alarm severity. Also, the behavior of the shelf lamps (Critical, Major, Minor) and ACO (Alarm Cut Off) are consistent with the provisioned alarm severity.

If there is an active alarm during a provisioning change, the active alarm with the old alarm severity is cleared and the alarm is raised again with the new alarm severity. When the alarm with the old severity clears, alarms that were masked by the old severity, are no longer masked and are raised.

Severity is the only attribute of an alarm that can be edited. All other alarm information, such as the alarm text is not editable. Alarms can not be disabled and the alarm hierarchy is not altered when the alarm severity is changed. As a result, it is possible for a minor alarm to mask a major alarm.

> ***Note:*** The TL1 interface does not support the provisioning of alarm severity. However, it is consistent to the System Manager when reporting alarms.

The System Manager provides the interface to provision the severity of individual alarms as Critical, Major, Minor, or Warning. Some alarms have dual severities; a severity for a service affecting condition and a severity for a non-service affecting condition. This feature allows each of these dual severities to be provisioned.

For each alarm, the System Manager provides an indication as to whether the alarm severity is default or not. To reset the alarm severity to the default value for an individual alarm or for all alarms see, Procedure 1-11, Restoring the severity of an alarm to its default on a shelf.

Requirements

You must be an Admin level user to configure alarm severity on a shelf.

—continued—

Procedure 1-10 (continued)
Provisioning alarm severity on a shelf

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	From the Edit menu, select Provision Alarm Severity. *The Provision Alarm Severity dialog box opens.*
3	Select the shelf that you want to provision alarm severities from the **Shelf** drop-down list. *The alarm list appears.*
4	Double click on the row that contains the alarm that you want to change the severity of. *The Configure Alarm Severity window opens*
5	From the Alarm Severity - (SA or NSA) pull-down menu select the desired alarm severity (Critical, Major, Minor or Warning).
6	Click **OK** in the Configure Alarm Severity window.
7	Click **Yes** to confirm changing the alarm severity. *The Configure Alarm Severity window closes, the severity is changed and a check mark appears in the Severity Changed column of the selected alarm row.*

—end—

Procedure 1-11
Restoring the severity of an alarm to its default on a shelf

Use this procedure to reset the alarm severity of an alarm or all of the alarms back to its default value on a shelf.

Requirements

You must be an Admin level user to configure alarm severity on a shelf.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	From the Edit menu, select Provision Alarm Severity. *The Provision Alarm Severity dialog box opens.*
3	Select the shelf that you want to reset alarm severities from the **Shelf** drop-down list. *The alarm list appears.*
4	**If** you want to reset alarm severity for … **Then** all alarms on a shelf … step 5 one alarm … step 9

Resetting all alarms

5	Click **Reset All to Default**.
6	Click **Yes** to confirm resetting of the alarm severities on the shelf.
7	Click **OK**.
8	You have competed this procedure.

Resetting one alarm

9	Double click on the row that contains the alarm that you want to reset the severity. *The Configure Alarm Severity window opens*
10	Check the Reset Severity To Default box.
11	Click **OK** in the Configure Alarm Severity window.
12	Click **Yes** to confirm changing the alarm severity. *The Configure Alarm Severity window closes, the severity is reset back to the default value and the check mark is removed from the Severity Changed column.*

—end—

Procedure 1-12
Saving the alarm list

Use this procedure to save the alarm list in the Active Alarms window.

Precautions

CAUTION
Risk of information loss
If your computer has a Windows operating system, do not use any of the following characters in your file names: / : " < | > * ?. In most cases, an error message indicates that the file will not save properly. If you use * or ? in the file name, Windows does not save the file, and fails to provide any error message or warning that information will be lost.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Fault tab.
3	Select the Active Alarms tab.
4	From the File menu, select Save as. *The Save As dialog box appears.*
5	Name your file using a .csv extension and select a location for it. ***Note:*** Save your event log with a .csv (comma separated value) extension so that you can open it easily in spreadsheet programs.

—end—

Procedure 1-13
Printing the alarm list

Use this procedure to print the information in alarm and event lists.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Fault tab.
3	Select the Active Alarms tab.
4	From the File menu, select Print. *The Print dialog box appears.*
5	Click **OK** in the Print dialog box to confirm printing. *The file prints to your default printer.*

—end—

Procedure 1-14
Acknowledging visual alarms

Use this procedure to acknowledge visual alarms in the System Manager.

The alarm banner uses red, orange, and yellow to indicate alarms that are not acknowledged. When the alarm indicator is gray, no new alarms exist. The bottom row of the alarm banner displays the alarm counts for the selected shelves. The top row of the alarm banner displays alarm counts for all the shelves in the network. For more information about the alarm banner, refer to "System Manager main window" in Chapter 7 of *Software and User Interface*, 323-1701-101.

Acknowledge alarms when you know the cause of the alarm. When you acknowledge an alarm, the alarm indicator turns gray again. Subsequent alarms change the color of the banner indicating new alarms. When you select a different shelf in the Selected Shelves drop-down list, the alarm banner returns to the unacknowledged state.

> ***Note:*** When you acknowledge an alarm, you are not clearing the alarm. You must remove the cause of an alarm to clear it from the System Manager. Refer to *Trouble Clearing and Alarm Reference Guide*, 323-1701-542, for more information on trouble and alarm clearing.

Table 1-6 lists the color and the related status of alarm indicators. When the alarm banner is blue, the System Manager cannot poll the shelf for alarm status.

—continued—

Procedure 1-14 (continued)
Acknowledging visual alarms

Table 1-6
Alarm indicator colors in the System Manager

Alarm or alert type	Color	Meaning
Critical	red	There are unacknowledged critical alarms.
	gray	There are no unacknowledged critical alarms.
Major	red	There are unacknowledged major alarms.
	gray	There are no unacknowledged major alarms.
Minor	orange	There are unacknowledged minor alarms.
	gray	There are no unacknowledged minor alarms.
Warning	yellow	There are unacknowledged alerts.
	gray	There are no unacknowledged alerts.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, “Logging into the network” on page 1-7.
2	Make sure that you know the active alarms.
3	Click on the highlighted alarm counter in the top right corner of the System Manager window to acknowledge the alarm count. *The alarm is acknowledged and the alarm indicator is no longer highlighted, but the alarm is still present on the system.*

—end—

Procedure 1-15
Selecting shelves

Use this procedure to select shelves.

When you select shelves, only information for the selected shelves appears in the information windows. The information displayed in the windows depends on the shelves you select with the network shelf selector. The bottom row of the alarm banner displays the alarm counts for the selected shelves. The top row of the alarm banner displays alarm counts for all the shelves in the network. For more information about the alarm banner, refer to the "System Manager main window" section of *Software and User Interface*, 323-1701-101.

You can perform tasks on the entire information table, such as sorting, saving, or printing. You can also perform tasks on a single row or cell within the table, such as adding, deleting, or retrieving details. You can also sort the Event Console.

Table 1-7 lists the commands available to select shelves. The list of selected shelves updates when you confirm your selection by clicking **OK**.

Table 1-7
Key controls for selecting shelves

Action	Function
Left-click	Resets the list of selected shelves to the shelf or group under the cursor. Used to select a single shelf or group of shelves.
Ctrl+Left-click	Toggles the selection of the shelf or group of shelves under the cursor location on or off. Used to select multiple shelves in random order before committing the selection.
Shift+Left-click	When you Shift+left-click an item in a list, and then Shift+left-click a second item, you select all items between the first and second items. Used to select multiple shelves in continuous order before committing the selection.
Double-click	When you double-click on a shelf or a group of shelves, the shelf or shelves are selected.

—continued—

Procedure 1-15 (continued)
Selecting shelves

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Click the **Selected Shelves** drop-down list to display the network tree.
3	Select the network, sites, or shelves using the commands in Table 1-7 on page 1-38.
4	Click **Apply** at the bottom left of the System Manager window to display the information about the shelves you selected.
5	Click **Refresh** at the top right of the System Manager window to refresh the connection with the network.

—end—

Procedure 1-16
Sorting shelves

Use this procedure to reorder the shelf list of the primary shelf for that site. You can also use the Group Shelves By Site to group shelves by site.

Action

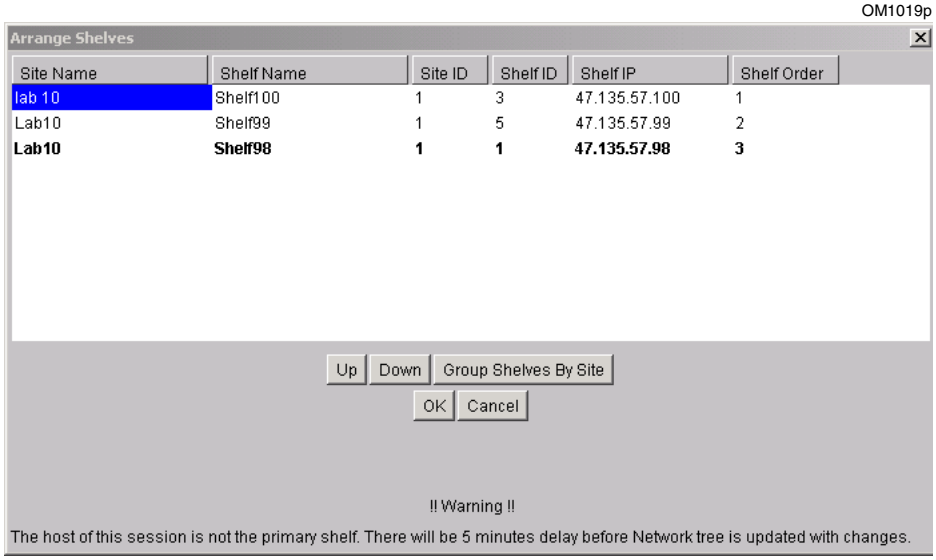
Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	In the System Manager, select the Configuration tab. *The Configuration window appears.*
3	Select the Shelf List tab. *The Shelf List window appears.* ***Note:*** The primary shelf is shown in bold text.
4	Right-click on the primary shelf and select Order Shelves. *The Arrange Shelves window appears.* ***Note 1:*** You cannot sort the information by clicking on the column headers in this window. ***Note 2:*** It is recommended that you do the reordering at the primary shelf so that you can see the changes immediately. If the reordering is not done at the primary shelf, a warning message will be displayed at the bottom of the Arrange Shelves window.

—continued—

Procedure 1-16 (continued)
Sorting shelves

Step	Action

OM1019p



5 If you want to move the selected shelf up, click **Up**.

Note: When you select the top shelf of a ring with multiple sites and press the Up button, all the shelves of the site move up.

6 If you want to move the selected shelf down, click **Down**.

Note: When you select the bottom shelf of a ring with multiple sites and press the Down button, all shelves in the site move down.

7 If you want to regroup all the shelves by site, click **Group Shelves By Site**.

8 Click **OK** to confirm the changes.

Note: Depending on the size of the system, System Manager can take several minutes to update the information on the screen.

—end—

Procedure 1-17
Sorting information

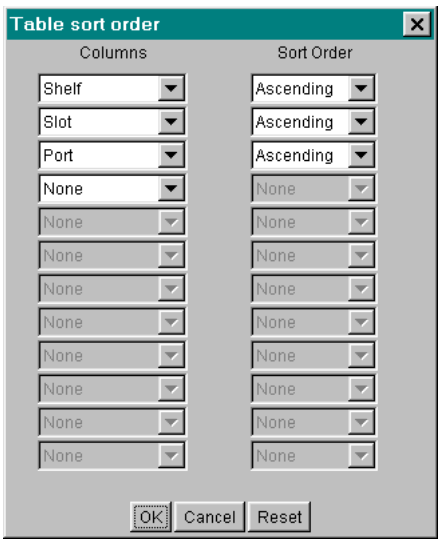
Use this procedure to sort information in the System Manager.

You can sort the data in the information windows in ascending or descending order. The type of information that you can sort depends on the information table.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the tab for the System Manager window that you want to sort.
3	From the View menu, select Sort Order. *The Table sort order dialog box appears.*

OM0375



Note: For easy sorting, click on the column headers on the main windows. When you click on a column header, you can toggle the contents of the column between ascending and descending order.

—continued—

Procedure 1-17 (continued)
Sorting information

Step	Action
4	In the Columns area, select the headers that you want to use to sort the contents of the window.
5	In the Sort Order area, select Ascending, Descending, or None. *The information in the window appears in the sort that you selected.*
6	Click **OK**. ***Note:*** Click **Reset** to reset all columns and sort selections to None.

—end—

Procedure 1-18
Saving information

Use this procedure to save information in any table in the System Manager.

Precautions

CAUTION
Risk of information loss
If your computer uses a Windows operating system, do not use any of the following characters in your file names: / : " < | > * ?. In most cases, an error message indicates that the file will not save properly. If you use * or ? in the file name, Windows does not save the file, and fails to provide any error message or warning that information will be lost.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Navigate to the window that contains the information that you want to save.
3	From the File menu, select Save As. *The Save As dialog box appears.*
4	Select a name and location for the file.
5	Click **Save**. ***Note:*** Save your event log with a .csv (comma separated value) extension so that you can open it easily in spreadsheet programs.

—end—

Procedure 1-19
Printing information

Use this procedure to print information in any table in the System Manager.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Navigate to the window that you want to print information from.
3	From the File menu, select Print. *The Print dialog box appears.* ***Note:*** Make sure that the window information that you are selecting does not exceed the printed paper size. If it does, some of the information may not print properly.
4	Click **OK** in the Print dialog box to confirm printing. *The file prints to your default printer.*

—end—

Procedure 1-20
Modifying, adding, deleting, and viewing details

Use this procedure to

- modify, add, or delete information in an editable field for a selected shelf
- view details or performance monitoring (PM) information for a selected shelf

Requirements

You must be an Admin level user to modify, add, or delete information for a selected shelf.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Click the **Selected Shelves** drop-list to display the network tree.
3	Select a shelf from the network tree.
4	Click the appropriate tab under the **Fault**, **Equipment**, **Connections**, **Configuration, Admin, Performance Monitor** or **Troubleshooting Security** tab.
5	Select a line from the list of displayed shelf items.
6	Right-click a shelf item. *A pop-up menu appears.*
7	Select an item from the pop-up menu: • Details • Modify • Add • Delete • PM Info *Menu items that are not available for the selected shelf item are grayed out in the menu.The menu items will vary depending on tab selection.*
8	Make modifications, additions, or deletions in the editable fields or view the details.
9	Click **OK**.

—end—

Procedure 1-21
Querying the inventory list

Use this procedure to query the inventory list on the Equipment window.

The Inventory window displays information about the physical equipment installed in the shelf.

Query the inventory list when you want information about the state of circuit packs installed in a shelf.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Equipment tab and then select the Inventory tab.
3	From the View menu, select Refresh Current Window, or click the **Refresh** button at the top right corner of the System Manager window. *The Inventory window appears with updated information for the shelves that you selected.*

—end—

Procedure 1-22
Querying facilities

Use this procedure to query the facilities list on the Equipment window.

The Facilities window displays information about the operational status of the circuit packs in the shelf.

Query the facilities list when you want information about the operational status of the circuit packs installed in the shelf.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Equipment tab and then select the Facilities tab.
3	From the View menu, select Refresh Current Window, or click the **Refresh** button at the top right corner of the System Manager window. *The Facilities window appears with updated information for the shelves that you selected.*

—end—

Procedure 1-23
Querying channel assignments

Use this procedure to query channel assignments.

The Channel Assignments window of the System Manager shows channel assignment provisioning and status information.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Connections tab. *The Channel Assignments window appears.*
3	Select the Band, Channel, or None radio button for your scope of view. ***Note:*** Band scope displays all the channel assignments within the ring with the same band as the selected row. Channel scope displays all the channel assignments within the ring with the exact same channel name (case-sensitive) as the selected row. A scope of None displays all the channel assignments for all the shelves that are in focus on the Network tree.
4	Click on the **Refresh** button to refresh the window based on the selected scope of view. ***Note:*** The selected scope takes precedence over network tree selection for Channel Assignment screen refresh.
5	Double-click the line that contains the channel assignment that you want to query. *The Channel Assignments details dialog box appears.* ***Note:*** Double-clicking on an "SRM aggregate" line displays information about the port assignments for an OCI SRM. Double-clicking on an "GFSRM aggregate" line displays information about the port assignments for an OCI SRM GbE/FC. Double-clicking on an MOTR line displays information about the port assignments for a Muxponder.
6	Click **OK** to close the window.

—end—

Procedure 1-24
Changing the date and time on a shelf

Use this procedure to change the date and time for commissioned shelves.

The System Manager platform generates the time stamps for the event console in relation to the "Gained contact with shelf" and the "Lost contact with shelf" events. If you set a time on the System Manager platform that is different from the shelf, the time stamps of these events can appear incorrect relative to other events (for which the time stamp is generated by the shelf). Nortel Networks recommends that you set the System Manager platform and the shelf with the same time.

> ***Note:*** An alternative way to change the date and time on a shelf is to right-click a row in the Shelf List window under the Configuration tab, and then select Network Date/Time.

Requirements

You must be an Admin level user to edit the date and time on a shelf.

Precautions

ATTENTION

You must change the date and time on the primary shelf in the network in order for the change to remain in effect. If you change the date and time on a secondary shelf, the change only lasts until the next time the shelf synchronizes its date and time with the primary shelf.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Configuration tab.
3	Select the Naming or Communications tab.
4	Double-click on the shelf for which you want to change the date and time. *The Shelf Configuration window appears.*
5	Select the Time tab.
6	Change the date and time.
7	Click **OK** to close the window.

—end—

Procedure 1-25
Provisioning Ethernet port alarms

Use this procedure to enable or disable the Ethernet Port 1 alarm and the Ethernet Port 2 alarm.

Note: Both Ethernet port alarms are disabled upon commissioning.

Requirements

You must be an Admin level user to provision Ethernet port alarms.

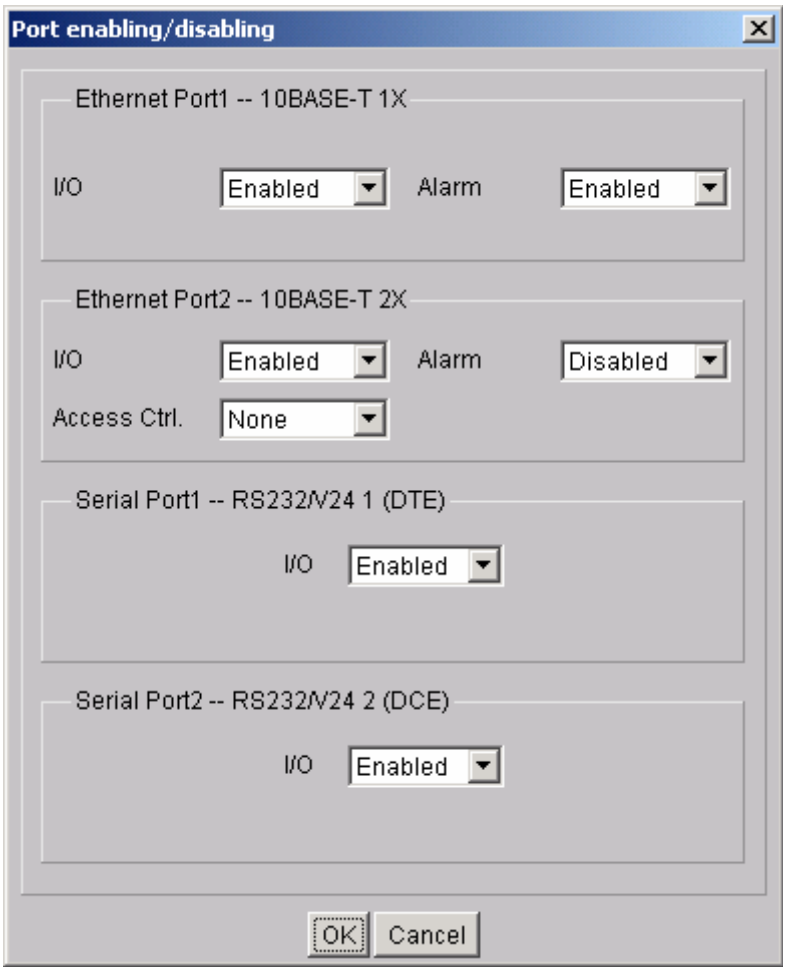
Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Configuration tab.
3	Select the Communications tab.
4	Double-click on the appropriate shelf. *The Shelf Configuration window appears.*
5	Click on the **Port Control** button. *The Port enabling/disabling window appears.*

—continued—

Procedure 1-25 (continued)
Provisioning Ethernet port alarms

Step	Action



6 Select the appropriate alarm setting for each Ethernet port.

7 Click **OK** to confirm the port alarm settings.

8 Click **OK** to close the Shelf Configuration window.

—end—

Procedure 1-26
Provisioning Ethernet and serial ports

Use this procedure to enable or disable Ethernet ports 1 and 2 and serial port 1.

> ***Note:*** Serial port 2 is not supported. Nortel Networks recommends that this port be disabled.

The default values for Ethernet ports 1 and 2 and Serial port 1 are enabled upon commissioning.

If a shelf is decommissioned, Ethernet port 1 defaults to enabled, Ethernet port 2 defaults to disabled and Serial port 1 defaults to enabled.

Requirements

You must be an Admin level user to enable or disable Ethernet ports or Serial ports.

Precautions

CAUTION
Risk of losing visibility
If all the ports on a shelf are disabled, you cannot use the System Manager to access the shelf locally. You must access the shelf from another shelf in the network with the same bands to enable the ports.

CAUTION
Risk of losing visibility of shelves in the Ethernet hub group
If the shelf configuration includes an Ethernet hub, and the 10Base-T 2X port on the host shelf is disabled, you can only monitor other shelves with the same bands as the host shelf. To see all shelves with all bands, you must enable the 10Base-T 2X port on the host shelf.

CAUTION
Risk of losing contact
If all ports on all shelves in a network are disabled, you must contact Nortel Networks Technical support to re-establish a network surveillance connection.

—continued—

Procedure 1-26 (continued)
Provisioning Ethernet and serial ports

CAUTION
Backup configuration changes
Backup the shelf after altering port settings. Otherwise, the shelf could be restored from an out-of-date backup file in the event of shelf failure. See Procedure 1-36 "Backing up shelf configuration data" for details.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Configuration tab.
3	Select the Communications tab.
4	Double-click on the appropriate shelf. *The Shelf Configuration window appears.*
5	Click on the **Port Control** button. *The Port enabling/disabling window appears.*
6	Select the appropriate I/O setting for the port.
7	Click **OK** to confirm the port settings.
8	Click **OK** to close the Shelf Configuration window.

—end—

Procedure 1-27
Provisioning Ethernet port 2 access control

Use this procedure to disable, enable, or change the mode of Ethernet Port 2 access control for all of the shelves in a hubbing group.

> ***Note:*** You must disable and then re-enable the Ethernet port 2 access control feature when you are replacing an SP circuit pack with a previous version of software or when you are reconfiguring hubbing groups. See Procedure 3-13 "Replacing an SP circuit pack" in *Maintenance and Replacement Procedures*, 323-1701-546.

Requirements

You must be an Admin level user to enable or disable Ethernet ports.

Ethernet port 2 must be enabled for every shelf in the hubbing group.

All shelves in the hubbing group must be running Release 6.0 or higher.

All shelves in the same hubbing group must be connected by way of a 10BASE-T hub. You must disable Ethernet port 1 on all remote shelves and enable both Ethernet port 2 and alarm reporting for Ethernet port 2 for every shelf in the hubbing group. Disabling the Ethernet Port 1 ensures that unauthorized users cannot access the data communication network (DCN) through the port. Enabling Ethernet port 2 alarm reporting ensures that any attempt to bypass the access control feature is detected immediately.

The Encrypted Ethernet port 2 access control mode can only be used with a 10Base-T hub. It cannot be used with a 10Base-T switch.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	All shelves in the hubbing group must be running Release 6.0 or higher. If a shelf is not running Release 6.0, upgrade the Optical Metro 5100/5200 software on this shelf before going to step 3.
3	Select the Configuration tab.
4	Select the Communications tab.

—continued—

Procedure 1-27 (continued)
Provisioning Ethernet port 2 access control

Step	Action
5	Click on the **Refresh** button at the top right corner of the System Manager window and confirm that all shelves are in contact. ***Note:*** If there is a loss of contact between the shelves in the hubbing group, correct the problem before going to step 6.
6	Double-click on one shelf in the hubbing group. *The Shelf Configuration window appears with the Communications tab selected.*
7	Click on the **Port Control** button. *The Port enabling/disabling window appears.*

ATTENTION
When you change the Ethernet port 2 access control values on one shelf, the values for all shelves within the same Ethernet hubbing group change (as long as Ethernet connectivity exists).

8	Under the Ethernet Port 2 -- 10Base-T 2X section, in the Access Ctrl. field, select one of the following: **a.** To disable access control for all shelves in the hubbing group, select None, and then close the warning message window. **b.** To filter incoming packets on all shelves in the hubbing group, select Filter. **c.** To reject unencrypted incoming packets and encrypt outgoing packets on all shelves in the hubbing group, select Encrypt.
9	Click **OK** in the Port enabling/disabling window.
10	Click **OK** in the Shelf Configuration window. *An information window appears confirming the changes.*
11	Click **Close** on the information window.
12	Wait 2 minutes for the changed data to propagate to the other shelves in the hubbing group.
13	In the Communications tab, verify the new Enet2 Access Control state for each shelf in the hubbing group.
14	Select the Fault tab and then the Event Console tab, and verify the events for all shelves in the hubbing group.

—continued—

Procedure 1-27 (continued)
Provisioning Ethernet port 2 access control

Step	Action	
15	**If**	**Then**
	the Description field of the Event Console window displays PASS for the Ethernet port 2 access control change event	you have completed this procedure
	otherwise	go to step 16
16	Perform step 3 through step 14 to set the state of the Ethernet port 2 access control feature back to the state that was in place before the error occurred and call your next level of support.	

—end—

Procedure 1-28
Provisioning IP forwarding on Ethernet port 1

Use this procedure to disable or enable IP forwarding on Ethernet Port 1 on a GNE shelf configured in private IP address mode.

When IP forwarding is disabled on Ethernet Port 1 of the GNE shelf, any IP access to the customer's DCN that is initiated from any remote shelf through Ethernet Port 1 of the GNE shelf, is blocked (that is, the intercepted IP packets are dropped). Only the GNE shelf can exchange IP packets with computers on the customer's DCN.

Requirements

You must be an Admin level user to disable or enable IP forwarding on Ethernet Port 1.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Configuration tab.
3	Select the Communications tab.
4	Double-click on the GNE shelf. *The Shelf Configuration window appears with the Communications tab selected.*
5	Click on the **Port Control** button. *The Port enabling/disabling window appears.*
6	Under the Ethernet Port 1 -- 10Base-T 1X section, in the IP Forwarding drop-down list, select one of the following: **a.** to block IP access to the customer's DCN from any remote shelf through Ethernet Port 1 of the GNE shelf, select Disabled. **b.** to allow IP access to the customer's DCN from any remote shelf through Ethernet Port 1 of the GNE shelf, select Enabled.
7	Click **OK** in the Port enabling/disabling window.
8	Click **OK** in the Shelf Configuration window.

—end—

Procedure 1-29
Defining or changing advanced communications settings for the network

Use this procedure to change advanced communications settings for the network. Advanced communications settings include internal Open Shortest Path First (OSPF) setting, Network Address Translation (NAT) setting, assignable IP setting, and shelf Domain Name Server (DNS) setting.

This procedure includes steps for setting the internal OSPF Area ID and NAT. If you want to assign IP addresses for Ethernet port 2 and Serial port 1, see Procedure 1-30, "Assigning IP addresses for Ethernet port 2 and Serial port 1". If you want to set the DNS settings, see Procedure 1-31 "Enabling or disabling the DNS proxy service", and Procedure 1-32 "Setting up the DNS proxy service".

For more information about advanced communications settings, refer to the "Data communications in the Optical Metro 5100/5200 network" chapter of *Network Planning and Link Engineering,* 323-1701-110.

Requirements

You must be an Admin level user to edit configuration information on a shelf.

Make sure that you understand all of the restrictions that govern IP addressing in the Optical Metro 5100/5200. For information about restrictions on user-assignable IP addresses, see the "IP address restrictions" section in the "Data communications in the Optical Metro 5100/5200 network" chapter of *Network Planning and Link Engineering*, 323-1701-110.

Precautions

CAUTION
Risk of losing visibility
If you provision incorrect information in the Configuration window, you can lose access to one or more shelves and impact intershelf communication.

CAUTION
Risk of incorrect backup file
After you change the shelf configuration, backup the configuration data of all affected shelves. See Procedure 1-36, "Backing up shelf configuration data" on page 1-95 for more information.

—continued—

Procedure 1-29 (continued)
Defining or changing advanced communications settings for the network

ATTENTION
You must be connected locally to the shelf when you change the internal OSPF Area ID value since visibility will be lost to shelves until all the shelves have the new OSPF area ID. This always applies unless you are changing the value from 0.0.0.0 to the current IP address of the primary shelf. See Procedure 1-8, "Connecting locally to a commissioned shelf using Ethernet port 1 or port 2 and configuring DHCP (Windows 2000/NT/XP)" and Procedure 1-9, "Connecting locally to a commissioned GNE shelf using Ethernet port 1 and configuring a static IP address (Windows 2000/NT/XP)" in *Commissioning Procedures,* 323-1701-220 for procedures on how to connect locally to a shelf.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Configuration tab.
3	Select the Communications tab.
4	Double-click on the appropriate shelf or right-click on the line and then select Modify. *The Shelf Configuration dialog box appears.*
5	Click the **Advanced...** button. *The Advanced Communications Settings dialog box appears.*
6	**If** / **Then** go to you want to edit the OSPF Area ID — step 7 you want to edit the NAT setting — step 8

—continued—

Procedure 1-29 (continued)
Defining or changing advanced communications settings for the network

Step	Action
7	Enter a new OSPF Area ID in the Internal OSPF Setting section of the dialog box, then go to step 10. ***Note 1:*** All shelves in a network must have the same value for the OSPF Area ID. If the OSPF Area ID is left as the value of 0.0.0.0, the shelves use the primary shelf address as their OSPF Area ID. This applies whether the external routing protocol is OSPF, BGP, or Proxy ARP. ***Note 2:*** If you wish to assign a non-default OSPF area ID (not the primary shelf address), you can use whatever area you want as long as each shelf has the same area. Additionally, if the external routing protocol is OSPF, you must make sure that the area assigned is unique in your DCN. ***Note 3:*** You must be connected locally to the shelf when you change the internal OSPF Area ID value since visibility will be lost to shelves until all the shelves have the new OSPF area ID. This always applies unless you are changing the value from 0.0.0.0 to the current IP address of the primary shelf.
8	In the Advanced Communications Settings dialog box, select or deselect the Inbound NAT Enabled option to enable or disable the Inbound NAT feature. ***Note:*** All external Manager sessions using Optical Metro 5100/5200 internal IP addresses must be de-registered before Inbound NAT is disabled.
9	If necessary, type a new value in the Inbound NAT Alias field to replace the default alias, then go to step 10. ***Note 1:*** All external Manager sessions using Optical Metro 5100/5200 internal IP addresses must be de-registered before the Inbound NAT alias is changed. ***Note 2:*** All System Manager sessions using Optical Metro 5100/5200 internal IP addresses must be restarted after an alias change.
10	Click the **OK** button on the Advanced Communications Settings dialog box.
11	Click the **OK** button on the Shelf Configuration dialog box. ***Note:*** Depending on the size of the system, System Manager can take several minutes to update the information on the screen. *A Confirm commissioning data modification dialog box can appear.*

12	**If**	**Then**
	a Confirm commissioning data modification dialog box appears in step 11	go to step 13. A shelf restart is required to complete this procedure.
	otherwise	you have completed this procedure

13	Click the **Yes** button. *The shelf restarts with the new configuration data.*

—end—

Procedure 1-30
Assigning IP addresses for Ethernet port 2 and Serial port 1

Use this procedure to assign IP addresses for Ethernet port 2 and Serial port 1.

Note: Serial port 2 is not supported.

If you are using a multiple IP address shelf configuration, you can manually assign the IP addresses for Ethernet port 2 and Serial port 1. If you do not assign an IP address, the system assigns the default address shown in Table 1-8 on page 1-64.

The 10.0.x.x (where x=0 to 255) IP addresses are for internal use in an Optical Metro 5100/5200 network. You cannot assign these reserved IP addresses in the network.

If you assign addresses outside the 10.0.x.x through 10.4.x.x range to Ethernet port 2 or Serial port 1, and OSPF backbone routing is configured on the gateway network element (GNE) shelves, these addresses can be advertised into the OSPF backbone area.

Requirements

You must be an Admin level user to edit configuration information on a shelf.

You must assign unique IP addresses to avoid conflicts in the network.

Make sure that you understand all of the restrictions that govern IP addressing in the Optical Metro 5100/5200. For information about restrictions on user-assignable IP addresses, see the "IP address restrictions" section in the "Data communications in the Optical Metro 5100/5200 network" chapter of *Network Planning and Link Engineering*, 323-1701-110.

Precautions

CAUTION
Risk of losing visibility
If you provision incorrect information in the Configuration window, you can lose access to one or more shelves and impact intershelf communication.

—continued—

Procedure 1-30 (continued)
Assigning IP addresses for Ethernet port 2 and Serial port 1

CAUTION
Risk of incorrect backup file
After you change the shelf configuration, backup the configuration data of all affected shelves. See Procedure 1-36 "Backing up shelf configuration data" on page 1-95 for more information.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Configuration tab.
3	Select the Communications tab.
4	Double-click on the appropriate shelf or right-click on the line and then select Modify. *The Shelf Configuration dialog box appears.*
5	Click the **Advanced...** button. *The Advanced Communications Settings dialog box appears.*
6	Click the **Set Port IPs...** button. *The Assignable IP Settings dialog box appears.*
7	Assign the IP addresses and click the **OK** button. See Table 1-8 for the assignable IP settings values.
8	Click the **OK** button on the Advanced Communications Settings dialog box.

—continued—

Procedure 1-30 (continued)
Assigning IP addresses for Ethernet port 2 and Serial port 1

Step	Action
9	Click the **OK** button on the Shelf Configuration dialog box. ***Note:*** Depending on the size of the system, System Manager can take several minutes to update the information on the screen. *A Confirm commissioning data modification dialog box can appear.*

10	**If**	**Then**
	a Confirm commissioning data modification dialog box appears in step 9.	go to step 11. A shelf restart is required to complete this procedure.
	otherwise	you have completed this procedure

11	Click the **Yes** button. *The shelf restarts with the new configuration data.*

—end—

Table 1-8
Assignable IP Settings dialog box

Field name	Definition	Value/range
Enet Port 2 IP	IP address for 10BaseT 2X	IP address. The default value is 10.2.hubbinggroup.shelfID.
Enet Port 2 Mask	Subnet mask for 10BaseT 2X	IP address. The default value is 255.255.255.0.
Enet Port 2 DHCP	DHCP address for 10BaseT 2X	IP address. The default value is 10.2.hubbinggroup.(shelfID + 128).
Serial Port1 Local IP	DTE local	IP address. The default value is 10.3.shelfID.1.
Serial Port1 Remote IP	DTE remote	IP address. The default value is 10.3.shelfID.2.
Serial Port 2 Local IP (see Note)	DCE local	IP address. The default value is 10.4.shelfID.1.
Serial Port 2 Remote IP (see Note)	DCE remote	IP address. The default value is 10.4.shelfID.2.
Note: Serial port 2 is not supported.		

Procedure 1-31
Enabling or disabling the DNS proxy service

Use this procedure to enable or disable the Domain Name Server (DNS) proxy service. When enabled, the DNS proxy service allows access to an Optical Metro 5100/5200 shelf from a directly connected PC, by name rather than IP address. For further information on the DNS proxy service, see the chapter "Data communications in the Optical Metro 5100/5200 network" in *Network Planning and Link Engineering*, 323-1701-110.

Requirements

You must be an Admin level user to enable or disable DNS proxy service on a shelf.

A domain name and IP address must be entered for every network element into the DNS server database. To set up the DNS proxy service, see Procedure 1-32, "Setting up the DNS proxy service".

Action

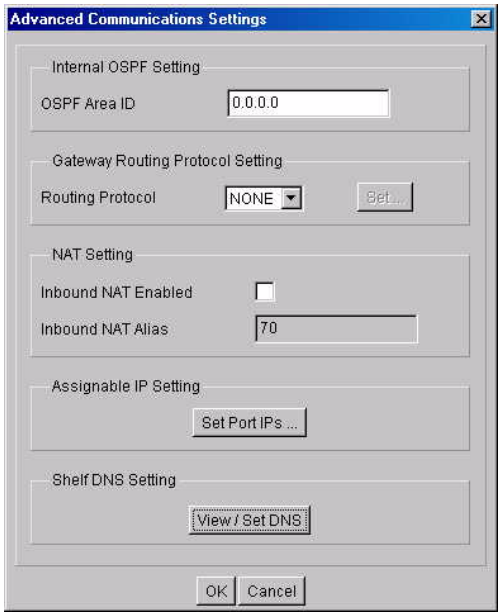
Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Configuration tab.
3	Select the Communications tab.
4	Double-click on the primary shelf or right-click on the line and select Modify. *The Shelf Configuration window appears.*
5	Click the **Advanced...** button in the Communication tab. *The Advanced Communications Settings dialog box appears.*

—continued—

Procedure 1-31 (continued)
Enabling or disabling the DNS proxy service

Step	Action

OM0737t



6 Click the **View/Set DNS** button.

The DNS Settings dialog box appears.

7 Select **Enable** or **Disable** button.

Note 1: The Enable option is rejected unless at least one DNS server has been set to a valid IP address. For information on setting a DNS server to an IP address, see Procedure 1-32 “Setting up the DNS proxy service”.

Note 2: Parameters (or configuration information) can only be modified on the primary shelf. All parameters are distributed from the primary shelf to all other shelves in the shelf list.

8

If	Then
you select **Disable**	the Confirm DNS Disable dialog box appears. Go to step 9.
otherwise	go to step 10

9 Click **Yes** in the Confirm DNS Disable dialog box to confirm the operation. Go to step 11.

10 Click the **Apply** button.

11 Click the **Cancel** button to close the DNS Settings window.

12 Click the **OK** button to close the Advanced Communications Settings window.

13 Click the **OK** button to close the Shelf Configuration window.

—end—

Procedure 1-32
Setting up the DNS proxy service

Use this procedure to set an IP address for one or two (for redundancy) Domain Name Servers (DNS) to which DNS queries are forwarded, and set the DNS suffix. The PC which originates the DNS query attaches the suffix to make a fully qualified domain name (FQDN). If the user enters a FQDN, the PC does not attach the suffix.

Modifications of the DNS suffix will only be activated after a restart of the shelf with the DNS proxy service enabled. For further information on the DNS proxy service, see the chapter "Data communications in the Optical Metro 5100/5200 network" in *Network Planning and Link Engineering*, 323-1701-110.

Requirements

You must be an Admin level user to configure a DNS proxy service on a shelf.

To use the DNS proxy service, the service must be enabled. For information on enabling the DNS service, see Procedure 1-31, "Enabling or disabling the DNS proxy service".

Make sure that you understand all of the restrictions that govern IP addressing in the Optical Metro 5100/5200. For information about restrictions on user-assignable IP addresses, see the "IP address restrictions" section in the "Data communications in the Optical Metro 5100/5200 network" chapter of *Network Planning and Link Engineering*, 323-1701-110.

Action

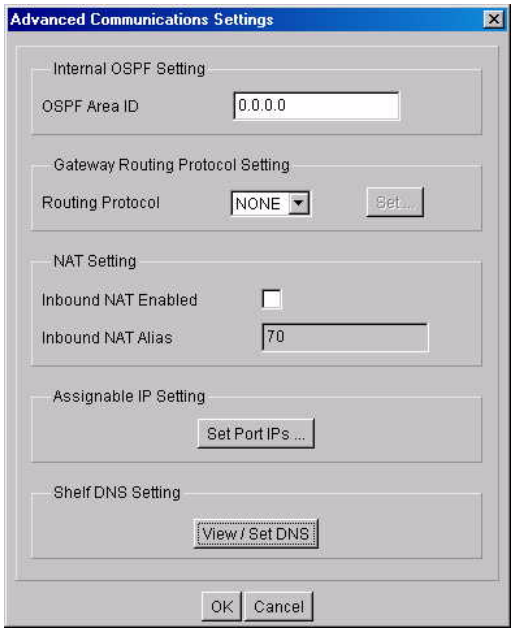
Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Configuration tab.
3	Select the Communications tab.
4	Double-click on the primary shelf or right-click on the line and select Modify. *The Shelf Configuration window appears.*
5	Click the **Advanced...** button in the Communications tab. *The Advanced Communications Settings dialog box appears.*

—continued—

Procedure 1-32 (continued)
Setting up the DNS proxy service

Step	Action

OM0737t



6 Click the **View/Set DNS** button.

The DNS Settings dialog box appears.

7 Set the IP address for the first DNS server by entering a valid IP address into the first line of the DNS Servers section.

Note 1: The IP address for a DNS server cannot be modified if the DNS proxy service is enabled. For information on disabling the DNS proxy service, see Procedure 1-31 “Enabling or disabling the DNS proxy service”.

Note 2: Parameters (or configuration information) can only be modified on the primary shelf. All parameters are distributed from the primary shelf to all other shelves in the shelf list.

8 If necessary, set the address for the second DNS server by entering a valid IP address into the second line of the DNS Servers section.

9 Set the suffix by entering a valid character string into the DNS Suffix section.

Note 1: The DNS suffix can be any combination of letters and numbers, up to 128 characters. The maximum length of a “label” (string of characters between two periods) is 63 characters.

Note 2: The characters used must be supported by the DNS server(s).

Note 3: The DNS suffix cannot be set or modified if the DNS proxy service is enabled. For information on disabling the DNS proxy service, see Procedure 1-31 “Enabling or disabling the DNS proxy service”.

—continued—

Procedure 1-32 (continued)
Setting up the DNS proxy service

Step	Action
	Note 4: Parameters (or configuration information) can only be modified on the primary shelf. All parameters are distributed from the primary shelf to all other shelves in the shelf list.
10	Click the **Apply** button. *The DNS Suffix Change Warning dialog box appears.* ***Note:*** Modifications of the DNS suffix will only be activated after a restart of the shelf with the DNS proxy service enabled. For information on enabling the DNS proxy service, see Procedure 1-31 "Enabling or disabling the DNS proxy service". For information on restarting the shelf, see Procedure 4-3 "Restarting a shelf".
11	Click **Yes** in the DNS Suffix Change Warning dialog box to confirm the restart.
12	Click the **Cancel** button to close the DNS Settings window.
13	Click the **OK** button to close the Advanced Communications Settings window.
14	Click the **OK** button to close the Shelf Configuration window.

—end—

Procedure 1-33
Converting from private IP addressing to public IP addressing

Use this procedure to convert from private IP addressing to public IP addressing.

Requirements

The following requirements apply:

- You must be logged into the System Manager as an Admin level user to change configuration information for a shelf.
- The System Manager must have contact with the shelves.
- Data-fill Table 1-9 on page 1-72 as follows:
  - — Record the shelf name of your primary shelf into the Shelf name field. Use an up-to-date map of your network to locate your primary shelf. You can also find this information in the System Manager by selecting the network name in the Selected Shelves area and then accessing the Configuration/Naming tab. The primary shelf is identified with the letter P in the Role field.
  - — Record the shelf name of all the other shelves in your network into the Shelf name field. You can find this information in the System Manager by selecting the network name in the Selected Shelves area and then accessing the Configuration/Naming tab.
  - — Enter a check for each shelf that is a DCN Gateway shelf. You can find this information in the System Manager by selecting the network name in the Selected Shelves area and then accessing the Configuration/Naming tab. A DCN Gateway shelf is identified with the letter G in the Role field.
  - — For each DCN Gateway shelf, record the external routing mode (either Proxy ARP, OSPF or BGP) in the External Routing Mode field and the default gateway address in the Default Gateway Address field. For more information about IP addressing, refer to the "Data communications in the Optical Metro 5100/5200 network" chapter of *Network Planning and Link Engineering,* 323-1701-110.
  - — Record the IP address, DHCP address and Subnet mask for each shelf according to the new IP addressing plan. For more information about IP addressing, refer to the "Data communications in the Optical Metro 5100/5200 network" chapter of *Network Planning and Link Engineering,* 323-1701-110.

—continued—

Procedure 1-33 (continued)
Converting from private IP addressing to public IP addressing

- Before starting this procedure, ensure that the Internal OSPF Setting – OSPF Area ID in the Advanced Communications Settings panel is set to a value other than 0.0.0.0. Failure to do so will result in loss of IP routing capability between some of the shelves, which in turn may produce loss of contact with some shelves. In the event that the internal OSPF Area ID is set to 0.0.0.0, it is recommended to change it in every shelf to the current primary shelf address. See Procedure 1-29 "Defining or changing advanced communications settings for the network" on page 1-59.

Precautions

CAUTION
Risk of incorrect backup file
After you complete this procedure, back up the configuration data of all affected shelves. See Procedure 1-36, "Backing up shelf configuration data" on page 1-95 for more information.

CAUTION
Risk of loss of contact - Optical Network Manager /OMEA
If you change the NE configuration (for example, change the NE TID or NE IP address) (relevant for all configurations—private or public IP configurations) for Optical Metro 5100/5200 network elements, do not make the change and then attempt to rediscover the NE. The correct procedure is as follows: first delete the NE from OMEA and then make the change, and finally manage the NE again.

See *Optical Manager Element Adapter, Standard Operations Guide,* 450-3121-301, for procedures on deleting a network element and managing a network element.

CAUTION
Risk of loss of contact - SNMP
If the network is being managed by an SNMP manager there will be loss of contact with some or all of the shelves after you complete this procedure. To regain contact with the shelves, see "SNMP proxy service" in *Network Planning and Link Engineering,* 323-1701-110.

—continued—

Procedure 1-33 (continued)
Converting from private IP addressing to public IP addressing

Table 1-9
Procedure data

Shelf #	Shelf name	IP address	DHCP address	Subnet Mask	DCN Gateway	External Routing Mode	Default Gateway Address
Primary							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							

Table 1-9 (continued)
Procedure data

Shelf #	Shelf name	IP address	DHCP address	Subnet Mask	DCN Gateway	External Routing Mode	Default Gateway Address
26							
27							
28							
29							
30							
31							
32							
33							
34							
35							
36							
37							
38							
39							
40							
41							
42							
43							
44							
45							
46							
47							
48							
49							
50							
51							
52							

Table 1-9 (continued)
Procedure data

Shelf #	Shelf name	IP address	DHCP address	Subnet Mask	DCN Gateway	External Routing Mode	Default Gateway Address
53							
54							
55							
56							
57							
58							
59							
60							
61							
62							
63							
64							

Action

Step	Action	
1	**If**	**Then** go to
	the primary shelf is a DCN Gateway and you have one or more DCN Gateway shelves	step 2
	the primary shelf is not a DCN Gateway and you have a single DCN Gateway shelf	step 21
	the primary shelf is not a DCN Gateway and you have multiple DCN Gateway shelves	step 23
2	Log into a DCN Gateway shelf. See Procedure 1-1, "Logging into the network" on page 1-7. ***Note:*** Procedure 1-1 asks that you log into the primary shelf, instead, log into a DCN Gateway shelf although the DCN Gateway shelf and the primary shelf may be the same shelf.	
3	In the Selected Shelves area: • click on a remote shelf (a shelf which is not a DCN Gateway shelf) • click on the **Apply** button	

—continued—

Procedure 1-33 (continued)
Converting from private IP addressing to public IP addressing

Step	Action
4	In the Optical Metro System Manager window: • click on the Configuration tab • click on the Communications tab *The Communications list appears.*
5	In the Communications list, double-click on the shelf. *The Shelf Configuration window appears.*
6	In the Shelf Configuration window, set the parameters as follows: • Shelf is DCN Gateway box is cleared (External Routing Mode is automatically set to None) • Shelf address is set according to Table 1-9 on page 1-72. • Primary Shelf Address is set to the IP address of the primary shelf • Subnet Mask is set according to Table 1-9 on page 1-72. • DHCP Address is set according to Table 1-9 on page 1-72. • Default Gateway Address is set to 0.0.0.0
7	In the Shelf Configuration dialog, click on the **OK** button. *The Confirm commissioning data modification dialog box appears.*
8	In the Confirm commissioning data modification dialog, click on the **Yes** button. *The shelf restarts.*
9	Wait 5 minutes for the shelf to complete the restart and become visible within the System Manager session.
10	**If** / **Then** there are other DCN shelves / repeat step 2 to step 9 there are no other DCN shelves but there are remote shelves / go to step 11
11	In the Selected Shelves area: • click on the DCN Gateway shelf you logged into • click on the **Apply** button
12	In the Optical Metro System Manager window: • click on the Configuration tab • click on the Communications tab *The Communications list appears.*
13	In the Communications list, double-click on the shelf. *The Shelf Configuration window appears.*

—continued—

Procedure 1-33 (continued)
Converting from private IP addressing to public IP addressing

Step	Action
14	In the Shelf Configuration window, set the parameters as follows: • Shelf is DCN Gateway box is checked • External Routing Mode is set according to Table 1-9 on page 1-72 • Shelf address is set according to Table 1-9 on page 1-72 • Primary Shelf Address is set to the IP address of the primary shelf • Subnet Mask is set according to Table 1-9 on page 1-72 • DHCP Address is set to 0.0.0.0 • Default Gateway Address is set according to Table 1-9 on page 1-72
15	In the Shelf Configuration dialog, click on the **OK** button. *The Confirm commissioning data modification dialog box appears.*
16	In the Confirm commissioning data modification dialog, click on the **Yes** button. *The System Manager closes and the shelf restarts.*
17	Wait 5 minutes for the shelf to complete the restart.
18	**If** / **Then** go to there are other DCN Gateway shelves — step 19 otherwise — step 58
19	**If** / **Then** there are other remote shelves — repeat step 2 to step 9 there are no other remote shelves — go to step 20 ***Note:*** Procedure 1-1 asks that you log into the primary shelf, instead, log into a DCN Gateway shelf although the DCN Gateway shelf and the primary shelf may be the same shelf.
20	Repeat step 11 to step 18.
21	Log into the DCN Gateway shelf. See Procedure 1-1, "Logging into the network" on page 1-7. ***Note:*** Procedure 1-1 asks that you log into the primary shelf, instead log into the DCN Gateway shelf.
22	Go to step 24.
23	Log into the DCN Gateway shelf. See Procedure 1-1, "Logging into the network" on page 1-7. ***Note:*** Procedure 1-1 asks that you log into the primary shelf, instead log into the DCN Gateway shelf.

—continued—

Procedure 1-33 (continued)
Converting from private IP addressing to public IP addressing

Step	Action
24	In the Selected Shelves area: • click on the primary shelf • click on the **Apply** button
25	In the Optical Metro System Manager window: • click on the Configuration tab • click on the Communications tab *The Communications list appears.*
26	In the Communications list, double-click on the shelf. *The Shelf Configuration window appears.*
27	In the Shelf Configuration window, set the parameters as follows: • Shelf is DCN Gateway box is cleared (External Routing Mode is automatically set to None) • Shelf address is set according to Table 1-9 on page 1-72 • Primary Shelf Address is set according to Table 1-9 on page 1-72 ***Note:*** The Primary Shelf Address and the Shelf Address should match since the shelf you are modifying is the primary shelf. • Subnet Mask is set according to Table 1-9 on page 1-72 • DHCP Address is set according to Table 1-9 on page 1-72 • Default Gateway Address is set to 0.0.0.0
28	In the Shelf Configuration dialog, click on the **OK** button. *A Warning dialog box appears.*
29	In the Warning dialog, click on the **Yes** button. *The Confirm commissioning data modification dialog box appears.*
30	In the Confirm commissioning data modification dialog, click on the **Yes** button. *The shelf restarts.*
31	Wait 5 minutes for the shelf to complete the restart, and for the modified primary data to get propagated around the network and for the shelf to become visible within the System Manager session.
32	**If** / **Then** go to there are other remote shelves (a shelf which is not a DCN Gateway shelf or the primary shelf) — step 33 otherwise — step 41

—continued—

Procedure 1-33 (continued)
Converting from private IP addressing to public IP addressing

Step	Action
33	In the Selected Shelves area: • click on a remote shelf (a shelf which is not the DCN Gateway shelf or the primary shelf) • click on the **Apply** button
34	In the Optical Metro System Manager window: • click on the Configuration tab • click on the Communications tab *The Communications list appears.*
35	In the Communications list, double-click on the shelf. *The Shelf Configuration window appears.*
36	In the Shelf Configuration window, set the parameters as follows: • Shelf is DCN Gateway box is cleared (External Routing Mode is automatically set to None) • Shelf address is set according to Table 1-9 on page 1-72 • Primary Shelf Address is set to the IP address of the primary shelf ***Note:*** This address is the same as the address you used as the “Primary Shelf Address” and “Shelf Address” in step 27. • Subnet Mask is set according to Table 1-9 on page 1-72 • DHCP Address is set according to Table 1-9 on page 1-72 • Default Gateway Address is set to 0.0.0.0
37	In the Shelf Configuration dialog, click on the **OK** button. *The Confirm commissioning data modification dialog box appears.*
38	In the Confirm commissioning data modification dialog, click on the **Yes** button. *The shelf restarts.*
39	Wait 5 minutes for the shelf to complete the restart and become visible within the System Manager session.
40	**If** — **Then** go to there are other remote shelves (i.e. a shelf which is not a DCN gateway shelf or the primary shelf) — step 41 otherwise — step 49

—continued—

Procedure 1-33 (continued)
Converting from private IP addressing to public IP addressing

Step	Action
41	In the Selected Shelves area: • click on the DCN Gateway shelf • click on the **Apply** button
42	In the Optical Metro System Manager window: • click on the Configuration tab • click on the Communications tab *The Communications list appears.*
43	In the Communications list, double-click on the shelf. *The Shelf Configuration window appears.*
44	In the Shelf Configuration window, set the parameters as follows: • Shelf is DCN Gateway box is checked • External Routing Mode is set according to Table 1-9 on page 1-72 • Shelf address is set according to Table 1-9 on page 1-72 • Primary Shelf Address is set to the IP address of the primary shelf ***Note:*** This address is the same as the address you used as the "Primary Shelf Address" and "Shelf Address" in step 27. • Subnet Mask is set according to Table 1-9 on page 1-72 • DHCP Address is set to 0.0.0.0 • Default Gateway Address is set according to Table 1-9 on page 1-72
45	In the Shelf Configuration dialog, click on the **OK** button. *The Confirm commissioning data modification dialog box appears.*
46	In the Confirm commissioning data modification dialog, click on the **Yes** button. *The System Manager closes and the shelf restarts.*
47	Wait 5 minutes for the shelf to complete the restart.
48	**If** / **Then** there are other remote shelves / repeat step 41 to step 47 there are no other remote shelves / go to step 49
49	Log into another DCN Gateway shelf. See Procedure 1-1, "Logging into the network" on page 1-7. ***Note:*** Procedure 1-1 asks that you log into the primary shelf, instead log into the DCN Gateway shelf.

—continued—

Procedure 1-33 (continued)
Converting from private IP addressing to public IP addressing

Step	Action
50	In the Selected Shelves area: • click on the DCN Gateway shelf you logged into • click on the **Apply** button
51	In the Optical Metro System Manager window: • click on the Configuration tab • click on the Communications tab *The Communications list appears.*
52	In the Communications list, double-click on the shelf. *The Shelf Configuration window appears.*
53	In the Shelf Configuration window, set the parameters as follows: • Shelf is DCN Gateway box is checked • External Routing Mode is set according to Table 1-9 on page 1-72 • Shelf address is set according to Table 1-9 on page 1-72 • Primary Shelf Address is set to the IP address of the primary shelf • Subnet Mask is set according to Table 1-9 on page 1-72 • DHCP Address is set to 0.0.0.0 • Default Gateway Address is set according to Table 1-9 on page 1-72
54	In the Shelf Configuration dialog, click on the **OK** button. *The Confirm commissioning data modification dialog box appears.*
55	In the Confirm commissioning data modification dialog, click on the **Yes** button. *The System Manager closes and the shelf restarts.*
56	Wait 5 minutes for the shelf to complete the restart.
57	Repeat step 49 to step 56 for other DCN Gateway shelves, if any.
58	Log into a DCN Gateway shelf. See Procedure 1-1, "Logging into the network" on page 1-7. ***Note:*** Procedure 1-1 asks that you log into the primary shelf, instead, log into a DCN Gateway shelf although the DCN Gateway shelf and the primary shelf may be the same shelf.
59	In the Selected Shelves area: • click on the network name • click on the **Apply** button
60	Verify that the System Manager has contact with the shelves.

—end—

Procedure 1-34
Converting from public IP addressing to private IP addressing

Use this procedure to convert from public IP addressing to private IP addressing.

Requirements

- The following requirements apply:
- You must be logged into the System Manager as an Admin level user to change configuration information for a shelf.
- The System Manager must have contact with the shelves.
- Data-fill Table 1-10 on page 1-83 as follows:
  - — Record the shelf name of your primary shelf into the Shelf name field. Use an up-to-date map of your network to locate your primary shelf. You can also find this information in the System Manager by selecting the network name in the Selected Shelves area and then accessing the Configuration/Naming tab. The primary shelf is identified with the letter P in the Role field.
  - — Record the shelf name of all the other shelves in your network into the Shelf name field. You can find this information in the System Manager by selecting the network name in the Selected Shelves area and then accessing the Configuration/Naming tab.
  - — Enter a check for each shelf that is a DCN Gateway shelf. You can find this information in the System Manager by selecting the network name in the Selected Shelves area and then accessing the Configuration/Naming tab. A DCN Gateway shelf is identified with the letter G in the Role field.
  - — For each DCN Gateway shelf, record the default gateway address in the Default Gateway Address field.
  - — Record the IP address, DHCP address and Subnet mask for each shelf according to the new IP addressing plan. For more information about IP addressing, refer to the "Data communications in the Optical Metro 5100/5200 network" chapter of *Network Planning and Link Engineering,* 323-1701-110.

—continued—

Procedure 1-34 (continued)
Converting from public IP addressing to private IP addressing

- Before starting this procedure, ensure that the Internal OSPF Setting – OSPF Area ID in the Advanced Communications Settings panel is set to a value other than 0.0.0.0. Failure to do so will result in loss of IP routing capability between some of the shelves, which in turn may produce loss of contact with some shelves. In the event that the internal OSPF Area ID is set to 0.0.0.0, it is recommended to change it in every shelf to the current primary shelf address. See Procedure 1-29 "Defining or changing advanced communications settings for the network" on page 1-59.

Precautions

CAUTION
Risk of incorrect backup file
After you complete this procedure, back up the configuration data of all affected shelves. See Procedure 1-36, "Backing up shelf configuration data" on page 1-95 for more information.

CAUTION
Risk of loss of contact - Optical Network Manager /OMEA
If you change the NE configuration (for example, change the NE TID or NE IP address) (relevant for all configurations—private or public IP configurations) for Optical Metro 5100/5200 network elements, do not make the change and then attempt to rediscover the NE. The correct procedure is as follows: first delete the NE from OMEA and then make the change, and finally manage the NE again.

See *Optical Manager Element Adapter, Standard Operations Guide,* 450-3121-301, for procedures on deleting a network element and managing a network element.

CAUTION
Risk of loss of contact - SNMP
If the network is being managed by an SNMP manager there will be loss of contact with some or all of the shelves after you complete this procedure. To regain contact with the shelves, see "SNMP proxy service" in *Network Planning and Link Engineering,* 323-1701-110.

—continued—

Procedure 1-34 (continued)
Converting from public IP addressing to private IP addressing

Table 1-10
Procedure data

Shelf #	Shelf name	IP address	DHCP address	Subnet Mask	DCN Gateway	External Routing Mode	Default Gateway Address
Primary							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							

Table 1-10 (continued)
Procedure data

Shelf #	Shelf name	IP address	DHCP address	Subnet Mask	DCN Gateway	External Routing Mode	Default Gateway Address
26							
27							
28							
29							
30							
31							
32							
33							
34							
35							
36							
37							
38							
39							
40							
41							
42							
43							
44							
45							
46							
47							
48							
49							
50							
51							
52							

Table 1-10 (continued)
Procedure data

Shelf #	Shelf name	IP address	DHCP address	Subnet Mask	DCN Gateway	External Routing Mode	Default Gateway Address
53							
54							
55							
56							
57							
58							
59							
60							
61							
62							
63							
64							

Action

Step	Action
1	**If** — **Then** go to the primary shelf is a DCN Gateway and you have one or more DCN Gateway shelves — step 2 the primary shelf is not a DCN Gateway and you have a single DCN Gateway shelf — step 20 the primary shelf is not a DCN Gateway and you have multiple DCN Gateway shelves — step 28
2	Log into a DCN Gateway shelf. See Procedure 1-1, "Logging into the network" on page 1-7. ***Note:*** Procedure 1-1 asks that you log into the primary shelf, instead, log into a DCN Gateway shelf although the DCN Gateway shelf and the primary shelf may be the same shelf.
3	In the Selected Shelves area: • click on the DCN Gateway shelf you logged into • click on the **Apply** button

—continued—

Procedure 1-34 (continued)
Converting from public IP addressing to private IP addressing

Step	Action
4	In the Optical Metro System Manager window: • click on the Configuration tab • click on the Communications tab *The Communications list appears.*
5	In the Communications list, double-click on the shelf. *The Shelf Configuration window appears.*
6	In the Shelf Configuration window, set the parameters as follows: • Shelf is DCN Gateway box is checked • External Routing Mode is set to None • Shelf address is set according to Table 1-10 on page 1-83 • Primary Shelf Address is set to the IP address of the primary shelf • Subnet Mask is set according to Table 1-10 on page 1-83 • DHCP Address is set to 0.0.0.0 • Default Gateway Address is set according to Table 1-10 on page 1-83
7	In the Shelf Configuration dialog, click on the **OK** button. *The Confirm commissioning data modification dialog box appears.*
8	In the Confirm commissioning data modification dialog, click on the **Yes** button. *The System Manager closes and the shelf restarts.*
9	Wait 5 minutes for the shelf to complete the restart.
10	**If** / **Then** there are other DCN shelves / repeat step 2 to step 9 there are no other DCN shelves but there are remote shelves / go to step 11
11	In the Selected Shelves area: • click on a remote shelf (i.e., a shelf which is not a DCN Gateway shelf) • click on the **Apply** button
12	In the Optical Metro System Manager window: • click on the Configuration tab • click on the Communications tab *The Communications list appears.*
13	In the Communications list, double-click on the shelf. *The Shelf Configuration window appears.*

—continued—

Procedure 1-34 (continued)
Converting from public IP addressing to private IP addressing

Step	Action
14	In the Shelf Configuration window, set the parameters as follows: • Shelf is DCN Gateway box is cleared (External Routing Mode is automatically set to None) • Shelf address is set according to Table 1-10 on page 1-83 • Primary Shelf Address is set to the IP address of the primary shelf • Subnet Mask is set according to Table 1-10 on page 1-83 • DHCP Address is set according to Table 1-10 on page 1-83 • Default Gateway Address is set to 0.0.0.0
15	In the Shelf Configuration dialog, click on the **OK** button. *The Confirm commissioning data modification dialog box appears.*
16	In the Confirm commissioning data modification dialog, click on the **Yes** button. *The shelf restarts.*
17	Wait 5 minutes for the shelf to complete the restart and become visible within the System Manager session.
18	**If** / **Then** go to there are other DCN Gateway shelves — step 19 otherwise — step 64
19	**If** / **Then** there are other remote shelves — repeat step 2 to step 9 there are no other remote shelves — go to step 20
20	Log into the DCN Gateway shelf. Procedure 1-1, "Logging into the network" on page 1-7. ***Note:*** Procedure 1-1 asks that you log into the primary shelf, instead, log into the DCN Gateway shelf.
21	In the Selected Shelves area: • click on the DCN Gateway shelf you logged into • click on the **Apply** button
22	In the Optical Metro System Manager window: • click on the Configuration tab • click on the Communications tab *The Communications list appears.*
23	In the Communications list, double-click on the shelf. *The Shelf Configuration window appears.*

—continued—

Procedure 1-34 (continued)
Converting from public IP addressing to private IP addressing

Step	Action
24	In the Shelf Configuration window, set the parameters as follows: • Shelf is DCN Gateway box is checked • External Routing Mode is set to None • Shelf address is set according to Table 1-10 on page 1-83 • Primary Shelf Address remains set to what the primary IP address currently is - do not alter this parameter now • Subnet Mask is set according to Table 1-10 on page 1-83 • DHCP Address is set to 0.0.0.0 • Default Gateway Address is set according to Table 1-10 on page 1-83
25	In the Shelf Configuration dialog, click on the **OK** button. *The Confirm commissioning data modification dialog box appears.*
26	In the Confirm commissioning data modification dialog, click on the **Yes** button. *The System Manager closes and the shelf restarts.*
27	Wait 5 minutes for the shelf to complete the restart.
28	Log into the DCN Gateway shelf. Procedure 1-1, "Logging into the network" on page 1-7. ***Note:*** Procedure 1-1 asks that you log into the primary shelf, instead, log into the DCN Gateway shelf.
29	In the Selected Shelves area: • click on the primary shelf • click on the **Apply** button
30	In the Optical Metro System Manager window: • click on the Configuration tab • click on the Communications tab *The Communications list appears.*
31	In the Communications list, double-click on the shelf. *The Shelf Configuration window appears.*

—continued—

Procedure 1-34 (continued)
Converting from public IP addressing to private IP addressing

Step	Action
32	In the Shelf Configuration window, set the parameters as follows: • Shelf is DCN Gateway box is cleared (External Routing Mode is automatically set to None) • Shelf address is set according to Table 1-10 on page 1-83 • Primary Shelf Address is set according to Table 1-10 on page 1-83 ***Note:*** The Primary Shelf Address and the Shelf Address should match since the shelf you are modifying is the primary shelf. • Subnet Mask is set according to Table 1-10 on page 1-83 • DHCP Address is set according to Table 1-10 on page 1-83 • Default Gateway Address is set to 0.0.0.0
33	In the Shelf Configuration dialog, click on the **OK** button. *A Warning dialog box appears.*
34	In the Warning dialog, click on the **Yes** button. *The Confirm commissioning data modification dialog box appears.*
35	In the Confirm commissioning data modification dialog, click on the **Yes** button. *The shelf restarts.*
36	Wait 5 minutes for the shelf to complete the restart, for the modified primary data to get propagated around the network and for the shelf to become visible within the System Manager session.
37	**If** / **Then** go to there are other remote shelves (i.e., a shelf which is not a DCN Gateway shelf or the primary shelf) — step 38 otherwise — step 54
38	In the Selected Shelves area: • click on a remote shelf (a shelf which is not the DCN Gateway shelf or the primary shelf) • click on the **Apply** button
39	In the Optical Metro System Manager window: • click on the Configuration tab • click on the Communications tab *The Communications list appears.*
40	In the Communications list, double-click on the shelf. *The Shelf Configuration window appears.*

—continued—

Procedure 1-34 (continued)
Converting from public IP addressing to private IP addressing

Step	Action
41	In the Shelf Configuration window, set the parameters as follows: • Shelf is DCN Gateway box is cleared (External Routing Mode is automatically set to None) • Shelf address is set according to Table 1-10 on page 1-83 • Primary Shelf Address is set to the IP address of the primary shelf ***Note:*** This address is the same as the address you used as the Primary Shelf Address and Shelf Address in step 27. • Subnet Mask is set according to Table 1-10 on page 1-83 • DHCP Address is set according to Table 1-10 on page 1-83 • Default Gateway Address is set to 0.0.0.0
42	In the Shelf Configuration dialog, click on the **OK** button. *The Confirm commissioning data modification dialog box appears.*
43	In the Confirm commissioning data modification dialog, click on the **Yes** button. *The shelf restarts.*
44	Wait 5 minutes for the shelf to complete the restart and become visible within the System Manager session.
45	Repeat step 33 to step 39 for other remote shelves, if any. Otherwise continue with the next step.
46	In the Selected Shelves area: • click on the DCN Gateway shelf • click on the **Apply** button
47	In the Optical Metro System Manager window: • click on the Configuration tab • click on the Communications tab *The Communications list appears.*
48	In the Communications list, double-click on the shelf. *The Shelf Configuration window appears.*
49	In the Shelf Configuration window, set the Primary Shelf Address parameter to the IP address of the primary shelf. ***Note:*** This address is the same as the address you used as the Primary Shelf Address and Shelf Address in step 27.
50	In the Shelf Configuration dialog, click on the **OK** button. *The Confirm commissioning data modification dialog box appears.*

—continued—

Procedure 1-34 (continued)
Converting from public IP addressing to private IP addressing

Step	Action
51	In the Confirm commissioning data modification dialog, click on the **Yes** button. *The System Manager closes and the shelf restarts.*
52	Wait 5 minutes for the shelf to complete the restart.
53	**If** / **Then** there are other remote shelves — repeat step 38 to step 53 there are no other remote shelves — go to step 54
54	Log into another DCN Gateway shelf. Procedure 1-1, "Logging into the network" on page 1-7. ***Note:*** Procedure 1-1 asks that you log into the primary shelf, instead log into a DCN Gateway shelf.
55	In the Selected Shelves area: • click on the DCN Gateway shelf you logged into • click on the **Apply** button
56	In the Optical Metro System Manager window: • click on the Configuration tab • click on the Communications tab *The Communications list appears.*
57	In the Communications list, double-click on the shelf. *The Shelf Configuration window appears.*
58	In the Shelf Configuration window, set the parameters as follows: • Shelf is DCN Gateway box is checked • External Routing Mode is set to None • Shelf address is set according to Table 1-10 on page 1-83 • Primary Shelf Address is set to the IP address of the primary shelf • Subnet Mask is set according to Table 1-10 on page 1-83 • DHCP Address is set to 0.0.0.0 • Default Gateway Address is set according to Table 1-10 on page 1-83
59	In the Shelf Configuration dialog, click on the **OK** button. *The Confirm commissioning data modification dialog box appears.*
60	In the Confirm commissioning data modification dialog, click on the **Yes** button. *The System Manager closes and the shelf restarts.*
61	Wait 5 minutes for the shelf to complete the restart.

—continued—

Procedure 1-34 (continued)
Converting from public IP addressing to private IP addressing

Step	Action
62	Repeat step 49 to step 56 for other DCN Gateway shelves, if any. Otherwise continue with the next step.
63	Log into a DCN Gateway shelf. Procedure 1-1, "Logging into the network" on page 1-7. ***Note:*** Procedure 1-1 asks that you log into the primary shelf, instead, log into a DCN Gateway shelf although the DCN Gateway shelf and the primary shelf may be the same shelf.
64	In the Selected Shelves area: • click on the network name • click on the **Apply** button
65	Verify that the System Manager has contact with the shelves.

—end—

Procedure 1-35
Changing the target identifier (TID) properties

Use this procedure to change the target identifier (TID) properties of a shelf.

You can manually enter or change the TID value as well as change the following TID settings:

- TID is set to the shelf name
- TID is required for all TL1 commands

The TID must be between 1 and 20 alphanumeric characters. The first character must be a letter. The remaining characters can be any combination of letters, numbers, and hyphens (-). The TID is not case-sensitive. Unsupported characters include semicolon (;), underscore (_), period (.), colon (:), ampersand (&), greater than (>), less than (<), backslash (\), comma (,), spaces, and control characters. For more information on the TID, and TID naming restrictions, see the section "Target identifier and source identifier"in *TL1 Interface*, 323-1701-190.

If you change the NE configuration (for example, change the NE TID) (relevant for all configurations—private or public IP configurations) for Optical Metro 5100/5200 network elements, do not make the change and then attempt to rediscover the NE. The correct procedure is as follows: first delete the NE from OMEA and then make the change, and finally manage the NE again.

See *Optical Manager Element Adapter, Standard Operations Guide,* 450-3121-301, for procedures on deleting a NE and managing a NE.

Requirements

You must be an Admin level user to change the TID properties of a shelf.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Configuration tab.
3	Select the Naming tab.
4	Double-click on the shelf or right-click on the line and select Modify. *The Shelf Configuration dialog box appears.*
5	Click the **TID Properties** button. *The Shelf TID Change dialog box appears.*

—continued—

Procedure 1-35 (continued)
Changing the target identifier (TID) properties

Step	Action

6

If	Then go to
you want to change the set TID to shelf name setting	step 7
you want to manually change the TID value	step 9
you want to change the TID is required for all TL1 commands setting	step 11

7 Select or deselect the Set TID to Shelf Name check box to enable or disable this setting.

If	Then
selected	the Shelf Name field is enabled and the TID field is disabled. The TID value is automatically set to the current Shelf Name and any changes to the Shelf Name modify the current TID value. The Shelf Name must comply with the TID format or the setting is rejected.
deselected	the Shelf Name field is disabled and the TID field is enabled. You can modify the TID value manually.

8 Go to step 12.

9 Make sure the Set TID to Shelf Name check box is not selected and enter the TID into the TID field.

10 Go to step 12.

11 Select or deselect the TID required for all TL1 commands check box to enable or disable this setting.

If	Then
selected	all TL1 commands must include the TID parameter. A TL1 command executed with no TID is treated as a TL1 command with an invalid TID.
deselected	TL1 commands must not specify a TID

12 Click the **OK** button.

13 Click the **OK** button to close the Shelf Configuration window.

—end—

Procedure 1-36
Backing up shelf configuration data

Use this procedure to back up the configuration data for a shelf.

The network supports one instance of a backup operation for a particular shelf at any given time. You can perform multiple backups of different shelves in the network at the same time.

ATTENTION

Nortel Networks strongly recommends that you perform this procedure after commissioning a new shelf, changing shelf configuration, changing shelf passwords, or changing IP addresses. Perform backups as required according to your operating practices.

Note: Normally, System Manager does not backup the default target identifier (TID), the current active path for path switching, or the current active OCM for equipment switching. If the TID is not the default, or if the active path or the active OCM are forced switches, System Manager will backup and restore this data.

Requirements

You must be an Admin level user to back up configuration data on a shelf.

To perform a backup, the software load on the shelf must be in a committed state. The shelf must be commissioned and operational.

Optical Metro 5200

During a backup operation for an Optical Metro 5200 shelf, make sure that the SP circuit pack and at least one OCM circuit pack are inserted in the shelf and are in-service. If you do not do this, data can be lost after the backup operation.

Optical Metro 5100

During a backup operation for an Optical Metro 5100 shelf, make sure that the SP circuit pack and at least one non-SP circuit pack that carries the database are seated in the shelf and are in-service. If you do not do this, data can be lost after the backup operation.

—continued—

Procedure 1-36 (continued)
Backing up shelf configuration data

Precautions

CAUTION
Risk of information loss
If your computer uses a Windows operating system, do not use any of the following characters in your file names: / : " < | > * ?. In most cases, an error message indicates that the file will not save correctly. If you use * or ? in the file name, Windows does not save the file, and fails to provide any error message or warning that information will be lost.

CAUTION
Risk of a loss of contact
If the Access Control State of the shelf is different from the existing Access Control State of the other shelves in the hubbing group, a loss of contact may occur with the remote shelves during a Backup and Restore procedure (if the original shelf does not have any Overhead Communication available). Make sure the Access Control State of all the shelves in the hubbing group is the same.

CAUTION
Risk of incorrect backup file
Make sure that all personnel do not perform any provisioning changes or start a software upgrade during the backup procedure.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Configuration tab.
3	Select the Naming tab.
4	Double-click on the shelf that you want to backup or right-click on the line and select Modify. *The Shelf Configuration window appears.*

—continued—

Procedure 1-36 (continued)
Backing up shelf configuration data

Step	Action
5	Click **Backup**. *The Save Backup File As: window appears.* ***Note:*** System Manager proposes that you save the backup file to /NortelNetworks/OpteraMetro/Backup/ for Windows, or to /home/user/OpteraMetro/Backup for UNIX. The proposed file naming convention is: <shelf IP>_<shelf type> _<version/load number>_<system time>_<date>.dat as in '47.114.241.165_terminal_6.0.28.2_1258_12Feb2003.dat'.
6	If required, change the proposed file name and default directory. Click **Save**. *The Confirm Backup dialog box appears.*
7	Click **Yes** to confirm. *The Backup Status dialog box appears. It takes 3 to 5 seconds to complete the backup. While the backup is in progress a "Backup In progress" message is displayed on the Shelf Configuration window. When the backup is complete, the Backup Status dialog box appears.*
8	Read the status messages and click **Close**. ***Note 1:*** If the backup procedure fails, an error message is displayed in the Backup Status dialog. ***Note 2:*** Normally, System Manager does not backup the default target identifier (TID), the current active path for path switching, or the current active OCM for equipment switching. If the TID is not the default, or if the active path or the active OCM are forced switches, System Manager backs up and restores this data.

—end—

Procedure 1-37
Restoring shelf configuration data

Use this procedure to restore a commissioned shelf to service after a major failure.

The network supports one instance of a restore operation for a particular shelf at any given time. You can restore different shelves in the network at the same time.

System Manager prompts you to restart the shelf to complete this procedure.

> ***Note:*** Normally, System Manager does not backup the default target identifier (TID), the current active path for path switching, or the current active OCM for equipment switching. If the TID is not the default, or if the active path or the active OCM are forced switches, System Manager will backup and restore this data.

Requirements

You must be an Admin level user to restore configuration data on a shelf.

The configuration restore file must be of the same release as the commissioned shelf.

Optical Metro 5200
During a restore operation for an Optical Metro 5200 shelf, make sure that the SP circuit pack and at least one OCM circuit pack are inserted in the shelf and are in-service. If you do not do this, data can be lost after the restore operation.

Optical Metro 5100
During a restore operation for an Optical Metro 5100 shelf, make sure that the SP circuit pack and at least one non-SP circuit pack that carries the database are seated in the shelf and are in-service. If you do not do this, data can be lost after the restore operation.

Precautions

CAUTION
Risk of losing information
The restore operation overwrites all previous configuration information stored on the SP and OCM circuit packs in the target shelf. Once you commit the load on the shelf as outlined in step 12, cancellation is not possible.

—continued—

Procedure 1-37 (continued)
Restoring shelf configuration data

CAUTION
Risk of traffic loss
Nortel Networks recommends that you only restore shelf configuration data to an out-of-service shelf.

CAUTION
Risk of a loss of contact
If the Access Control State of the shelf is different from the existing Access Control State of the other shelves in the hubbing group, a loss of contact may occur with the remote shelves during a Backup and Restore procedure (if the original shelf does not have any Overhead Communication available). Make sure the Access Control State of all the shelves in the hubbing group is the same.

ATTENTION
If a circuit pack was deleted in the shelf inventory before the backup, the circuit pack autoprovisions after the restore operation.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Configuration tab.
3	Select the Naming tab.
4	Double-click on the shelf that you want to restore or right-click on the line and select Modify. *The Shelf Configuration dialog box appears.*
5	Click **Restore**. *The Restore dialog box appears.*

—continued—

Procedure 1-37 (continued)
Restoring shelf configuration data

Step	Action
6	In the Restore dialog box, select which aspects of the data file you want to load to the shelf. If you do not select any items, System Manager defaults to the basic shelf configuration. The following list describes the data associated with each selection item. • User Profile—includes (but is not limited to) user names, passwords, and privileges • Commissioning Data—shelf information which includes (but is not limited to) network name, shelf site name, shelf name, shelf description, node type, shelf number, site identifier, shelf identifier, primary node address, hubbing group, IP address, subnet mask, DHCP address, gateway IP address, TID, gateway flag, TCP port, Telnet port, maximum number of TCP sessions, maximum number of Telnet sessions, maximum number of sessions connected to other nodes (gateway sessions)
7	Click the **Transfer** button. *The Choose Restore File dialog box appears.*
8	Browse through the file system and select the correct file to restore the shelf. Click **Open**. *The Confirm Transfer dialog box appears.*
9	Click **Yes** to confirm the file transfer to the target shelf or click **No** to back out of the restore process. *When the transfer is completed a message indicating success appears on the Shelf Configuration dialog box ("Successful file transfer to the SP"). The restore file resides on the SP circuit pack of the target shelf.*
10	Click the **Load** button. *The Confirm Load dialog box appears.*
11	Click **Yes** to confirm the shelf load or click **No** to back out of the restore process. *A message indicating the status of the shelf load appears on the Shelf Configuration dialog box ("Successful data load").*
12	Click the **Commit** button to commit the load to the shelf. ***Note:*** It is not possible to cancel the shelf restore process once the load is committed. If you do not want to commit the load, click **Cancel**. *A Confirm Commit dialog box appears.*

—continued—

Procedure 1-37 (continued)
Restoring shelf configuration data

Step	Action
13	Click **Yes** to confirm the commit or click **No** to back out of the restore process. *A message indicates the status of the restore process, which takes approximately 40 seconds. Once complete, the Restore Status dialog box appears. If the commit operation is successful, a shelf level restart is triggered, which shuts down System Manager (on the shelf where System Manager was invoked).* ***Note:*** Restore only one shelf at a time and wait for five minutes between two restores.
14	Click **Close**.
15	Restart your browser to restart System Manager on the host shelf.

—end—

Procedure 1-38
Changing clock reference settings for the OCI SRM SONET/SDH 1310 nm

Use this procedure to change clock reference settings for an OCI SRM SONET/SDH 1310 nm circuit pack.

For more information about OCI SRM SONET/SDH 1310 nm circuit packs, see "See Table 4-6 for actions during the holdoff period." in the "General circuit pack information" chapter of *Hardware Description*, 323-1701-102.

Requirements

ATTENTION

If you use a OCI SRM SONET/SDH 1310 nm circuit pack, you must make sure that the four OC-12/STM-4 source signals come from a single SONET/SDH transport product that can be configured for either BITS synchronization or line timing. You cannot connect the OC-12/STM-4 signals to a SONET/SDH SRM OCI from a source that cannot function as a SONET/SDH transport product.

The four OC-12/STM-4 source traffic signals that are to be connected to the SONET/SDH SRM OCI must be frequency synchronous to a single internal clock source.

You must be an Admin level user to change the clock reference settings for an OCI SRM SONET/SDH 1310 nm circuit pack.

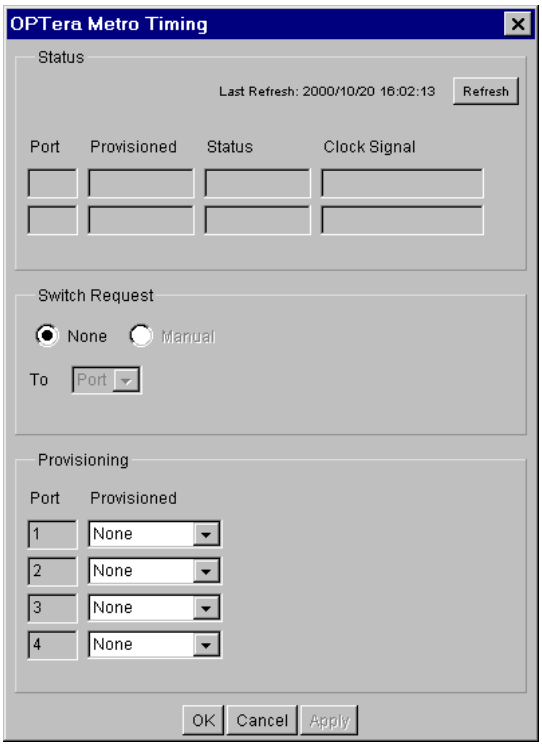
Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Connections tab.
3	Select the Channel Assignments tab.
4	Right-click on the SRM circuit pack that represents the appropriate OCI SRM SONET/SDH.
5	From the menu that appears, select Timing Ref. *The Optical Metro Timing dialog box appears.*

—continued—

Procedure 1-38 (continued)
Changing clock reference settings for the OCI SRM SONET/SDH 1310 nm

Step	Action



Note 1: The Timing Ref. menu item is available only when you select an OCI SRM SONET/SDH circuit pack. If it is not available, check that you have selected the correct type of SRM circuit pack.

Note 2: When you create a channel assignment for an OCI SRM SONET/SDH circuit pack, the first port that you select for a channel assignment is automatically used as the primary clock reference for the SONET/SDH signal. The second port that you select for a channel assignment is automatically used as the secondary clock reference for the SONET/SDH signal. You can change the clock reference at any time after making channel assignments.

Note 3: A port facility must be in-service to be selected as a timing reference.

6 In the Provisioning area, use the drop-down menus to select one port to be the primary clock reference and one port to be the secondary clock reference. This action does not affect traffic.

7 Click **Apply**.

Note: The change can take up to 10 seconds to occur. The status updates when the change is complete. You can also click **Refresh** to update the status.

8 Click **OK**.

—end—

Procedure 1-39
Performing a health check

Use this procedure to check on the operating performance of any shelf in the network. Nortel Networks recommends that you perform a health check

- before starting a software upgrade
- after completing a software upgrade to verify the successful completion of the upgrade on all the shelves in the network
- after seating the circuit packs and powering up the shelf to verify the hardware baseline

For information about how to troubleshoot exceptions in health check reports, follow "Troubleshooting hardware baseline exceptions in Health Check reports" in the *Trouble Clearing and Alarm Reference Guide*, 323-1701-542.

Requirements

You must be an Admin level user to perform a health check on a shelf.

Precautions

CAUTION
Risk of information loss
If your computer has a Windows operating system, do not use any of the following characters in your file names: / : " < | > * ?. In most cases, an error message indicates that the file will not save properly. If you use * or ? in the file name, Windows does not save the file, and fails to provide any error message or warning that information will be lost.

CAUTION
Risk of unreliable health check status on shelves prior to release 5.0
If the target shelf is running a software release lower than release 5.0, you must verify the content of the health check report to find out if the shelf is healthy. You cannot rely only on the health check status in the System Manager. To verify the content of a health check report, see Procedure 1-40, "Saving a health check report". This procedure allows you to save a health check report and use any text editor to view the report. Use "Troubleshooting hardware baseline exceptions in Health Check reports" in the *Trouble Clearing and Alarm Reference Guide*, 323-1701-542, to troubleshoot any exceptions in the health check report.

—continued—

Procedure 1-39 (continued)
Performing a health check

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Admin tab. *The Software Upgrade window appears.*
3	Right-click on the target shelf.
4	Click the Health Check menu item. *The H/W Baseline File Section dialog box appears.*
5	Select the appropriate hardware baseline file location and click **OK**. *A progress bar indicates the percentage progress of the health check as it runs on the target shelf. When complete, the Health Check Status dialog box prompts the user.*

6

If	Then
the Health Check Status dialog box indicates that the health check was completed successfully	go to step 7
otherwise	call your next level of support

—continued—

Procedure 1-39 (continued)
Performing a health check

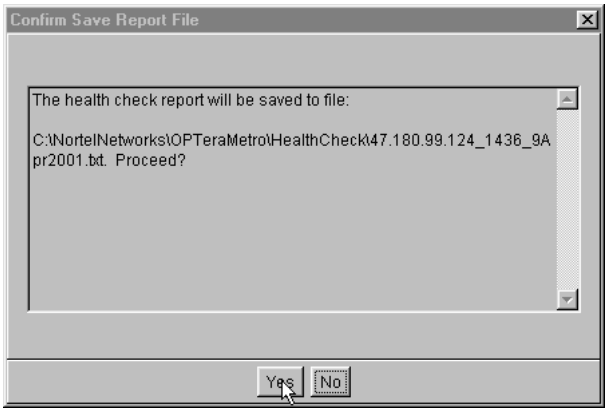
Step	Action
7	Click **Yes** to save the report. *The Save Report File As: window appears.* ***Note:*** System Manager proposes that you save the report to /NortelNetworks/OpteraMetro/HealthCheck/ for WIndows, or to /home/user/OpteraMetro/HealthCheck for UNIX. The proposed file naming convention is: <shelf IP>_<system_time>_<date>.txt as in '47.114.241.165_1304_12Feb2003.txt'.

ATTENTION
Make sure that the file extension specified is ".txt". Healthcheck reports are saved in plain text format.

8 If required, change the proposed file name and default directory.

9 Click **Save**.

OM0573



The Confirm Save Report File dialog box appears.

10 Click **Yes** to complete the process.

—end—

Procedure 1-40
Saving a health check report

Use this procedure to verify if a health check report exists on the SP and to save the health check report file. The health check report file is saved in a text format and can be viewed using any text editor.

For information about how to troubleshoot exceptions in health check reports, follow "Troubleshooting hardware baseline exceptions in Health Check reports" in the *Trouble Clearing and Alarm Reference Guide*, 323-1701-542.

Requirements

You must be an Admin level user to save a health check report for a shelf.

Action

Step	Action	
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.	
2	Select the Admin tab. *The Software Upgrade window appears.* ***Note:*** To list all shelves in the Software Upgrade window, check the **All shelves** box and click on **Refresh**.	
3	Right-click on the target shelf. *A menu appears.*	
4	Click the Report menu item.	
5	**If**	**Then** go to
	a report file already exists	step 7
	otherwise	step 6
6	A Report File Status dialog box is displayed advising the user to perform a health check. Refer to Procedure 1-39 "Performing a health check" in this book to perform a health check on the target shelf.	
7	A Save Report File As: window appears specifying the file name and the default directory. Click **Save** to save the report. A Confirm Save Report File dialog box appears. ***Note:*** System Manager proposes that you save the health check report to /NortelNetworks/OpteraMetro/HealthCheck/ for WIndows, or to /home/user/OpteraMetro/HealthCheck for UNIX. The proposed file naming convention is: <shelf IP>_<system_time>_<date>.txt as in '47.114.241.165_1304_12Feb2003.txt'.	

—continued—

Procedure 1-40 (continued)
Saving a health check report

Step	Action

ATTENTION
Make sure that the file extension specified is ".txt". Healthcheck reports are saved in plain text format.

8 Click **Yes**.

9 To view details of the report file, open the health check report file using any text editor.

—end—

Procedure 1-41
Displaying shelf level graphics

Use this procedure to display a graphical representation of a shelf through the System Manager. The shelf level graphic window displays provisioning information, physical circuit pack information, shelf details, and alarm information on a per slot basis.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Click the **Selected Shelves** button to display the network tree.
3	Make sure that the desired shelf is selected in the network tree. By default the shelf you are logged into is displayed as the selected shelf. You can select any shelf in the network. For more information on selecting a shelf see Procedure 1-15 "Selecting shelves", in this chapter.
4	Display the Shelf Level Graphics window by: • clicking on the **Shelf Level Graphics** button on the Equipment—Inventory window • selecting Shelf Level Graphics from the menu that appears when you right-click on a circuit pack in the Equipment—Inventory window • selecting Shelf Level Graphics from the menu that appears when you right-click on the Active Alarms window when the alarm display is not empty *After a few seconds, the Shelf Level Graphics window appears.*

—continued—

Procedure 1-41 (continued)
Displaying shelf level graphics

Step	Action
5	Review the information in the Shelf Level Graphics window to see an overview of the current state of the shelf. The Shelf Level Graphics window consists of a graphical view of the shelf, an area (bottom left) for displaying shelf details, and an area (bottom right) for displaying circuit pack details. The graphical view of the shelf displays different components that make up the shelf. Circuit pack graphics are shown located within their proper slots. The state of the circuit pack is represented graphically. If there are alarms for that circuit pack, the highest severity alarm is displayed on the circuit pack and the graphic is outlined in the appropriate alarm color. The Shelf Details area initially displays shelf details. The Circuit Pack Selection area is initially populated with the details of the selected circuit pack. ***Note 1:*** The Shelf icon that appears to the right of the shelf graphic indicates alarms that are raised against non-circuit pack items, such as a shelf alarm. You can display information about any of these alarms by right-clicking on the icon and selecting Show Alarms from the popup menu. When you do this, an Alarm Filtering window opens, showing the Active Alarms selected. ***Note 2:*** In the shelf graphics window alarms refresh automatically but equipment/inventory data does not. For example, if you seat a circuit pack into slot 2, it does not appear in the Shelf Level Graphics window until you click the Refresh button. ***Note 3:*** If you do not want visual alarm indicators displayed in the Shelf Level Graphics window, de-select the Alarm check box in the window. The alarms for that shelf are no longer displayed when the alarms check box is not checked. **—end—**

Procedure 1-42
Displaying shelf level graphic details for a shelf circuit pack

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

Action

Step	Action
1	Display the shelf graphics for the selected network element. See Procedure 1-41 “Displaying shelf level graphics”, in this chapter.
2	Click on a circuit pack within the Shelf Level Graphics window to select it. ***Note:*** If a circuit pack has alarms against it, the color and severity of the highest alarm raised against that circuit pack is displayed.
3	Review the circuit pack information in the Circuit Pack Selection details area. ***Note 1:*** When a new alarm is raised against a circuit pack, an alarm balloon appears on that circuit pack in the Shelf Level Graphics window. Alarm balloons indicate new alarms that have appeared since the last refresh of the Shelf Level Graphics window. It is a visual indication to the user that a new alarm has been reported since the last time the data in the window was refreshed. When the user first enters the Shelf Level Graphics window, no balloons are displayed. Instead, circuit packs with alarms are outlined in the alarm severity color. After this point, any new alarms that appear are indicated by an alarm balloon against the circuit pack or the shelf alarm icon. The user can clear the balloon by right-clicking on the balloon and selecting “Clear balloon”. Refreshing the Shelf Level Graphics window also clears all alarm balloons. ***Note 2:*** When you right-click on the circuit pack in the graphics display and select Show Alarms from the popup menu, an Alarm Filtering window opens showing the Active alarms for the selected circuit pack. ***Note 3:*** If you do not want visual alarm indicators displayed in the Shelf Level Graphics window, de-select the Alarm check box in the window. The alarms for that shelf are no longer displayed when the alarms check box is not checked.

—end—

Procedure 1-43
Enabling or disabling automatic laser shutdown

The Automatic Laser Shutdown (ALS) feature shuts down DWDM lasers and consequently brings the power level down to the Class I hazard level (10 dBm) within three seconds in case of a fiber break. The ALS feature applies to all Optical Metro 5100/5200 OADM, Mixed and terminal shelves. For the Mixed shelf type, ALS is not applicable to OFA or APBE circuit pack. Use this procedure to enable or disable the feature in the System Manager at the shelf level. ALS is disabled by default.

Note: The ALS must be enabled at both the near end and far end to take effect.

Requirements

You must be an Admin or Operator level user to enable or disable automatic laser shutdown on a shelf.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, “Logging into the network” on page 1-7.
2	In the System Manager main window, select the Admin tab.
3	Select the NE Admin tab.
4	Select the shelf where you want to enable or disable automatic laser shutdown.
5	Right-click on the highlighted row. From the popup menu, select Auto. Laser Shutdown, and then Enable/Disable. *The Auto. Laser Shutdown Enable/Disable window appears.*
6	In the Auto. Laser Shutdown area, select the Enable or Disable radio button.
7	Click the **OK** button. *After a few seconds, the ALS window appears, indicating that the ALS modification is successful.*
8	Click the **Close** button.

—end—

Procedure 1-44
Enabling or disabling automatic laser recovery

If automatic laser shutdown (ALS) is enabled, lasers between OCLDs and OTRs are shut down in case of a fiber break. After the broken fiber is repaired, lasers can be restored either automatically or manually. Use this procedure to enable or disable automatic laser recovery in the System Manager at the shelf level. Automatic laser recovery is disabled by default. When automatic laser recovery is enabled, it takes up to five minutes for the optical power to restore automatically. If you want to recover traffic earlier, you can also issue a manual recovery command even when automatic recovery is enabled.

For more information about enabling manual laser recovery, refer to Procedure 1-45 “Enabling manual laser recovery” on page 1-115.

Requirements

You must be an Admin or Operator level user to enable or disable automatic laser recovery on a shelf.

Automatic laser recovery is available only after ALS has been enabled.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, “Logging into the network” on page 1-7.
2	In the System Manager main window, select the Admin tab.
3	Select the NE Admin tab.
4	Select the shelf where you want to enable or disable automatic laser recovery.
5	Right-click on the highlighted row. From the menu that appears, select Auto. Laser Shutdown, and then Enable/Disable. *The Auto. Laser Shutdown Enable/Disable window appears.*
6	In the Auto. Laser Shutdown area, make sure that the Enable radio button is selected. ***Note:*** If the Enable radio button is not selected, you cannot enable or disable Auto. Laser Recovery.
7	In the Auto. Laser Recovery area, select the Enable or Disable radio button.

—continued—

Procedure 1-44 (continued)
Enabling or disabling automatic laser recovery

Step	Action
8	Click the **OK** button. *After a few seconds, the ALS window appears, indicating that the ALS modification is successful.*
9	Click the **Close** button.

—end—

Procedure 1-45
Enabling manual laser recovery

If automatic laser shutdown (ALS) is enabled, lasers between OCLDs and OTRs are shut down in case of a fiber break. After the broken fiber is repaired, lasers can be restored either automatically or manually. Use this procedure to enable manual laser recovery in the System Manager at the shelf level. Manual recovery is disabled by default. Manual recovery restores traffic immediately. You can also issue a manual activation command when automatic recovery is enabled but you do not want to wait for up to five minutes for laser recovery.

For more information about enabling or disabling automatic laser recovery, refer to Procedure 1-44 “Enabling or disabling automatic laser recovery” on page 1-113.

Requirements

You must be an Admin or Operator level user to enable manual laser recovery on a shelf.

You cannot set manual recovery if ALS is disabled.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, “Logging into the network” on page 1-7.
2	In the System Manager main window, select the Admin tab.
3	Select the NE Admin tab.
4	Select the shelf where you want to enable manual laser recovery.
5	Right-click on the highlighted row. From the menu that appears, select Auto. Laser Shutdown, and then Manual Activation. *The Auto. Laser Shutdown Manual Activation window appears.*
6	In the Auto. Laser Shutdown area, click the **Manual Activation** button. *The ALS window appears, indicating that the ALS manual activation is successful.*
7	Click the **Close** button to return to the Auto. Laser Shutdown Manual Activation window.
8	Click the **OK** button.

—end—

Procedure 1-46
Enabling or disabling remote fault notification

Use this procedure to enable or disable remote fault notification.

If you enable remote fault notification, the system raises a service-affecting alarm at the near-end node when the far-end node has a service-affecting alarm. This ensures that at least one service-affecting alarm is reported by the system in case the communications between the far-end node and the gateway network element (GNE) are lost.

Requirements

You must be an Admin or Operator level user to enable or disable remote fault notification.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	In the System Manager main window, select the Admin tab.
3	Select the NE Admin tab.
4	Select the shelf where you want to enable or disable remote fault notification.
5	Right-click on the highlighted row. From the menu that appears, select Remote Fault Notification. *The Remote Fault Notification dialog box appears.*
6	Select either the Enable or Disable radio button.
7	Click **OK**. *A dialog box opens indicating that the operation was successful.*
8	Click **Close**.

—end—

Procedure 1-47
Enabling or disabling passive slot numbering

Use this procedure to enable or disable passive slot numbering on a shelf.

When the passive slot numbering feature is enabled for the first time, all passive slot numbers are mapped to their default values. After you enable passive slot numbering, you can then edit the slot number for all passive devices. See Procedure 3-33 "Provisioning the slot number of a passive device".

For more information on the user provisionable slot numbers feature including the default slot assignments, refer to "User provisionable slot numbers" on page 6-4 in *Software and User Interface*, 323-1701-101.

Requirements

You must be an Admin or Operator level user to enable or disable passive slot numbering.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	In the System Manager main window, select the Admin tab.
3	Select the NE Admin tab.
4	Select the shelf where you want to enable or disable passive slot numbering.
5	Right-click on the highlighted row. From the menu that appears, select Passive Slot Numbering. *The Passive Slot Numbering dialog box appears.*
6	Select either the Enable or Disable radio button.
7	Click **OK**. *A confirmation dialog box opens.*
8	Click **Yes** to confirm the operation.

—end—

Procedure 1-48
Exiting the System Manager

Use this procedure to exit the System Manager.

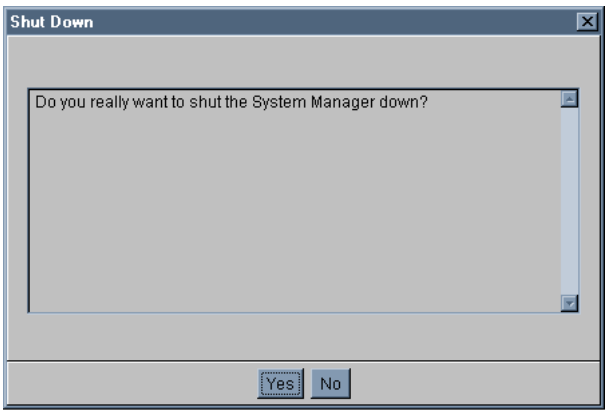
Requirements

You must be logged in to the System Manager to perform this procedure.

Action

Step	Action
1	From the File menu, select Exit. *The Shut Down dialog box appears.*

OM0236



2	**If**	**Then** click
	you want to exit System Manager	**Yes**
	otherwise	**No**

—end—

Managing security and user accounts

Follow the procedures in this chapter to manage network security and user accounts in System Manager.

For more information on planning your network security, see Chapter 11 "Network security planning" in *Network Planning and Link Engineering*, 323-1701-110.

Before you begin

Before you begin the procedures in this chapter, make sure that you have commissioned the network according to the "Commissioning a shelf" chapter, in *Commissioning Procedures,* 323-1701-220.

Log in to the System Manager as an Admin level user.

Precautions

CAUTION
Risk of shelf malfunction
Nortel Networks recommends that you do not use cellular phones at any Optical Metro 5100/5200 site. The use of cellular phones in proximity to Optical Metro equipment can cause shelf malfunction.

CAUTION
Risk of affecting network reliability
Make sure that all connectors are cleaned before you make the connections (or re-connections) described in this procedure. For cleaning information, see the chapter "Cleaning connectors", in *Installing Optical Metro 5200 Shelves and Components*, 323-1701-201.

CAUTION
Risk of incorrect backup file
Back up the shelf after provisioning changes. Otherwise, the shelf could be restored from an out-of-date backup file in the event of shelf failure. See Procedure 1-36 "Backing up shelf configuration data" for details.

Procedure list

Table 2-1 lists the procedures in this chapter.

Table 2-1
Procedures for managing security and user accounts

Procedure	Page	Comments
2-1 Viewing user account details for a shelf	2-3	Required.
2-2 Adding a user account	2-4	Required.
2-3 Changing a user account	2-6	Required.
2-4 Deleting a user account	2-10	Required.
2-5 Viewing the login user list	2-12	Required.
2-6 Changing your password	2-13	Required.
2-7 Changing the community name	2-15	Required.
2-8 Setting the centralized security administration attributes	2-18	Required.
2-9 Setting intrusion attempts handling	2-21	Required.
2-10 Setting the primary or secondary RADIUS server attributes	2-22	Required.
2-11 Changing the challenge/response shared secret for a shelf	2-24	Required.
2-12 Changing the shared secret for the primary or secondary RADIUS server	2-25	Required.
2-13 Clearing security alarms	2-26	Required.

Procedure 2-1
Viewing user account details for a shelf

Use this procedure to view the list of all user accounts for a shelf and the associated details.

Requirements

You must be logged in to the System Manager as an Admin level user to view user account details.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Security tab.
3	Select the User Profile List tab. *The User Profile List window appears.* The existing user accounts for the selected shelf are listed in the User Profile List window. The following user account details are provided in the table: • the user index (the maximum number of local users is ten) • the user IDs, which are the account names for the selected shelf • the user privilege class associated with each account (ADMIN, OPERATOR, OBSERVER, CUSTOMER1, or CUSTOMER2) • the status of the account, indicating whether the account is enabled or disabled • the Idle Timeout setting **—end—**

Procedure 2-2
Adding a user account

Use this procedure to add a new local user account. Three user accounts are available by default: admin, operator and observer (at Index 1 through 3). In addition to the default user accounts, you can provision up to seven user accounts for the ring. The additional user accounts can be any of the following user classes: admin, operator, observer, customer1, and customer2.

> ***Note:*** You cannot delete the three default user accounts, but you can modify their user IDs. See Procedure 2-3 "Changing a user account".

Each user ID has a provisionable name and a user privilege class of admin, operator, observer, customer1, or customer2.

This procedure sets the following user account parameters:

- user identifier
- user privilege class
- password
- account status (enabled or disabled)
- idle timeout period

Requirements

You must be logged in to the System Manager as an Admin level user to add a user account.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Click on the Selected Shelves drop-down list, and double-click on the shelf for which you want to add a user account.
3	Select the Security tab.
4	Select the User Profile List tab. *The User Profile List window appears.*
5	Highlight an empty index row (4 through 10).
6	Double-click the row, or right-click the row and select Add. *The Add User dialog box appears.*

—continued—

Procedure 2-2 (continued)
Adding a user account

Step	Action
7	Enter a user identification in the UserID field. ***Note:*** The user ID is a character string (between 5 and 8 characters) that can be any combination of letters and numbers.
8	Select a user privilege class from the User Class drop-down list, see Table 1-1 on page 1-2 for definitions.
9	Enter a password in the User Password field. ***Note 1:*** The password is case sensitive and must be between eight and ten characters. ***Note 2:*** Passwords are not echoed on the screen. Asterisks are displayed in the Password field.
10	Enter the password again in the Confirm Password field.
11	Select enabled from the User Status drop-down list to enable the user account.
12	Enter a value in the Idle Timeout field. ***Note:*** The idle timeout period range is 0 to 999 minutes. This field indicates the period a shelf can remains idle before a timeout occurs. If the field is set to zero, the shelf never times out.
13	Click OK to return to the User Profile List window. You have completed this procedure.
14	Click **OK**.

—end—

Procedure 2-3
Changing a user account

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

- user identifier
- user privilege class

  Note: You cannot modify the user privilege class of the three default users: admin, operator and observer (at Index 1 through 3). Also, the Admin-level user cannot disable the default local Admin-level user.

- password
- account status (enabled or disabled)
- Idle Timeout

Requirements

You must be logged in to the System Manager as an Admin level user to modify a user account.

Precautions

CAUTION
Risk of incorrect backup file
Once password changes are made at the primary shelf, back up all affected shelves. Otherwise, the shelf could be restored from an out-of-date backup file in the event of shelf failure. See Procedure 1-36, "Backing up shelf configuration data" for details.

CAUTION
Risk of a System Manager shut down after password changes
Once a password is changed, a dialog box appears asking the user to shut down System Manager. Only the local user who is currently in the System Manager session that changed the password can ignore this request. All other users who are accessing System Manager remotely must shut down and restart System Manager after password changes.

—continued—

Procedure 2-3 (continued)
Changing a user account

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Click on the Selected Shelves drop-down list, and double-click on the shelf for which you want to modify a user account.
3	Select the Security tab.
4	Select the User Profile List tab. *The User Profile List window appears.*
5	Select the user account to be modified.
6	Double-click the row, or right-click the row and select Modify. *The Modify User dialog box appears.*

7 **If** you want to modify a user's — **Then** go to

user ID	step 8
user privilege class	step 11
password	step 14
account status	step 18
Idle Timeout	step 21

Modifying a user ID

8 In the UserID field, type a new user ID.

Note: The user ID is a character string (between 5 and 8 characters) that can be any combination of letters and numbers.

9 **If** you — **Then** go to

want to modify more user profile attributes	step 7
do not want to modify more user profile attributes	step 10

10 Click OK to return to the User Profile List window.

You have completed this procedure.

—continued—

Procedure 2-3 (continued)
Changing a user account

Step	Action

Modifying a user privilege class

11 Select a user privilege class from the User Class drop-down list.

Note: You cannot modify the user privilege class of the three default users.

12

If you	**Then** go to
want to modify more user profile attributes	step 7
do not want to modify more user profile attributes	step 13

13 Click OK to return to the User Profile List window.

You have completed this procedure.

Modifying a password

14 Enter a new password in the User Password field.

Note: The password is case sensitive and must be between eight and ten characters.

15 Re-enter the new password in the Confirm Password field.

16

If you	**Then** go to
want to modify more user profile attributes	step 7
do not want to modify more user profile attributes	step 17

17 Click OK to return to the User Profile List window.

You have completed this procedure.

Modifying the user account status

18 Select a user account status from the User Status drop-down list.

Note 1: You cannot disable the default Admin user at Index 1. You can disable the default Operator and Observer users at Index 2 and Index 3.

Note 2: If you disable a user account, System Manager notifies and disables all active sessions logged in using that user account.

19

If you	**Then** go to
want to modify more user profile attributes	step 7
do not want to modify more user profile attributes	step 20

20 Click OK to return to the User Profile List window.

You have completed this procedure.

—continued—

Procedure 2-3 (continued)
Changing a user account

Step	Action

Modify the Idle Timeout period

21 Enter a new value in the Idle Timeout field.

Note: The idle timeout period range is 0 to 999 minutes. This field indicates the period a shelf can remains idle before a timeout occurs. If the field is set to zero, the shelf never times out.

22 Click OK to return to the User Profile List window.

—end—

Procedure 2-4
Deleting a user account

Use this procedure to delete a local user account. When you delete a user account, System Manager notifies and closes all active sessions logged in using the deleted account.

> ***Note:*** You cannot delete the three default user accounts, but you can modify their user IDs, and you can disable the default Operator and Observer accounts. See Procedure 2-3 "Changing a user account". However, the Admin-level user cannot disable the default local Admin-level user.

Requirements

You must be logged in to the System Manager as an Admin level user to delete a user account.

—continued—

Procedure 2-4 (continued)
Deleting a user account

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Click on the Selected Shelves drop-down list, and double-click on the shelf for which you want to delete a user account.
3	Select the Security tab.
4	Select the User Profile List tab. *The User Profile List window appears.*
5	Select the user account to be deleted. ***Note:*** You cannot delete the three default user accounts (index 1 through index 3).
6	Right-click the row and select Delete. *The Confirm User Delete dialog box appears.*
7	Click **OK** to delete the user account. *System Manager notifies and closes all active sessions logged in using the deleted account.*

—end—

Procedure 2-5
Viewing the login user list

Use this procedure to view the list of active user sessions that are logged in a shelf through the System Manager or TL1.

Requirements

You must be logged in to the System Manager as an Admin level user to view the login user list.

Action

Step	Action
1	Log in to the System Manager with your user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	Select the Security tab.
3	Select the Login User List tab. *The Login User List window appears.* ***Note 1:*** The Shelf Name and Shelf IP are the name and IP address of the host shelf. The Machine IP is the user IP address where SMI session is running or TL1 session is started. The Group.User ID column lists the user group and user ID for the session. The Trap Port is only applicable to SMI sessions, indicating the communication port through which the SMI session receives information. The Session Type indicates whether the session is System Manager (SMI) or Transaction Language 1 (TL1). ***Note 2:*** The Group.UserID field could also indicate an "emsmetro" user. The emsmetro account is an alias to Admin user and used by Optical Manager Element Adapter (OMEA) to establish a network management session. ***Note:*** If the physical connection between a System Manager session and a network element breaks (for example if a cable is unplugged), the inactive System Manager continues to appear in the login user list until 10 minutes have elapsed. **—end—**

Procedure 2-6
Changing your password

Use this procedure to change your account password for an Optical Metro 5100/5200 shelf. All local and centralized users have sufficient privilege to change their own password at any time.

In the case of local password change, system Manager sends all password changes to the primary shelf. The primary shelf updates and propagates passwords to the other shelves in the ring.

In the case of a centralized user password change the new password is propagated through RADIUS protocol.

> ***Note:*** Changing the centralized user's password through RADIUS protocol using System Manager is only supported with OMEA that has an embedded RADIUS server.

Precautions

CAUTION
Risk of incorrect backup file
Once password changes are made at the primary shelf, back up all affected shelves. Otherwise, the shelf could be restored from an out-of-date backup file in the event of shelf failure. See Procedure 1-36, "Backing up shelf configuration data" for details.

CAUTION
Risk of a System Manager shut down after password changes
Once a password is changed, a dialog box appears asking the user to shut down System Manager. Only the local user who is currently in the System Manager session that changed the password can ignore this request. All other users who are accessing System Manager remotely must shut down and restart System Manager after password changes.

—continued—

Procedure 2-6 (continued)
Changing your password

CAUTION
Risk of affecting the Emsmetro user
The Emsmetro account is used by the Optical Network Manager /OMEA to establish a network management session. The Emsmetro user has the same privileges and uses the same password as the Admin user. If you change the Admin password, your change also affects the Emsmetro user account.

Action

Step	Action
1	Log in to the System Manager. See Procedure 1-1, "Logging into the network" on page 1-7.
2	From the Security menu, select Change Password. *The Change Password dialog box appears.*
3	Enter your current password in the Old Password field.
4	Enter your new password in the New Password field. ***Note:*** The password is case sensitive and must be between eight and ten characters.
5	Enter your new password again in the Confirm Password field.
6	Click **OK**. *The Shut Down warning dialog box appears.*
7	**If** — **Then** you want to shut down immediately — click **Yes**. The System Manager shuts down. otherwise — click **No**

—end—

Procedure 2-7
Changing the community name

A Simple Network Management Protocol (SNMP) community is a logical relationship between an SNMP agent and one or more SNMP managers, such as the System Manager. The community has a name, and all members of a community have the same access privileges. The SNMP community prevents unauthorized managers from viewing or changing the configurations of SNMP manageable devices. If you have the Admin privilege, you can provision different community names for each user class.

Use this procedure to change the SNMP community name on a shelf.

Requirements

You must be an Admin level user to change the SNMP community name on the primary shelf.

Precautions

CAUTION
Risk of a System Manager session shut down
SNMP community name changes affect all users with the same access privileges as the user class that is being changed. All System Manager sessions with the same user class are shut down after the SNMP community name is changed.

CAUTION
Risk of incorrect backup file
After you change the SNMP community name on the primary shelf, back up the configuration data for all affected shelves. See Procedure 1-36, "Backing up shelf configuration data" for more information.

—continued—

Procedure 2-7 (continued)
Changing the community name

CAUTION
Risk of a System Manager shut down after SNMP community name changes
When SNMP community names are changed, a dialog box appears asking the user to shut down the System Manager. Only the local user who is currently in the System Manager session that changed the community name can ignore this request. All other users who are accessing System Manager remotely must shut down and restart System Manager after SNMP community name changes.

ATTENTION
SNMP community name changes during software upgrade and SP replacement
During a software upgrade or SP circuit pack replacement, when the primary shelf is upgraded to the current release and the other shelves are not, community name changes only allow all other shelves to do upgrades and surveillance (viewing alarms and events). If the community name is accidentally changed, the workaround is to change the primary shelf back to user class "admin" with the community name "admin".

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	From the Security menu, select Advanced. *The Change Community Name dialog box appears.* ***Note:*** The Advanced menu item is available only to Admin level users. It is grayed out for non-Admin level users.
3	In the User Class field, select the user class for which you want to change the community name.
4	In the New Community Name field, enter your new community name. ***Note:*** The community name is case sensitive and must be between one to eight characters. The following special characters are not allowed: ; : & ? , " and space.

—continued—

Procedure 2-7 (continued)
Changing the community name

Step	Action	
5	In the Confirm Community Name field, re-enter your new community name to confirm.	
6	Click the **OK** button. *The Confirm Community Name Change dialog appears.*	
7	Click the **Yes** button. *The Shut Down warning dialog box appears.*	
8	**If**	**Then**
	you want to shut down immediately	click **Yes**. The System Manager shuts down.
	otherwise	click **No**

—end—

Procedure 2-8
Setting the centralized security administration attributes

Use this procedure to set the

- authentication mode and the alternate login method for a shelf
- the primary and secondary security gateways

System Manager sends all changes to the centralized security administration attributes to the primary shelf. The primary shelf updates and propagates the changes to the other shelves in the ring.

If you change the security authentication mode (local/centralized) for the NE (relevant for all configurations—private or public IP configurations), do not make the change and then attempt to rediscover the NE using OMEA. The correct procedure is as follows: first delete the NE from OMEA and then make the change, and finally manage the NE again.

See *Optical Manager Element Adapter, Standard Operations Guide,* 450-3121-301, for procedures on deleting a network element and managing a network element.

Requirements

You must be an Admin level user to set the centralized security gateway attributes.

Precautions

CAUTION
Risk of incorrect backup file
Once the security administration provisioning is made, backup the database for all shelves in the network. Otherwise, the shelf could be restored from an out-of-date backup file in the event of shelf failure. See Procedure 1-36, "Backing up shelf configuration data" for details.

—continued—

Procedure 2-8 (continued)
Setting the centralized security administration attributes

CAUTION
Risk of login failure
If you are using a centralized security scheme, the network administrator must make sure that the Radius server IP address(es) and ports are correct and reachable. Also, the network administrator must make sure that the Radius shared secret provisioned on the Optical Metro 5100/5200 shelf exactly matches with the shared secret that is provisioned on the RADIUS server product. Otherwise, the user will not be able to login to the shelf.

CAUTION
Risk of login failure
If Challenge/Response is provisioned as the alternate method under the centralized security administration scheme, the network administrator must remember and make sure that the Challenge/Response shared secret is kept secure. Otherwise, the user will not be able to login to the shelf in the event that the RADIUS server(s) is not available.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	From the Security menu, select Authentication Provision. *The Authentication Provision dialog box appears.*
3	Select Centralized from the Authentication Mode drop-down list. Centralized authentication uses Remote Authentication Dial-In User Service (RADIUS). Local authentication uses either local accounts or local challenge-response.
4	Select an alternate login method for the shelf from the Alternate Login Method drop-down list. The system uses the alternate mehtod when centralized authentication is enabled but unavailable.

—continued—

Procedure 2-8 (continued)
Setting the centralized security administration attributes

Step	Action	
5	**If** the alternate authentication mode is	**Then** go to
	Challenge/Response	step 6
	Local User	step 10
6	Click on the Shared Secret for Challenge/Response button. *The Set Shared Secret for Challenge/Response dialog box appears.*	
7	Enter a shared secret in the Shared Secret field. The shared secret can be any alphanumeric string between 6 and 20 characters.	
8	Enter the shared secret again in the Confirm Shared Secret field.	
9	Click **OK**.	
10	Select the shelf IP address to use as the primary and secondary security gateways from the Primary Security Gateway and Secondary Security Gateway drop-down lists. ***Note:*** To deprovision the current primary or secondary gateway, select “not provisioned” from the Primary Security Gateway or Secondary Security Gateway drop-down list.	
11	Follow Procedure 2-9 “Setting intrusion attempts handling” to provision the Failed Login Attempt Threshold and Lockout Interval (Seconds).	
12	Follow Procedure 2-10 “Setting the primary or secondary RADIUS server attributes” to provision a primary and secondary RADIUS server for a RADIUS security gateway.	

—end—

Procedure 2-9
Setting intrusion attempts handling

Use this procedure to set the maximum number of failed login attempts before an intrusion is detected and an alarm is generated. Also use this procedure to set the duration of the lockout after an intrusion is detected.

Requirements

You must be an Admin level user to set the intrusion attempts handling.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	From the Security menu, select Authentication Provision. *The Authentication Provision dialog box appears.*
3	In the Login Control area, enter the maximum number of failed login attempts in the Failed Login Attempt Threshold field. ***Note:*** The Failed Login Attempt Threshold value can be between 2 and 20. The default is 5.
4	Enter a duration, in seconds, for the lockout interval in the Lockout Interval (Seconds) field. ***Note:*** The Lockout Interval value can be between 0 and 60. The default is 60.
5	Click **OK**.

—end—

Procedure 2-10
Setting the primary or secondary RADIUS server attributes

Use this procedure to provision a primary and secondary RADIUS server for a RADIUS security gateway.

> ***Note:*** Up to two RADIUS servers can be provisioned on each security gateway shelf.

For more information on the RADIUS server attributes, see Chapter 11 "Network security planning" in *Network Planning and Link Engineering*, 323-1701-110.

Requirements

You must be an Admin level user to set the primary or secondary RADIUS server.

Precautions

CAUTION
Risk of login failure
If you are using a centralized security scheme, the network administrator must make sure that the Radius server IP address(es) and ports are correct and reachable. Also, the network administrator must make sure that the Radius shared secret provisioned on the Optical Metro 5100/5200 shelf exactly matches with the shared secret that is provisioned on the RADIUS server product. Otherwise, the user cannot login to the shelf.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	From the Security menu, select Authentication Provision. *The Authentication Provision dialog box appears.*
3	In the Radius Servers area, double-click on a shelf IP for the primary or secondary security gateway. *The Radius Server Provision dialog box appears.*

—continued—

Procedure 2-10 (continued)
Setting the primary or secondary RADIUS server attributes

Step	Action
4	Enter the IP address of the RADIUS server in the Radius server IP Address field.
5	Enter the server port number in the RADIUS server Port field. ***Note:*** The default RADIUS server port is 1812.
6	Enter the timeout value (in seconds) for communication between the shelf and RADIUS server in the Timeout field. The default value is 10 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:*** The default timeout value is 10 seconds.
7	Enter a shared secret in the Shared Secret field. The shared secret can be any alphanumeric string between 6 and 20 characters. ***Note:*** The shared secret string must match the shared secret provisioned on the RADIUS server for this security gateway NE. A shared secret string that does not match results in a “RADIUS Server Unavailable” security alarm the next time a user tries to login.
8	Enter the shared secret again in the Confirm Shared Secret field.
9	Click **OK**.

—end—

Procedure 2-11
Changing the challenge/response shared secret for a shelf

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

Requirements

You must be an Admin level user to change the shared secret for a shelf.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	From the Security menu, select Authentication Provision. *The Authentication Provision dialog box appears.*
3	Click on the Shared Secret for Challenge/Response button. *The Shared Secret for Challenge/Response dialog box appears.*
4	Enter a shared secret in the Shared Secret field. The shared secret can be any alphanumeric string between 6 and 20 characters.
5	Enter the shared secret again in the Confirm Shared Secret field.
6	Click **OK**.

—end—

Procedure 2-12
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 when centralized authentication mode is enabled.

Requirements

You must be an Admin level user to change the shared secret for the primary or secondary RADIUS server.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	From the Security menu, select Authentication Provision. *The Authentication Provision dialog box appears.*
3	In the Radius Servers area, double-click on a shelf IP for the primary or secondary security gateway. *The Radius Server Provision dialog box appears.*
4	Enter a shared secret in the Shared Secret field. ***Note:*** The shared secret can be any alphanumeric string between 6 and 20 characters.
5	Enter the shared secret again in the Confirm Shared Secret field.
6	Click **OK**.

—end—

Procedure 2-13
Clearing security alarms

Use this procedure to clear security alarms. For more information on security alarms, refer to Chapter 23 "Clearing security alarms" in *Trouble Clearing and Alarm Reference Guide*, 323-1701-542.

Note: Only Admin level users can view security events and alarms.

Requirements

You must be an Admin level user to clear security alarms.

Action

Step	Action
1	Log in to the System Manager with your Admin user ID and password. See Procedure 1-1, "Logging into the network" on page 1-7.
2	From the Security menu, select Clear Security Alarm. *The Security Alarms dialog box appears and lists all the security alarms that are currently raised on the selected shelves.*
3	Highlight the alarm that you want to clear and click **Clear**.
4	Repeat step 3 until you have cleared all the alarms that you want to clear.
5	Click **Close**.

—end—

Nortel

Optical Metro 5100/5200 Multiservice Platform

Provisioning and Operating Procedures, Part 1 of 2

323-1701-310
Standard Release 8.0 Issue 1
April 2005
Printed in Canada and the United Kingdom

NORTEL