NTN465GF 323-1059-543

Nortel Networks

OPTera Metro 3500 Multiservice Platform

Alarm and Trouble Clearing—Part 1 of 2

Standard Release 12.0 Issue 1 November 2003

What's inside...

See Part 2 for the following...

NORTEL NETWORKS

Printed in Canada

Contents

Alarm clearing A-K 4-1

List of procedures

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 contain topics found in Part 1 only. The table of contents in Part 2 contain topics found in Part 2 only. Part 2 continues sequential chapter numbering from Part 1.

You are reading Part 1 of Nortel Networks *OPTera Metro 3500 Multiservice Platform Alarm and Trouble Clearing*, 323-1059-543.

Part 1 of *OPTera Metro 3500 Multiservice Platform Alarm and Trouble Clearing*, 323-1059-543 covers problem identification strategy and techniques, interpretation of LED and fault messages, problem resolution, procedures for active alarms, events, alarm provisioning, alarm profiles, network alarm management, external controls, and procedures for equipment replacement.

Part 2 of *OPTera Metro 3500 Alarm and Trouble Clearing*, 323-1059-543 continues covers problem identification strategy and techniques, fault isolation, problem resolution, and the detailed procedures for active alarms.

Standards

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

Supported software

This document supports the software release for OPTera Metro 3500 Release 12.0.

Supported hardware

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

Hardware naming conventions

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

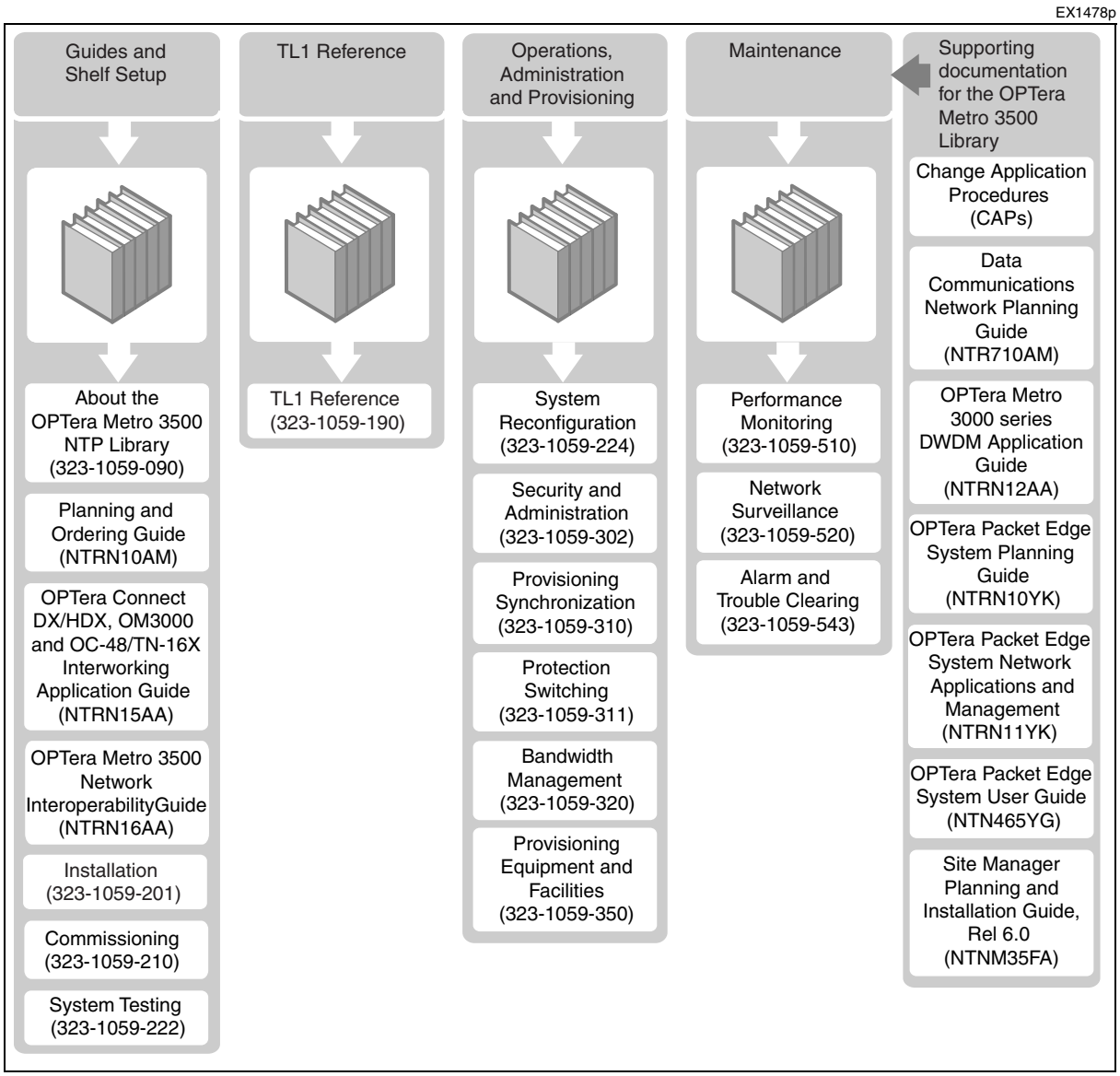
- The extended shelf processor (SPx) is referred to as the shelf processor.
- The extended network processor (NPx) is referred to as the network processor.

Audience

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

- planners
- provisioners
- network administrators
- transmission standards engineers

OPTera Metro 3500 NTP library



Technical support and information

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

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

Alarm and trouble clearing strategy

OPTera Metro 3500 hardware and software perform automatic fault detection and identification. When the network element detects faults, the network element issues autonomous alarms, activates office alarms, and displays alarms through light emitting diodes (LEDs).

The alarm clearing strategy is based on several assumptions:

- Protection circuitry exists.
- No external problem causes the alarm, such as power fluctuation.
- Primary fault generates primary and secondary alarms that you can clear with a single fault clearing procedure.
- Network element is provisioned correctly and works until the time of the alarm.

The network elements report alarms in the following ways:

- alarm LEDs on the network element and circuit packs
- autonomous alarm reports, through the TL1 interface
- network element alarm messages retrieved locally through Site Manager
- alarm messages retrieved remotely through the telemetry byte-oriented serial (TBOS) interface of Site Manager
- office alarms (optional)

The following steps make up the strategy for fault and alarm clearing:

- Detect that there is a fault.
- Identify the network element that raised the alarm.
- See if any FAIL indicator LEDs are illuminated on circuit packs.
- If a FAIL LED is illuminated, execute the procedure to replace a failed circuit pack or SFP module.
- If the FAIL LED is not illuminated, retrieve alarm messages and the trouble-clearing procedures through Site Manager.
- Identify local and remote alarms during the procedure.

- Identify alarm severity.
- Identify which network element to clear.
- Execute trouble-clearing procedures.
- Determine if there are additional alarms.
- If alarms continue to be active, begin the process again.
- If the alarms are cleared, then terminate.

Fault clearing strategy on page 1-3 shows the steps.

Alarm priority

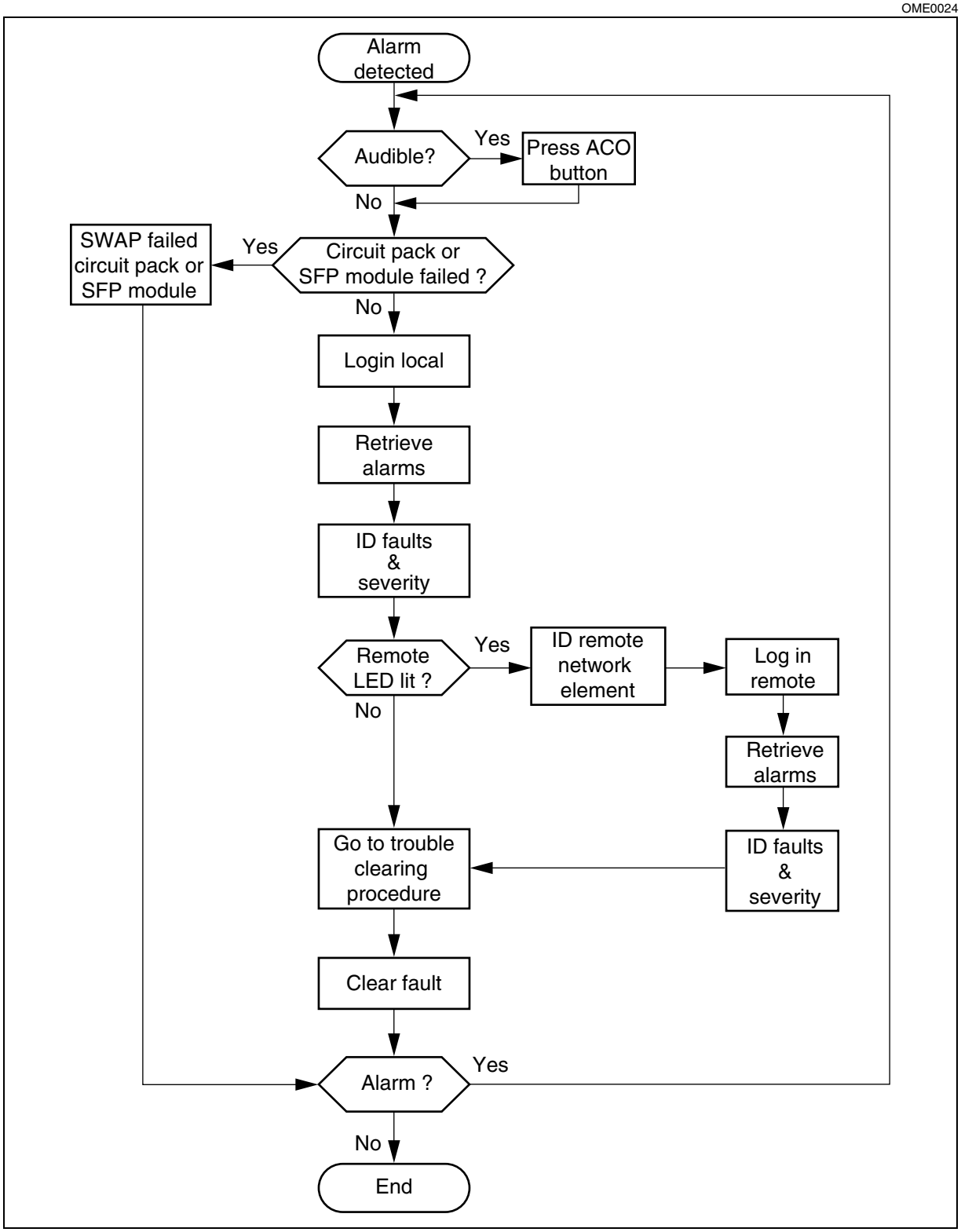
Clear alarms in order of severity:

- critical service-affecting (C SA) alarm
- failed circuit pack non-service-affecting (NSA) alarm
- major service-affecting (M SA) alarm
- major non-service-affecting (M NSA) alarm
- minor service-affecting (m SA) alarm
- minor non-service-affecting (m NSA) alarm

One fault can cause more than one alarm. Clear the alarm with the highest severity, and some other alarms often clear.

Figure 1-1
Fault clearing strategy

OME0024



Alarms

Procedures for active alarms

Procedures for events

Procedures for alarm provisioning

Procedures for alarm profiles

Procedures for network alarm monitoring and management

Procedures for external alarm provisioning

Procedures for external controls

Procedure 2-1
Retrieving active alarms for a network element

Use this procedure to retrieve the active alarms on a network element.

> ***Note:*** After you re-enable any alarm point that you disabled beyond the limit of 100, the alarm, if already active, will not appear in the Active Alarms window or in the Alarms on Disabled Points table in the Alarm Provisioning window until the condition that caused the alarm is cleared and then raised again.

Requirements

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation tree.
3	Select Active Alarms from the Faults drop-down menu. The Active Alarms window opens and displays the active alarms according to your last filter settings and the alarm points that are not disabled.

—end—

Procedure 2-2
Sorting active alarms for a network element

Use this procedure to sort the list of active alarms.

Step	Action
1	Retrieve the active alarms. See Retrieving active alarms for a network element on page 2-3. ***Note:*** When you first open the Active Alarms window, the columns are sorted from highest to lowest severity and then from most recent to oldest.
2	Click on a column header to sort the alarms by that column, in ascending order. ***Note:*** All columns are sorted in alphabetical order except the Date, Time column. The Date, Time column is sorted by date, then time.
3	After a short pause, click again on the same column header to sort the alarms in descending order.

—end—

Procedure 2-3
Filtering active alarms for a network element

Use this procedure to select the severities of active alarms to display. Active alarm severities are critical, major, minor, and warning.

Step	Action
1	Retrieve the active alarms. See Retrieving active alarms for a network element on page 2-3. ***Note 1:*** By default, the Active Alarms window displays active alarms of all severities. ***Note 2:*** If you return to the Active Alarms window during a session, the window displays the active alarms according to your previous filter settings.
2	To hide alarms of a specific severity from the Alarm List, uncheck the appropriate check box in the Show area. The Active Alarms window updates and no longer shows the alarms of that severity.
3	To display alarms filtered from the list, select the appropriate check box again in the Show area.

—end—

Procedure 2-4
Updating active alarms automatically

Use this procedure to set the Active Alarms window to automatically show new alarms or warnings when they become active.

Step	Action
1	Retrieve the active alarms. See Retrieving active alarms for a network element on page 2-3. ***Note:*** If the Auto refresh check box shows a check mark, the Active Alarms window automatically updates the alarm list. No action is necessary.
2	If the Auto refresh check box does not show a check mark, select the Auto refresh check box. ***Note:*** The Refresh button and the Last refresh field are no longer active.

—end—

Procedure 2-5
Updating active alarms manually

Use this procedure to update the Active Alarms window manually to show alarms or warnings that recently became active.

Step	Action
1	Retrieve the active alarms. See Retrieving active alarms for a network element on page 2-3. If the Auto refresh check box is not checked, go to step 3.
2	If the Auto refresh check box is checked, clear the check box to disable the auto refresh. ***Note:*** The Refresh button and the Last refresh field become active.
3	Click Refresh. The Last refresh field displays the time (hh:mm:ss) and date (Mmm-dd) of the most recent update of the Active Alarms window.

—end—

Procedure 2-6
Retrieving active alarm details

Use this procedure to retrieve detailed information about an active alarm.

Step	Action
1	Retrieve the active alarms. See Retrieving active alarms for a network element on page 2-3.
2	From the list of active alarms, click on the row for the alarm that you need to see in detail. The Alarm details area at the bottom of the Active Alarms window displays the details of the alarm. ***Note:*** You can view the details of only one alarm at a time.

—end—

Procedure 2-7
Printing active alarm details

Use this procedure to copy detailed information about active alarms to a text editor for printing.

Step	Action
1	Retrieve the details about an alarm. See Retrieving active alarms for a network element on page 2-3.
2	Highlight the alarm text from the Alarm details area.
3	Press Ctrl+C to copy the alarm text.
4	Paste the alarm text into a text editor according to the documentation for the text editor.
5	Print the alarm text according to the documentation for the text editor.

—end—

Procedure 2-8
Saving active alarm details

Use this procedure to copy detailed information about active alarms to a text editor for saving.

Step	Action
1	Retrieve the details about an alarm. See Retrieving active alarms for a network element on page 2-3.
2	Highlight the alarm text from the Alarm details area.
3	Press Ctrl+C to copy the alarm text.
4	Paste the alarm text into a text editor according to the documentation for the text editor.
5	Save the alarm text according to the documentation for the text editor.

—end—

Procedure 2-9
Retrieving events for a network element

Use this procedure to retrieve the event list for a network element.

Requirements

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation tree.
3	Select Events from the Faults drop-down menu. You can identify the events by looking for Log in the Severity column. Alerts have also the Log severity. ***Note:*** If you return to the Events window during a session, the window displays the events according to the previous filter settings. **—end—**

Procedure 2-10
Sorting events

Use this procedure to sort the Events List.

Step	Action
1	Retrieve the events. See Retrieving events for a network element on page 2-11. ***Note:*** When you first open the Events window, the columns are sorted from most recent to oldest.
2	Click on a column header to sort the events by that column, in ascending order. ***Note:*** All columns are sorted in alphabetical order except the Date, Time column. The Date, Time column is sorted by date and then time.
3	After a short pause, click again on the same column header to sort the alarms in descending order.

—end—

Procedure 2-11
Filtering events for a network element

Use this procedure to select the severities of events to display. Event severities are critical, major, minor, warning, cleared, and logged.

Step	Action
1	Retrieve the events. See Retrieving events for a network element on page 2-11. ***Note:*** If you return to the Events window during a session, the window displays the events according to your previous filter settings.
2	To hide events of a specific severity from the Event List, uncheck the appropriate check box in the Show area. The Event List window updates and no longer shows the events of that severity.
3	To display events filtered from the list, select the appropriate check box again in the Show area.

—end—

Procedure 2-12
Updating events window

Use this procedure to update the Events window manually to show events that recently became active.

Step	Action
1	Retrieve the events. See Retrieving events for a network element on page 2-11.
2	Click Refresh. The Last refresh field displays the time (hh:mm:ss) and date (mm-dd) of the most recent update of the Events window.

—end—

Procedure 2-13
Retrieving event details

Use this procedure to retrieve detailed information about an event.

For a list of autonomous events, see Autonomous events on page 2-19.

Step	Action
1	Retrieve the events. See Retrieving events for a network element on page 2-11.
2	From the Event List, click on the row for the event that you need to see in detail. The Event details area at the bottom of the Events window displays the details of the event. ***Note:*** You can view the details of only one event at a time.

—end—

Procedure 2-14
Printing event details

Use this procedure to copy detailed information about events to a text editor for printing.

Step	Action
1	Retrieve the details about an event. See Retrieving events for a network element on page 2-11.
2	Highlight the event text from the Event details area.
3	Press Ctrl+C to copy the event text.
4	Paste the event text into a text editor according to the documentation for the text editor.
5	Print the event text according to the documentation for the text editor.

—end—

Procedure 2-15
Saving event details

Use this procedure to copy detailed information about events to a text editor for saving.

Step	Action
1	Retrieve the details about an event. See Retrieving events for a network element on page 2-11.
2	Highlight the event text from the Event details area.
3	Press Ctrl+C to copy the event text.
4	Paste the event text into a text editor according to the documentation for the text editor.
5	Save the event text according to the documentation for the text editor.

—end—

Procedure 2-16
Allowing or inhibiting the display of Log, Inventory, and Database Change events

Use this procedure to allow or inhibit the display of Log, Inventory, and Database Change events. The display of Log and Inventory is disabled by default when you log in to a network element.

Requirements

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation tree.
3	Select the Faults drop-down menu. The Update on Data Changes menu option appears at the bottom of this menu. If a checkmark appears next to the Update on Data Changes option, then this option is enabled and the display of Log, Inventory, and Database Change events is allowed. If a checkmark does not appear next to the Update on Data Changes option, then this option is disabled and the display of Log, Inventory, and Database Change events is inhibited.
4	To change the status of Select Update on Data Changes menu option (to either enabled or disabled), select this option from the Faults drop-down menu.

—end—

Autonomous events

Autonomous events do not require action. Events report the activity status on the network elements. To retrieve events, see Retrieving events for a network element on page 2-11. The events listed in the Events window include the alarms that have been raised, both cleared or not cleared, and the logged alerts and events that do not require action.

Note: In Site Manager, the severity of alerts and events is Log.

Autonomous switch events

- Auto STS-1 Path Switch Complete
- Auto STS1 Path Switch Complete-EBER
- Auto STS1 Path Switch Complete-Sig. Deg.
- Auto STS1 Path Switch Complete-Sig. Fail
- Auto STS3C Path Switch Complete
- Auto STS3C Path Switch Complete-EBER
- Auto STS3C Path Switch Complete-Sig. Deg.
- Auto STS3C Path Switch Complete-Sig. Fail
- Auto STS12C Path Switch Complete
- Auto STS12C Path Switch Complete-EBER
- Auto STS12C Path Switch Complete-Sig. Deg.
- Auto STS12C Path Switch Complete-Sig. Fail
- Auto STS24C Path Switch Complete
- Auto STS24C Path Switch Complete-EBER
- Auto STS24C Path Switch Complete-Sig. Deg.
- Auto STS24C Path Switch Complete-Sig. Fail
- Auto STS48C Path Switch Complete
- Auto STS48C Path Switch Complete-EBER
- Auto STS48C Path Switch Complete-Sig. Deg.
- Auto STS48C Path Switch Complete-Sig. Fail
- Auto Switch Complete
- Auto Switch Complete-EBER
- Auto Switch Complete-EqpOOS
- Auto Switch Complete-EqptFail
- Auto Switch Complete-FacOOS
- Auto Switch Complete-Oscillation

- Auto Switch Complete-Protocol Mismatch
- Auto Switch Complete-Remote
- Auto Switch Complete-Signal Degrade
- Auto Switch Complete-Signal Fail
- Auto Switch Wait to Restore
- Auto Switch Wait-to-Restore-Remote
- Auto VT1.5 Path Switch Complete
- Auto VT1.5 Path Switch Complete-EBER
- Auto VT1.5 Path Switch Complete-Sig. Deg
- Auto VT1.5 Path Switch Complete-Sig Fail
- Wait to Restore
- Wait to Restore-Remote

BLSR configuration events

- BLSR audit fail: cannot connect to node in ring
- BLSR audit completed

FPGA events

- DO NOT restart/pull the card while download is running!
- Invoking FPGA Download, it should take approx 10 mins
- Otherwise your card will have to be replaced.
- The FPGA Download has Failed!
- The FPGA Download has finished successfully.
- Unable to communicate with the Transport Card!
- Unable to connect to a remote node (NP)!
- Unable to find the FPGA Load on the remote node (NP)!
- Verification step failed, retrying FPGA download again
- Verifying the FPGA load in flash memory...

Load installation events

- Blocked By Another Application
- Cancel Passed
- Check Failed
- Check Passed
- Commit Failed
- Commit Passed
- Committing New Release

- Downloading Release Load File
- Invoke Failed
- Invoke Passed
- Load Failed
- Load file checksum incorrect
- Load Passed
- Programming Load to FLASH
- Restoring Old Release
- Running from incorrect FLASH bank
- Unable to Access Release Files
- Unable to Program Load to FLASH
- Verifying load file checksum

OPTera Packet Edge events

- Authentication failure
- Cold restart
- Craft Enabled 1/1
- Craft Enabled 1/2
- Craft Enabled 1/3
- Craft Enabled 1/4
- Warm restart

Protection exerciser events

- Protection Exerciser Complete

Remote SID events

- Remote SID changed

Save and restore events

- A TL1 Command within the restored TL1 script has failed
- Cancel Save/Restore Completed
- Cancel Save/Restore Failed
- Cancel S/R Failed: Save and Restore not in progress
- Check S/R Failed: Blocked by presence of alarms
- Check S/R Failed: Could not connect to destination
- Check S/R Failed: Invalid destination
- Check Save/Restore Completed
- Check Save/Restore Failed

- Check S/R Failed: Blocked by another application
- Database Commit Failed
- Database Commit Failed: Blocked by another application
- Database Commit Failed: Blocked by presence of alarms
- Database Commit Failed: Restored backup is corrupt
- Database Rebuilt For Slot
- Database Restore Completed
- Database Restore Failed
- Database Restore Failed: Backup not from this node
- Database Restore Failed: Blocked by another application
- Database Restore Failed: Blocked by presence of alarms
- Database Restore Failed: Could not connect to source
- Database Restore Failed: Failure transferring file
- Database Restore Failed: Interrupted by card restart
- Database Restore Failed: Invalid source
- Database Restore Failed: Mismatched Software Releases
- Database Restore Failed: Restored backup is corrupt
- Database Save completed
- Database Save Failed
- Database Save Failed: Blocked by another application
- Database Save Failed: Blocked by presence of alarms
- Database Save Failed: Could not connect to destination
- Database Save Failed: Failure transferring file
- Database Save Failed: Interrupted by card restart
- Database Save Failed: Invalid destination
- Database Save in Progress
- Database Validate Failed
- Database Validate Failed: Restored backup is corrupt
- NE Provisioning Script file Commit Failed
- NE Provisioning Script file Commit Passed
- NE Provisioning Script file Load - Cancel Completed
- NE Provisioning Script file Load - Cancel Failed: Load Not in Progress
- NE Provisioning Script file Load Completed
- NE Provisioning Script file Load Failed

- NE Provisioning Script file Load Failed: Action interrupted by card restart
- NE Provisioning Script file Load In Progress
- Retrieving TL1SCRPT file <filename>
- SP Cancel Database S/R Completed
- SP Cancel Database S/R Failed: S/R not in progress
- SP Check S/R Completed
- SP Check S/R Failed
- SP Database Commit Completed
- SP Database Commit Failed
- SP Database Restore Completed
- SP Database Restore Failed
- SP Database Restore Failed: Action interrupted by card restart
- SP Database Restore in progress
- SP Database Save Completed
- SP Database Save Failed
- SP Database Save Failed: Action interrupted by card restart
- SP Database Save in progress

Security events

- Password will expire today
- Password will expire in <n> days

  Note: Value of n can be between 1 and 14 days.

- Password has expired. Contact your Admin
- Password has expired. Change it now
- Password file reset to defaults

Span of control events

- SOC Database Save Failed: Interrupted by card restart
- SOC Database Save Completed
- SOC Database Save Failed
- SOC Database Save in Progress
- SOC Check S/R Completed
- SOC Check S/R Failed
- SOC Cancel S/C Completed
- SOC Cancel S/C Failed: Save and Check not in progress

Test access events

- VT1.5 Path Test Access in Progress - Monitor
- STS1 Path Test Access in Progress - Monitor
- STS3c Path Test Access in Progress - Monitor
- STS12c Path Test Access in Progress - Monitor
- STS24c Path Test Access in Progress - Monitor
- STS48c Path Test Access in Progress - Monitor
- VT1.5 Path Test Access in Progress - Split
- STS1 Path Test Access in Progress - Split
- STS3c Path Test Access in Progress - Split
- STS12c Path Test Access in Progress - Split
- STS24c Path Test Access in Progress - Split
- STS48c Path Test Access in Progress - Split

Test signal events

- DS1 Idle Code Detected
- DS1 Test Signal Active-Error Received
- DS1 Test Signal Active-OutofSync

Timing and synchronization events

- BITSout-A Pri Ref Rx Degraded SSM
- BITSout-A Sec Ref Rx Degraded SSM
- BITSout-B Pri Ref Rx Degraded SSM
- BITSout-B Sec Ref Rx Degraded SSM
- Shelf Pri Ref Rx Degraded SSM
- Shelf Sec Ref Rx Degraded SSM
- Sync Reference Status Change
- Sync Reference Switch Completed
- Timing Generation Entry to Freerun
- Timing Generation Entry to Holdover

Upgrade events

- Upgrade in Progress

Procedure 2-17
Retrieving alarm points status based on alarm class

Use this procedure to retrieve information about alarms that have been enabled or disabled, based on the alarm class.

The alarm class filters the potential large list of alarm points.

Note 1: Alarm provisioning only affects alarm notification and has no effect on the alarm function.

Note 2: The SECU alarm class is not provisionable. You cannot enable or disable the alarm points on either of the two security alarms.

Requirements

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation tree.
3	Select Alarm Provisioning from the Configuration drop-down menu.
4	Select the Retrieve by Alarm Class tab.
5	Select the alarm class from the Alarm Class drop-down list. ***Note:*** The Alarm Class table in the center of the Alarm Provisioning window displays all the alarm points related to the selected class.
6	Select one or more alarm points from the Alarm Class table. ***Note 1:*** To select multiple alarm points, hold down the Shift or Ctrl key when you select the alarm points. ***Note 2:*** Depending on the alarm class and alarm points you select, the Type, Slot, WAN, Port, STS, VTG, and VT drop-down lists become available as necessary.
7	Select from the available Type, Slot, WAN, Port, STS, VTG, and VT drop-down lists.
8	Click Retrieve. The Alarm Status list at the bottom of the Alarm Provisioning window displays the status of the selected alarm points and the selected unit.

—end—

Procedure 2-18
Retrieving alarm points status based on equipment type

Use this procedure to retrieve information about alarms that have been enabled or disabled, based on the equipment type.

The equipment type filters the potential large list of alarm points.

Requirements

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation tree.
3	Select Alarm Provisioning from the Configuration drop-down menu.
4	Select the Retrieve by Equipment Type tab.
5	Select the equipment type from the Type drop-down list.
6	Select the slot number from the Slot drop-down list. ***Note:*** If the Slot drop-down list is not available or is disabled, go to the next step.
7	Select the port number from the Port drop-down list. ***Note:*** If the Port drop-down list is not available, go to the next step.
8	Select one or more alarm classes from the Alarm Class drop-down list. ***Note:*** To select multiple alarm classes, hold down the Shift or Ctrl key when you select the alarm classes.
9	Click Show. The Alarm Class table in the center of the Alarm Provisioning window displays all the alarm points related to the provisioned data.
10	Select one or more alarm points from the Alarm Class table. ***Note:*** To select multiple alarm points, hold down the Shift or Ctrl key when you select the alarm points.
11	Click Retrieve. The Alarm Status list at the bottom of the Alarm Provisioning window displays the status of the selected alarm points.

—end—

Procedure 2-19
Retrieving active alarms raised against disabled alarm points

Use this procedure to retrieve information about the active alarms raised against disabled alarm points.

> ***Note:*** After you re-enable any alarm point that you disabled beyond the limit of 100, the alarm, if already active, will not appear in the Active Alarms window or in the Alarms on Disabled Points table in the Alarm Provisioning window until the condition that caused the alarm is cleared and then raised again.

Requirements

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation tree.
3	Select Alarm Provisioning from the Configuration drop-down menu.
4	Select the Alarms on Disabled Points tab to display a list of all the active alarms raised against disabled alarm points.
5	Select the alarm that you need to see in detail from the Alarm List.

—end—

Procedure 2-20
Disabling alarm points

CAUTION
Risk of unidentified problem conditions
Disabling an alarm point prevents alarm notification if a fault occurs.

Use this procedure to disable alarm notification for selected alarm points.

Note 1: Alarm provisioning only affects alarm notification and has no effect on the alarm function.

Note 2: The SECU alarm class is not provisionable. You cannot enable or disable the alarm points on either of the two security alarms.

Note 3: You cannot modify the alarm provisioning of STS-1, STS-3c, STS-12c, and VT path alarms of protection channels 25-48 for non-RPR traffic in a BLSR. Provision STS-1, STS-3c, STS-12c, and VT path alarms for channels 25-48 as required prior to the reconfiguration to BLSR.

Note 4: Do not disable more than 100 alarm points. After you re-enable any alarm point that you disabled beyond the limit of 100, the alarm, if already active, will not appear in the Active Alarms window or in the Alarms on Disabled Points table in the Alarm Provisioning window until the condition that caused the alarm is cleared and then raised again.

Requirements

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

Step	Action
1	Retrieve the alarm points status. See Retrieving alarm points status based on alarm class on page 2-25 or Retrieving alarm points status based on equipment type on page 2-26.
2	Select one or more of the enabled alarms from the Alarm Status list at the bottom of the Alarm Provisioning window. ***Note:*** To select multiple alarms, hold down the Shift or Ctrl key when you select the alarms.
3	Click Disable.

—end—

Procedure 2-21
Enabling alarm points

Use this procedure to enable alarm notification for selected alarm points.

Note 1: Alarm provisioning only affects alarm notification and has no effect on the alarm function.

Note 2: The SECU alarm class is not provisionable. You cannot enable or disable the alarm points on either of the two security alarms.

Note 3: You cannot modify the alarm provisioning of STS-1, STS-3c, STS-12c, and VT path alarms of protection channels 25-48 for non-RPR traffic in a BLSR. Provision STS-1, STS-3c, STS-12c, and VT path alarms for channels 25-48 as required prior to the reconfiguration to BLSR.

Note 4: After you re-enable any alarm point that you disabled beyond the limit of 100, the alarm, if already active, will not appear in the Active Alarms window or in the Alarms on Disabled Points table in the Alarm Provisioning window until the condition that caused the alarm is cleared and then raised again.

Requirements

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

Step	Action
1	Retrieve alarm points status. See Retrieving alarm points status based on alarm class on page 2-25, or Retrieving alarm points status based on equipment type on page 2-26.
2	Select one or more of the disabled alarms from the Alarm Status list at the bottom of the Alarm Provisioning window. ***Note:*** To select multiple alarms, hold down the Shift or Ctrl key when you select the alarms.
3	Click Enable.

—end—

Procedure 2-22
Retrieving alarm profiles by alarm class

Use this procedure to retrieve information about alarm profiles using the alarm class to filter the alarm profiles.

> ***Note:*** The SECU alarm class is not provisionable. You cannot enable or disable the alarm points on either of the two security alarms.

Requirements

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation tree.
3	Select Alarm Profiles from the Configuration drop-down menu.
4	Ensure that All is selected in the Type drop-down list.
5	Select an alarm class from the Alarm Class drop-down list. The Profiles table in the center of the Alarm Profiles window displays the available alarm profiles for the selected alarm class.

—end—

Procedure 2-23
Retrieving alarm profiles by equipment or facility type

Use this procedure to retrieve information about alarm profiles by using the equipment or facility type and then the alarm class to filter the alarm profiles.

Requirements

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation tree.
3	Select Alarm Profiles from the Configuration drop-down menu.
4	Ensure that there is no selection in the Alarm Class drop-down list.
5	Select an equipment or facility type from the Type drop-down list. ***Note:*** Depending on the type you select, the Slot, Port, STS, VT Group, VT Number, T1, and T3 drop-down lists become available.
6	Select from the Slot, Port, STS, VT Group, VT Number, T1, and T3 drop-down lists that are available.
7	Select an alarm class from the Alarm Class drop-down list, if applicable. The Profiles table in the center of the Alarm Profiles window displays the available alarm profiles for the provisioned data.

—end—

Procedure 2-24
Retrieving details of an alarm profile

Use this procedure to retrieve information about an alarm profile.

Step	Action
1	Retrieve the alarm profiles of the network element. See Retrieving alarm profiles by alarm class on page 2-30, and Retrieving alarm profiles by equipment or facility type on page 2-31.
2	Select a profile from the Profiles table in the center of the Alarm Profiles window. The Profile details table at the bottom of the window displays all the alarm points applicable to the selected profile, and their status.

—end—

Procedure 2-25
Adding a new alarm profile

CAUTION
Risk of unidentified problem conditions
Disabling an alarm point prevents alarm notification if a fault occurs.

Use this procedure to add a new alarm profile to the list of available profiles.

Note 1: Alarm provisioning only affects alarm notification and has no effect on the alarm function.

Note 2: The SECU alarm class is not provisionable. You cannot enable or disable the alarm points on either of the two security alarms.

Note 3: You cannot modify the alarm provisioning of STS-1, STS-3c, STS-12c, and VT path alarms of protection channels 25-48 for non-RPR traffic in a BLSR. Provision STS-1, STS-3c, STS-12c, and VT path alarms for channels 25-48 as required prior to the reconfiguration to BLSR.

Note 4: Do not disable more than 100 alarm points. After you re-enable any alarm point that you disabled beyond the limit of 100, the alarm, if already active, will not appear in the Active Alarms window or in the Alarms on Disabled Points table in the Alarm Provisioning window until the condition that caused the alarm is cleared and then raised again.

Requirements

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

Step	Action
1	Retrieve the alarm profiles of the network element. See Retrieving alarm profiles by alarm class on page 2-30. ***Note:*** The Add button in the center of the Alarm Profiles window is enabled when less than five profiles exist for this alarm class.
2	Click Add. ***Note:*** The dialog box contains the Profile details table of the selected alarm class. Enabled is the default value for all the alarm points.
3	Enter the new profile name. ***Note:*** The profile name must contain 20 characters or less, and must not contain quotation marks (“) or backslashes (\).

—continued—

Procedure 2-25 (continued)
Adding a new alarm profile

Step	Action
4	Select one or more alarm points that you want to disable. ***Note:*** To select multiple alarm points, hold down the Shift or Ctrl key when you select the alarm points.
5	Click Disable.
6	Click OK.

—end—

Procedure 2-26
Editing an alarm profile

CAUTION
Risk of unidentified problem conditions
Disabling an alarm point prevents alarm notification if a fault occurs.

Use this procedure to edit an existing alarm profile.

Note 1: Alarm provisioning only affects alarm notification and has no effect on the alarm function.

Note 2: The SECU alarm class is not provisionable. You cannot enable or disable the alarm points on either of the two security alarms.

Note 3: You cannot modify the alarm provisioning of STS-1, STS-3c, STS-12c, and VT path alarms of protection channels 25-48 for non-RPR traffic in a BLSR. Provision STS-1, STS-3c, STS-12c, and VT path alarms for channels 25-48 as required prior to the reconfiguration to BLSR.

Note 4: Do not disable more than 100 alarm points. After you re-enable any alarm point that you disabled beyond the limit of 100, the alarm, if already active, will not appear in the Active Alarms window or in the Alarms on Disabled Points table in the Alarm Provisioning window until the condition that caused the alarm is cleared and then raised again.

Requirements

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

Step	Action
1	Retrieve the alarm profiles of the network element. See Retrieving alarm profiles by alarm class on page 2-30.
2	Select the profile to edit. ***Note 1:*** You cannot edit the All Alarms ON and All Alarms OFF profiles that the system has defined. ***Note 2:*** You cannot edit an alarm profile that is set as active.
3	Click Edit. The dialog box contains the Profile details table of the selected profile.
4	Select one or more alarm points that you want to enable or disable. ***Note:*** To select multiple alarm points, hold down the Shift or Ctrl key when you select the alarm points.

—continued—

Procedure 2-26 (continued)
Editing an alarm profile

Step	Action
5	Click Enable or Disable as applicable.
6	Repeat step 4 and step 5 until you have finished editing all the alarm points.
7	Click OK. The edited alarm point status is displayed in the Alarm Profiles window under Alarm Point.

—end—

Procedure 2-27
Deleting an alarm profile

Use this procedure to delete an existing alarm profile.

Note 1: Alarm provisioning only affects alarm notification and has no effect on the alarm function.

Note 2: The SECU alarm class is not provisionable. You cannot enable or disable the alarm points on either of the two security alarms.

Note 3: You cannot modify the alarm provisioning of STS-1, STS-3c, STS-12c, and VT path alarms of protection channels 25-48 for non-RPR traffic in a BLSR. Provision STS-1, STS-3c, STS-12c, and VT path alarms for channels 25-48 as required prior to the reconfiguration to BLSR.

Requirements

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

Step	Action
1	Retrieve the alarm profiles of the network element. See Retrieving alarm profiles by alarm class on page 2-30 or Retrieving alarm profiles by equipment or facility type on page 2-31.
2	Select the profile to delete. ***Note:*** You cannot delete the All Alarms ON and All Alarms OFF profiles that the system has defined, and the profiles set as default, set as active or both.
3	Click Delete.
4	Click Yes in the confirmation dialog box.

—end—

Procedure 2-28
Setting a default profile

CAUTION
Risk of unidentified problem conditions
Disabling an alarm point prevents alarm notification if a fault occurs.

Use this procedure to set the alarm profile of an alarm class as the default profile.

Note 1: Alarm provisioning only affects alarm notification and has no affect on the alarm function.

Note 2: You cannot modify the alarm provisioning of STS-1, STS-3c, STS-12c, and VT path alarms of protection channels 25-48 for non-RPR traffic in a BLSR. Provision STS-1, STS-3c, STS-12c, and VT path alarms for channels 25-48 as required prior to the reconfiguration to BLSR.

Note 3: Do not disable more than 100 alarm points. After you re-enable any alarm point that you disabled beyond the limit of 100, the alarm, if already active, will not appear in the Active Alarms window or in the Alarms on Disabled Points table in the Alarm Provisioning window until the condition that caused the alarm is cleared and then raised again.

Requirements

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

Step	Action
1	Retrieve the alarm profiles of the network element by alarm class. See Retrieving alarm profiles by alarm class on page 2-30 or Retrieving alarm profiles by equipment or facility type on page 2-31.
2	Select a profile from the Profiles table in the center of the Alarm Profiles window.
3	Click Set as Default. The word Default is displayed in the Alarm Class Default column on the row of the selected profile.

—end—

Procedure 2-29
Setting a profile as active for a specific unit of equipment or facility

CAUTION
Risk of unidentified problem conditions
Disabling an alarm point prevents alarm notification if a fault occurs.

Use this procedure to set the alarm profile of a specific unit of equipment or facility as the active profile.

Note 1: Alarm provisioning only affects alarm notification and has no affect on the alarm function.

Note 2: You cannot modify the alarm provisioning of STS-1, STS-3c, STS-12c, and VT path alarms of protection channels 25-48 for non-RPR traffic in a BLSR. Provision STS-1, STS-3c, STS-12c, and VT path alarms for channels 25-48 as required prior to the reconfiguration to BLSR.

Note 3: Do not disable more than 100 alarm points. After you re-enable any alarm point that you disabled beyond the limit of 100, the alarm, if already active, will not appear in the Active Alarms window or in the Alarms on Disabled Points table in the Alarm Provisioning window until the condition that caused the alarm is cleared and then raised again.

Requirements

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

Step	Action
1	Retrieve the alarm profiles of the network element by equipment. See Retrieving alarm profiles by equipment or facility type on page 2-31.
2	Select a profile from the Profiles table in the center of the Alarm Profiles window.
3	Click Set as Active. The word Active is displayed in the Active For Unit column on the row of the selected profile.

—end—

Procedure 2-30
Setting a profile as active for the Common or Facility alarm class

CAUTION
Risk of unidentified problem conditions
Disabling an alarm point prevents alarm notification if a fault occurs.

Use this procedure to set the profile for the Common or Facility alarm class as the active profile.

Note 1: Alarm provisioning only affects alarm notification and has no affect on the alarm function.

Note 2: You cannot modify the alarm provisioning of STS-1, STS-3c, STS-12c, and VT path alarms of protection channels 25-48 for non-RPR traffic in a BLSR. Provision STS-1, STS-3c, STS-12c, and VT path alarms for channels 25-48 as required prior to the reconfiguration to BLSR.

Note 3: Do not disable more than 100 alarm points. After you re-enable any alarm point that you disabled beyond the limit of 100, the alarm, if already active, will not appear in the Active Alarms window or in the Alarms on Disabled Points table in the Alarm Provisioning window until the condition that caused the alarm is cleared and then raised again.

Requirements

To perform this procedure, you must:

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation tree.
3	Select Alarm Profiles from the Configuration drop-down menu.
4	Ensure that All is selected in the Type drop-down list.
5	Select either Common or Facility from the Alarm Class drop-down list as required. The Profiles table in the center of the Alarm Profiles window displays the available alarm profiles for the selected alarm class.

—continued—

Procedure 2-30 (continued)
Setting a profile as active for the Common or Facility alarm class

Step	Action
6	Select a profile from the Profiles table.
7	Click Set as Active. The word Active is displayed in the Active For Unit column on the row of the selected profile.

—end—

Procedure 2-31
Setting a profile as active by alarm class for a particular equipment or facility

Use this procedure to set the alarm profile of an alarm class for a specific unit of equipment or facility as the active profile.

Note 1: Alarm provisioning only affects alarm notification and has no affect on the alarm function.

Note 2: You cannot modify the alarm provisioning of STS-1, STS-3c, STS-12c, and VT path alarms of protection channels 25-48 for non-RPR traffic in a BLSR. Provision STS-1, STS-3c, STS-12c, and VT path alarms for channels 25-48 as required prior to the reconfiguration to BLSR.

Note 3: Do not disable more than 100 alarm points. After you re-enable any alarm point that you disabled beyond the limit of 100, the alarm, if already active, will not appear in the Active Alarms window or in the Alarms on Disabled Points table in the Alarm Provisioning window until the condition that caused the alarm is cleared and then raised again.

Requirements

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

Step	Action
1	Retrieve the alarm profiles of the network element by alarm class. See Retrieving alarm profiles by alarm class on page 2-30.
2	Select an equipment type from the Type drop-down list. ***Note:*** Depending on the type that you select, the Slot, Port, VT Group, and VT Number drop-down lists become available.
3	Select from the Slot, Port, VT Group, and VT Number drop-down lists that are available. The Profiles table displays the available alarm profiles for the selected alarm class and selected equipment or facility instance.
4	Select a profile from the Profiles table.
5	Click Set as Active. The word Active is displayed in the Active For Unit column on the row of the selected profile.

—end—

Procedure 2-32
Using profiles to disable all alarms on a specific unit of equipment or facility

CAUTION
Risk of unidentified problem conditions
Disabling an alarm point prevents alarm notification if a fault occurs.

Use this procedure to disable all alarms on a specific unit of equipment or facility.

Note 1: Alarm provisioning only affects alarm notification and has no effect on the alarm function.

Note 2: The SECU alarm class is not provisionable. You cannot enable or disable the alarm points on either of the two security alarms.

Note 3: You cannot modify the alarm provisioning of STS-1, STS-3c, STS-12c, and VT path alarms of protection channels 25-48 for non-RPR traffic in a BLSR. Provision STS-1, STS-3c, STS-12c, and VT path alarms for channels 25-48 as required prior to the reconfiguration to BLSR.

Note 4: Do not disable more than 100 alarm points. After you re-enable any alarm point that you disabled beyond the limit of 100, the alarm, if already active, will not appear in the Active Alarms window or in the Alarms on Disabled Points table in the Alarm Provisioning window until the condition that caused the alarm is cleared and then raised again.

Requirements

To perform this procedure, you must:

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation tree.
3	Select Alarm Profiles from the Configuration drop-down menu.
4	Ensure that there is no selection in the Alarm Class drop-down list.

—continued—

Procedure 2-32 (continued)
Using profiles to disable all alarms on a specific unit of equipment or facility

Step	Action
5	Select an equipment type from the Type drop-down list. ***Note:*** Depending on the type that you select, the Slot, Port, VT Group, and VT Number drop-down lists become available.
6	Select from the Slot, Port, VT Group, and VT Number drop-down lists that are available.
7	Select any alarm class from the Alarm Class drop-down list, if available. ***Note:*** The Profiles table in the center of the Alarm Profiles window displays the available alarm profiles for the provisioned data.
8	Select the All Alarms OFF profile from the Profiles table.
9	Click Set as Active.
10	Repeat step 7 through step 9 for all alarm classes of the Alarm Class drop-down list. ***Note:*** All alarms against the selected unit of equipment or facility are disabled.

—end—

Procedure 2-33
Restarting a circuit pack

CAUTION
Risk of traffic loss
A cold restart on an unprotected circuit pack causes a traffic loss.

Use this procedure to initialize a circuit pack in a warm restart or cold restart mode.

Note 1: A cold restart can affect traffic. To prevent traffic loss, switch traffic to the standby circuit pack before performing a cold restart on an active circuit pack.

Note 2: The DS1 mapper cannot be restarted.

Note 3: The DSM DS1x84 termination module (TM) mapper can be restarted.

Note 4: A warm restart of the OC-3x4 circuit pack causes an SDCC link failure alarm. The SDCC link failure alarm will clear automatically.

Note 5: If you perform a warm or cold restart on an OC-3 or OC-3x4 circuit pack that is hosting a DSM DS1x84 TM circuit pack, you will lose the SDCC link to the DSM DS1x84 TM. The SDCC link is re-established automatically.

Requirements

To perform this procedure, you must:

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation tree.
3	Select Restart from the Faults drop-down menu.
4	Select the circuit pack you want to restart from the Card drop-down list.
5	Select the restart type from the Restart type drop-down list.

—continued—

Procedure 2-33 (continued)
Restarting a circuit pack

Step	Action
6	Click OK.
7	Click Yes in the confirmation dialog box. ***Note:*** The confirmation dialog box appears only if you selected the cold restart type.

—end—

Procedure 2-34
Restarting the shelf processor

Use this procedure to initialize the shelf processor in a warm restart or cold restart mode.

Note 1: After a shelf processor is restarted, the Duplicate SID alarm is masked for 20 minutes.

Note 2: A loss of connectivity to the shelf processor occurs when you restart the shelf processor. You must wait five minutes before logging back in.

Note 3: A warm or cold restart of the shelf processor causes the SDCC link failure alarm on the adjacent network elements. The SDCC link failure alarm will clear automatically.

Note 4: The date and time must be reset on the network element and network processor after restarting the shelf processor. See 323-1059-302, Changing the network element or network processor date, time, and time zone on page 3-40.

Note 5: After a shelf processor restart or a time change, the protection exerciser will resume its schedule on the next calendar day at the provisioned start time. Also, if you provisioned the number of times the exerciser runs, this counter is restarted when the exerciser resumes the next day.

Requirements

To perform this procedure, you must:

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

ATTENTION

Do not perform a warm restart of the SPx if a protection switch condition exists on a 1+1 protected circuit pack. The *Auto-Switch Complete - Signal Fail* alarm will no longer appear but the conditions causing the alarm are still in place.

—continued—

Procedure 2-34 (continued)
Restarting the shelf processor

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation tree.
3	Select Restart from the Faults drop-down menu.
4	Select the shelf processor from the Card drop-down list.
5	Select the restart type from the Restart type drop-down list.
6	Click OK.
7	Click Yes in the confirmation dialog box.

—end—

Procedure 2-35
Restarting the network processor

Use this procedure to initialize the network processor in a warm restart or cold restart mode.

Note 1: A loss of connectivity to the network processor occurs when you restart the network processor. You must wait 5 minutes before logging back in.

Note 2: The date and time must be reset on the network element and network processor after a system restart. See 323-1059-302, Changing the network element or network processor date, time, and time zone on page 3-40.

Requirements

To perform this procedure, you must:

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

Step	Action
1	Ensure you are logged in to the network processor. See 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Select the network processor in the navigation tree.
3	Select Restart from the Faults drop-down menu.
4	Select the restart type from the Restart type drop-down list.
5	Click OK.
6	Click Yes in the confirmation dialog box.

—end—

Procedure 2-36
Retrieving active alarms from the Shelf Level View window

Use this procedure to retrieve the following alarms from the Shelf Level View window:

- alarms raised against a circuit pack
- common equipment alarms
- environmental alarms
- facility alarms

The Shelf Level View window displays circuit packs with a colored border if alarms are raised against them.

The squares that appear to the right of the graphical representation indicate alarms that are raised against non-circuit pack items, such as common equipment, environment, and facility. The squares appear only if the alarms are raised.

Requirements

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation tree.
3	Select Shelf Level View from the Configuration drop-down menu.
4	Right-click on the circuit pack with a colored border, and select Show Alarms from the pop-up menu.
5	Repeat step 4 to retrieve alarms for other circuit packs with a colored border.
6	Right click on the square that may appear to the right of the graphical representation, and select Show Alarms from the pop-up menu.
7	Repeat step 6 for other squares that may appear.

—end—

Procedure 2-37
Identifying faults

Use this procedure to detect alarms, retrieve the alarm message from the network element or network processor, and identify the fault clearing procedure.

Alarms are detected as follows:

- audible office alarms
- visual office alarms
- alarm LEDs on the network element, DS1 service module (DSM), and circuit packs
- autonomous alarm reports, through the TL1 interface
- network element alarm messages retrieved locally
- alarm messages retrieved remotely through the telemetry byte-oriented serial (TBOS) interface

Requirements

To perform this procedure, you must

- understand the LEDs on the network element, DSM, and circuit packs
- ensure that TBOS mapping is set up according to the instructions in 323-1059-520, Procedures for TBOS on page 1-1
- locate the network element or DSM that raised the alarm

Step	Action
1	Clear audible alarms. See Clearing audible alarms and performing lamp tests on page 2-53.
2	If the network element or DSM that raises the alarm is local, identify any illuminated LEDs that indicate circuit pack failure.
3	Replace all failed circuit packs. Use the appropriate circuit pack replacement procedure. See Procedures for equipment replacement on page 3-1.
4	If additional alarm LEDs are illuminated on the network element, select TBOS from the Faults drop-down menu of Site Manager.
5	Identify the network element with the highest priority alarm.
6	Log in to the network element with the highest priority alarm, and execute the appropriate trouble clearing procedure. See Detailed procedures for active alarms on page 4-1.
7	Repeat step 4 through step 6 to clear other alarms.

—end—

Procedure 2-38
Identifying the circuit pack or facility that has raised an alarm

Use this procedure to identify the circuit pack or facility that has raised an alarm.

Step	Action
1	Retrieve the active alarms on the network element. See Retrieving active alarms for a network element on page 2-3.
2	Identify the alarm in the Alarm List. The Unit column identifies the equipment or facility that raises the alarm. For example, OC3-10-1 refers to an alarm raised by port 1 of the OC-3 optical interface circuit pack in slot 10.
3	To view details of an alarm, select the alarm in the Alarm List. The Alarm details area at the bottom of the Active Alarms window displays the details of the alarm.

—end—

Procedure 2-39
Clearing audible alarms and performing lamp tests

Use this procedure to clear audible alarms and perform lamp tests on network elements and DS1 service modules (DSM). The network element and DSM have relay contacts that you can connect to both visual and audible alarms.

There are four contact pairs for a network element and four contact pairs for a DSM. Therefore, you can connect critical, major, minor, and remote alarms to separate audible alarms for a network element or a DSM.

> ***Note:*** When you clear an audible alarm the alarmed LEDs and fault are not cleared.

Requirements

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

Step	Action

Clearing audible alarms manually

1 Locate the network element or DSM with the audible alarm.

- Press the ACO button on the left interface (LIF) once to reset the audible alarm relays for the network element including all the connected DSMs.

  Note 1: See Alarm cutoff button on the LIF and on the DS1 service module on page 2-55.

  Note 2: If you press the ACO button twice on the LIF, you will turn off the audible alarm and perform a lamp test on the network element including all the connected DSMs.

- Press the ACO button on the DSM once to reset the audible alarm relays for the DSM.

  Note 1: See Alarm cutoff button on the LIF and on the DS1 service module on page 2-55.

  Note 2: If you press the ACO button twice on the DSM, you will turn off the audible alarm and perform a lamp test on the DSM.

—continued—

Procedure 2-39 (continued)
Clearing audible alarms and performing lamp tests

Step	Action

Clearing audible alarms through Site Manager

2 Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1

3 Select the required network element in the navigation tree.

4 Select Alarm Cut-Off from the Faults drop-down menu.

5 Select the required network element or DSM from the Source drop-down list.

6 Click OK in the confirmation dialog box.

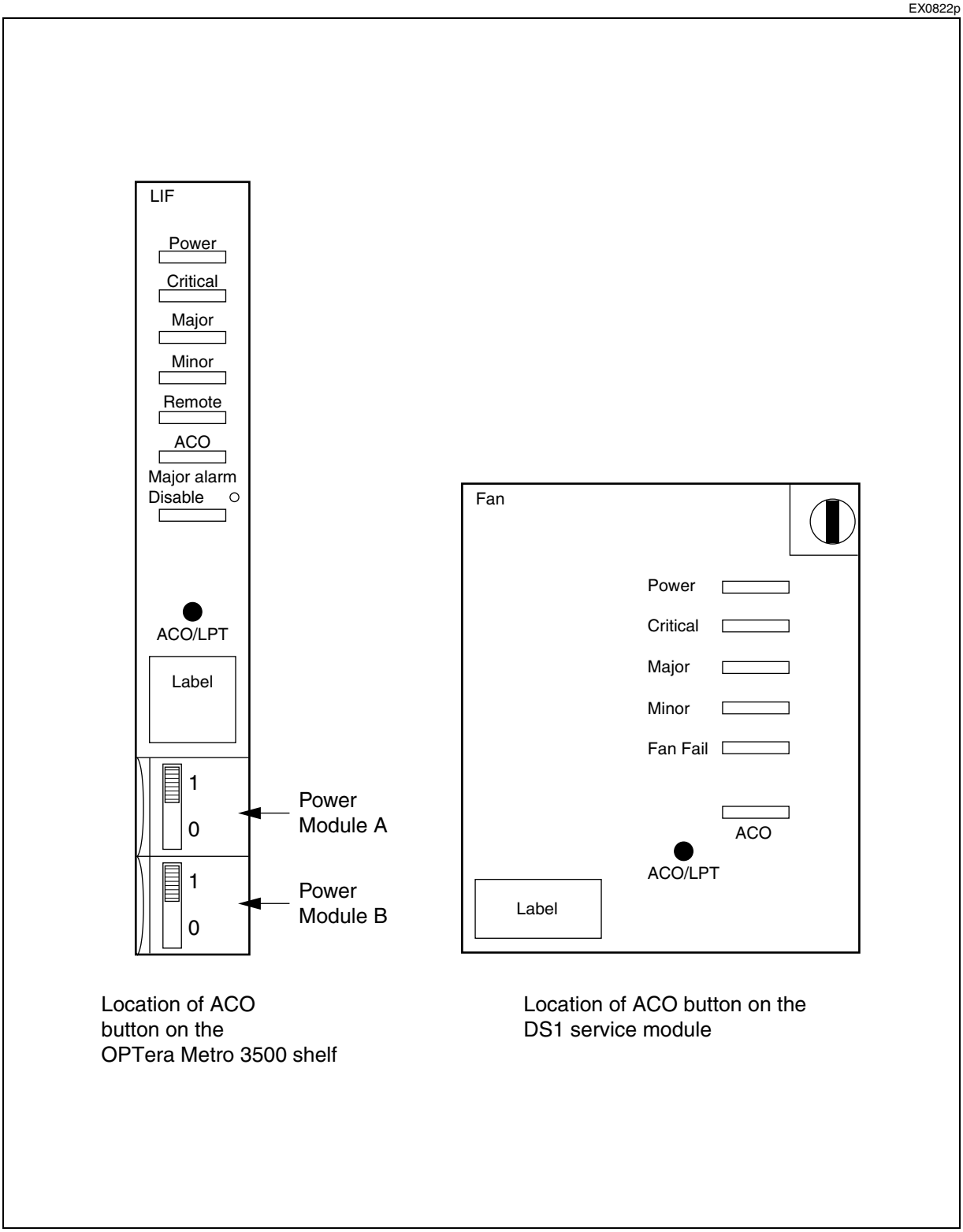
Note: Click Apply instead of OK and the window will remain open.

Note: To perform a lamp test through the Site Manager interface, see 323-1059-302, Procedures for shelf graphics and inventory on page 5-1.

—end—

Alarm cutoff button on the LIF and on the DS1 service module

EX0822p



Location of ACO button on the OPTera Metro 3500 shelf

Location of ACO button on the DS1 service module

Procedure 2-40
Retrieving environmental alarm attributes

Use this procedure to retrieve environmental alarm attributes.

Requirements

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation tree.
3	Select External Alarm Provisioning from the Configuration drop-down menu.
4	Select the network element or DS1 service module from the Source drop-down list.

—end—

Procedure 2-41
Editing environmental alarm attributes

Use this procedure to set up or change environmental alarm attributes on the network element or on a DS1 service module (DSM).

Environmental alarm attributes require resetting if you replace an existing environmental alarm with a different type of input. For example, when you replace a humidity alarm with a toxic gas detector, you must edit the environmental alarm attributes.

Requirements

To perform this procedure, you must:

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation tree.
3	Select External Alarm Provisioning from the Configuration drop-down menu.
4	Select the network element or DSM from the Source drop-down list.
5	Select any entry in the External Alarm Provisioning list to enable the Edit button.
6	Click Edit.
7	Select the contact you want to set or edit from the Contact drop-down list.
8	Select the label from the Label drop-down list.
9	Select the severity from the Severity drop-down list.
10	Edit the description if you want to describe the alarm with some specific text. ***Note:*** The description can contain a maximum of 40 characters.
11	Click Apply if you want to set or edit more contacts.
12	Repeat step 7 through step 11 if you want to set or edit more contacts.
13	Click OK.

—end—

Procedure 2-42
Deleting environmental alarm attributes

Use this procedure to delete defined environmental alarm attributes on the network element or DS1 service module (DSM).

When you remove a device for detecting an environmental alarm, you must delete the environmental alarm attributes.

Requirements

To perform this procedure, you must:

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the network element in the navigation tree.
3	Select External Alarm Provisioning from the Configuration drop-down menu.
4	Select the network element or DSM required from the Source drop-down list.
5	Select the contact from which you want to delete attributes in the External Alarm Provisioning list.
6	Click Clear Entry.
7	Click Yes in the confirmation dialog box.

—end—

Procedure 2-43
Editing external control attributes

Use this procedure to assign control labels and types to control relays on the network element or DS1 service module (DSM).

The network element allows four external control relays to turn external equipment on and off. There are four contact pairs on a DSM. To turn external controls on and off, refer to Operating external controls on page 2-62 and Releasing external controls on page 2-63.

The external control relays support the following external control types:

External control label	External control type
Air conditioning	Air conditioning
Engine	Engine
Fan	Fan
Generator	Generator
Heat	Heater
Light	Lighting
Miscellaneous	Miscellaneous
Sprinkler	Sprinkler
(Null)	No label is associated with the specific relay. However, some piece of external equipment can be connected to this relay.

Requirements

To perform this procedure, you must:

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the required network element in the navigation tree.

—continued—

Procedure 2-43 (continued)
Editing external control attributes

Step	Action
3	Select External Controls from the Configuration drop-down menu.
4	Select the required network element or DSM from the Source drop-down list.
5	Click Edit.
6	Select the relay label from the drop-down list at the relay for which you want to set or edit attributes.
7	Repeat step 5 and step 6 if you want to set or edit more relays.
8	Click OK.

—end—

Procedure 2-44
Retrieving external control status

Use this procedure to list the labels and status of all external controls. The External Controls window displays the status of the external control relays.

Requirements

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

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the required network element in the navigation tree.
3	Select External Controls from the Configuration drop-down menu.
4	Select the required network element or DSM from the Source drop-down list.

—end—

Procedure 2-45
Operating external controls

Use this procedure to turn on external control equipment.

Requirements

To perform this procedure, you must:

- use an account with at least a level 2 user privilege code (UPC)
- ensure you have all the documentation referenced in this procedure

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the required network element in the navigation tree.
3	Select External Controls from the Configuration drop-down menu.
4	Select the required network element or DSM from the Source drop-down list.
5	Select the required relay.
6	Click Operate.
7	Click Yes in the confirmation dialog box.

—end—

Procedure 2-46
Releasing external controls

Use this procedure to turn off external control equipment.

Requirements

To perform this procedure, you must:

- use an account with at least a level 2 user privilege code (UPC)
- ensure you have all the documentation referenced in this procedure

Step	Action
1	Ensure you are logged in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Select the required network element in the navigation tree.
3	Select External Controls from the Configuration drop-down menu.
4	Select the required network element or DSM from the Source drop-down list.
5	Select the required relay.
6	Click Release.
7	Click Yes in the confirmation dialog box.

—end—

Equipment replacement

Procedures for equipment replacement

Safety requirements

CAUTION
Loss of functionality
When you replace a circuit pack, the circuit pack can take up to 5 minutes to auto-upgrade. If you remove the circuit pack before the auto-upgrade process is complete, the circuit pack does not function properly.

CAUTION
Loss of functionality
All system functionality is lost when the shelf processor is removed. Only traffic is maintained.

CAUTION
Risk of circuit pack damage
Avoid touching any components on the printed circuit board. Electrostatic discharge can damage electrostatic-sensitive devices. Always connect yourself to ground before handling any circuit pack.

CAUTION
Risk of circuit pack damage
Do not force a circuit pack all the way to the back of a slot if it resists insertion. Before installing any of the circuit packs, make sure you know the detailed procedure for insertion of circuit packs.

CAUTION
Risk of service interruption
Electrostatic discharge can corrupt traffic. Severe discharges can cause temporary service interruptions.

CAUTION
Risk of service interruption
If you use radio communication devices like cellular telephones, service interruptions can occur. For example, a North American cellular telephone of approximately 1 W must not be used within 30 cm of a system with an open service access front cover.

Procedure 3-1
Reseating a circuit pack

Requirements

To perform this procedure, you must:

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 3-3 and *Installation*, 323-1059-201.

CAUTION
Risk of traffic loss
You will lose all traffic while reseating an unprotected circuit pack. Ensure that the circuit pack you are reseating is protected.

Step	Action

1 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

If the circuit pack you are reseating is in a	**Then**
1+1 linear system	step 2
UPSR configuration	step 3
BLSR configuration	step 4

2 Perform a manual switch to verify the protection path. See 323-1059-311, Operating a manual optical line switch in a 1+1 linear system on page 1-26.

- If traffic switches back autonomously to the working path, contact your next level of support or your Nortel Networks support group.
- If the circuit pack to be reseated is the working one, operate a forced switch. See 323-1059-311, Operating a forced optical line switch in a 1+1 linear system on page 1-27.
  If the circuit pack to be reseated is the protection one, operate a lockout. See 323-1059-311, Operating a lockout on an optical interface circuit pack in a 1+1 linear system on page 1-28.

3 Change the facility states to out of service for all facilities on the circuit pack. See 323-1059-350, Putting circuit pack equipment out of service (OOS) on page 2-15. Go to step 6.

4 Perform a manual switch. See 323-1059-311, Operating a manual switch in a BLSR on page 1-31.
If traffic switches back autonomously to the working path, contact your next level of support or your Nortel Networks support group.

5 Perform a forced switch. 323-1059-311, Operating a forced switch in a BLSR on page 1-32.

—continued—

Procedure 3-1 (continued)
Reseating a circuit pack

Step	Action
6	Pull the locking levers of the circuit pack to disengage the circuit pack from the backplane and wait 1 second.
7	Remove the circuit pack from the slot by pulling on the locking levers. ***Note:*** Alarms are raised, but cleared when the circuit pack is inserted back into the slot at the completion of this procedure.
8	Insert the circuit pack into the slot by lifting the locking levers and carefully guiding it into the slot guide grooves. ***Note:*** The circuit pack is right side up when the printed labels on the front faceplate are right side up.
9	Push the circuit pack all the way in until the locking levers touch their latches.
10	Lock the circuit pack into its slot by pushing the locking levers toward the faceplate at the same time. ***Note 1:*** Do not force the locking levers. If the levers do not close properly, remove the circuit pack and look for bent pins or damage to the module or shelf keys. The shelf keys are colored inserts at the top and bottom of the shelf connector. ***Note 2:*** The circuit pack can take 5 minutes to become available.
11	Change the facility states to in service for all facilities on the circuit pack. See 323-1059-350, Putting circuit pack equipment in service (IS) on page 2-16.

If the circuit pack you reseated is in a	**Then**
1+1 linear system	step 12
UPSR configuration	You have completed this procedure
BLSR configuration	step 13

12	Return traffic to the circuit pack by releasing the protection switch as follows: • Select Status from the Protection drop-down menu. • Select the appropriate optical interface circuit pack type (for example, OC12) from the Equipment/Path Type list. • Select the reseated circuit pack from the Equipment list. • Click Release. Click Yes in the confirmation dialog box. • If the circuit pack reseated was the working one, operate a manual switch. See 323-1059-311, Operating a manual optical line switch in a 1+1 linear system on page 1-26. You have completed this procedure.

—continued—

Procedure 3-1 (continued)
Reseating a circuit pack

Step	Action
13	Return traffic to the circuit pack by releasing the protection switch as follows: • Select Status from the Protection drop-down menu. • Select the appropriate optical interface circuit pack type (for example, OC12) from the Equipment/Path Type list. • Select the reseated circuit pack from the Equipment list. • Click Release. Click Yes in the confirmation dialog box. **—end—**

Procedure 3-2
Replacing the shelf processor

Use this procedure to replace the OPTera Metro 3500 shelf processor.

CAUTION
Loss of provisioning functionality
All provisioning functionality is lost when the shelf processor is removed. Only traffic is maintained.

CAUTION
Risk of database corruption and outage
Do not perform this procedure until you have cleared all Circuit Pack Failed, Circuit Pack Mismatch, Circuit Pack Missing, Circuit Pack Unknown, Intercard Failed, and Intercard Suspected alarms on the transport circuit packs.

Requirements

To perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- ensure that no other provisioned circuit packs are missing

  Note: If the system is carrying Packet Edge traffic both VTX modules must be present.

- obtain a replacement shelf processor
- observe all safety requirements described in Safety requirements on page 3-3, and in Installation, 323-1059-201
- ensure all alarms are enabled; see Enabling alarm points on page 2-29

—continued—

Procedure 3-2 (continued)
Replacing the shelf processor

Step	Action
1	Select Active Alarms from the Faults drop-down menu to retrieve alarms. ***Note:*** If the shelf processor is not functioning at all, and therefore you cannot retrieve any alarms; or you are sure you want to replace the shelf processor, go to step 3.
2	Clear all alarms raised against the shelf processor, except the alarms that require shelf processor replacement. ***Note:*** Performing step 2 may clear the alarms that require shelf processor replacement. Do not continue this procedure if you do not need to replace the shelf processor.
3	Replace the circuit pack. See Attaching or detaching a circuit pack from the back plane on page 3-94.
4	Wait 5 minutes for the shelf processor to boot.
5	Click OK in the Session Dropped confirmation dialog box that says 'The session has most likely dropped due to an inactive connection timeout.'
6	Log in to the network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
7	Click OK in the Login information box if the message 'TypeRelease for node' is raised. The shelf processor is running a lower release than the rest of the shelf.
8	Verify the current software version of the shelf processor. See 323-1059-302, Verifying the current shelf processor software version on page 6-75.

If the shelf processor is running	**Then** go to
a lower release than was previously running on the shelf	step 9
a higher release than was previously running on the shelf	step 10
the same release as was previously running on the shelf	step 12

9	Upgrade the shelf processor software. To upgrade the shelf processor software, see 323-1059-302, Installing a software load on a shelf processor from a local computer on page 6-49 or Installing a software load on a shelf processor using an Ethernet connection on page 6-52. Go to step 12. ***Note:*** After you upgrade the shelf processor software, you must perform a cold restart of the shelf processor circuit pack. See Restarting the shelf processor on page 2-47. FPGA load mismatches that occur after the shelf processor software upgrade are detected only after a cold restart of the shelf processor.

—continued—

Procedure 3-2 (continued)
Replacing the shelf processor

Step	Action
10	**If** / **Then** go to
	you want to upgrade the shelf — the appropriate change of application procedure (CAP) for upgrade activities of the shelf processor replacement in *OPTera Metro 3500 Multiservice Platform, Site Manager system software upgrade CAP*
	you do not want to upgrade the shelf — step 11
	Note: If the shelf processor is running a release prior to Release 12 and is inserted into a a shelf that is running Release 12 or later, the unmodifiable default login banner is enabled.
11	Replace the shelf processor with a shelf processor that is running the same release as the rest of the shelf. ***Note:*** If the shelf processor is running Release 12 or later and is inserted in a shelf that is running software prior to Release 12, the modifiable default login banner is enabled.
12	Select Active Alarms from the Faults drop-down menu to retrieve alarms. Clear all alarms raised against the shelf processor. ***Note:*** If the shelf processor is running Release 12 or later and is inserted in a shelf running Release 12 or later, the modifiable default login banner is enabled if it was previously provisioned on the shelf.

—end—

Procedure 3-3
Replacing the network processor

Use this procedure to replace an extended network processor (NPx).

> ***Note:*** Other than the changes specified in this procedure, do not make any provisioning changes to the network processor before you complete step 13.

Requirements

To perform this procedure, you must

- use an account with level 3 or higher user privilege code (UPC)
- obtain a replacement network processor
- observe all safety requirements described in Safety requirements on page 3-3
- ensure all alarms are enabled; see Enabling alarm points on page 2-29

Step	Action
1	Select Active Alarms from the Faults drop-down menu to retrieve alarms.
2	Clear all alarms raised against the network processor, except the alarms that require network processor replacement (for example, Circuit Pack Failed). ***Note:*** Performing step 2 may clear the alarms that require network processor replacement. Do not continue this procedure if you do not need to replace the network processor.
3	Verify that the Duplicate SID detected alarm is not active. If it is active, clear the alarm before continuing to step 4. See Duplicate SID Detected on page 4-154.
4	Log in to the network processor. See 323-1059-302, Procedures for logging in to a network processor on page 2-1.
5	If the COLAN facility is provisioned, save the provisioning data from the network processor. See 323-1059-302, Procedures for provisioning data and software management on page 6-1.
6	If the COLAN facility is provisioned, record the COLAN parameters: • Ensure that the network processor is selected in the navigation tree. • Select NP Facility from the Configuration drop-down menu. • Select COLAN from the NP Facility table. • Click Edit to open the Edit COLAN dialog box. • Record the parameters listed in the Edit COLAN dialog box. • Click Cancel to close the Edit COLAN dialog box.

—continued—

Procedure 3-3 (continued)
Replacing the network processor

Step	Action
7	Verify the manual area address. • Select the network element with the network processor, and select Node Information from the Configuration drop-down menu. • Select the General tab, then click Upper Layer SDCC, and verify that the manual area address is provisioned. • If the manual area address is required and is not provisioned, provision it. See 323-1059-350, Editing the upper layer SDCC on page 2-42.
8	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
9	Remove the network processor. See Attaching or detaching a circuit pack from the back plane on page 3-94. ***Note:*** Site Manager automatically logs out of the network processor when the network processor is removed from the shelf.
10	Click OK in the Session Dropped dialog box.
11	Insert the replacement network processor. See Attaching or detaching a circuit pack from the back plane on page 3-94. ***Note 1:*** Allow time for the network processor to reset. Wait until all network processor alarms clear. This can take 5 minutes. ***Note 2:*** When the replacement network processor is inserted, the co-located shelf processor raises the Remote Alarm(s) alarm. The Remote Alarm(s) alarm remains active for up to 5 minutes (until the network processor restart is complete) or until all network processor alarms clear. ***Note 3:*** While the network processor is inserted but not yet available, there is still ILAN communication to and from the co-located shelf processor and through the shelf.
12	Log in to the replacement network processor. See 323-1059-302, Procedures for logging in to a network processor on page 2-1. ***Note 1:*** If the network processor is running a release prior to Release 12 and is inserted in a shelf that is running Release 12 or later, the unmodifiable default login banner is enabled. ***Note 2:*** If the network processor is running Release 12 or later and is inserted in a shelf that is running software prior to Release 12, the modifiable default login banner is enabled. ***Note 3:*** If the network processor is running Release 12 or later and is inserted in a shelf running Release 12 or later, the modifiable default login banner is enabled if it was previously provisioned on the shelf. • If you can log in to the replacement network processor, go to step 13. • If you cannot log in to the replacement network processor, go to step 16.

—continued—

Procedure 3-3 (continued)
Replacing the network processor

Step	Action
13	Ensure that the software load is the same as the network element load. If the loads are not the same, install the required software load on the network processor. See 323-1059-302, Upgrading the software load on a network processor on page 6-55.
14	Ensure that the IP address and associated parameters are the same as the parameters you recorded in step 6. See 323-1059-520, Editing a COLAN facility on page 3-3.
15	Go to step 22.
16	Connect your PC to the shelf processor co-located with the replacement network processor directly by cable. ***Note:*** Use an RS-232 cable.
17	Log in to the replacement network processor using direct cable. See 323-1059-302, Logging in to a network processor using a direct cable connection on page 2-11. ***Note:*** Ensure that the replacement network processor ID is entered at Login NE field in the Login NE Information area.
18	Ensure that the software load is the same as the network element load. If the loads are not the same, install the required software load on the network processor. See 323-1059-302, Upgrading the software load on a network processor on page 6-55.
19	Ensure that the IP address and associated parameters are the same as the parameters you recorded in step 6. See 323-1059-520, Editing a COLAN facility on page 3-3.
20	Disconnect from the replacement network processor. See 323-1059-302, Disconnecting from a network processor or a network element on page 2-41.
21	Log in to the replacement network processor. See 323-1059-302, Procedures for logging in to a network processor on page 2-1.
22	Select Active Alarms from the Faults drop-down menu to retrieve alarms, and clear all alarms raised against the network processor.
23	If you had surveillance to the network processor before replacement, re-establish surveillance to your network processor and all network elements in the network processor SOC using the COLAN or X.25 network processor interface. If surveillance through the COLAN interface is required, you must use the IP address provisioned.

—end—

Procedure 3-4
Replacing the ILAN circuit pack

Requirements

To perform this procedure, you must

- obtain a replacement circuit pack
- observe all safety requirements described in Safety requirements on page 3-3
- ensure all alarms are enabled; see Enabling alarm points on page 2-29

Step	Action
1	Select Active Alarms from the Faults drop-down menu to retrieve alarms.
2	Clear all alarms raised against the ILAN circuit pack, except the alarms that require ILAN circuit pack replacement. ***Note:*** Performing step 2 may clear the alarms that require ILAN circuit pack replacement. Do not continue this procedure if you do not need to replace the ILAN circuit pack.
3	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
4	Lift the locking levers at the top and bottom of the circuit pack to unlock and disengage the circuit pack from the backplane.
5	Pull on the locking levers to remove the circuit pack from the slot. ***Note 1:*** The Circuit pack missing alarm is raised. ***Note 2:*** The Circuit pack missing alarm masks any alarms raised against the ILAN circuit pack.
6	Place the circuit pack in a static protection envelope.
7	Lift the replacement circuit pack by the locking levers and insert it carefully into the slot guide grooves. ***Note:*** The circuit pack is right side up when the printed labels on the front faceplate are right side up.
8	Push the circuit pack all the way in until the locking levers touch their latches.
9	Lock the circuit pack into its slot by pushing the upper locking lever down and the lower locking lever up at the same time. ***Note:*** Do not force the locking levers. If the levers do not close properly, remove the circuit pack and examine the connectors on the back of the circuit pack. Look for bent pins or damage to the circuit pack or shelf keys. The shelf keys are the colored inserts near the top and bottom of the shelf connector.

—continued—

Procedure 3-4 (continued)
Replacing the ILAN circuit pack

Step	Action
10	Select Shelf Level View from the Configuration drop-down menu, and click Refresh in the Shelf Level View window.
11	Select Active Alarms from the Faults drop-down menu to retrieve alarms. Clear all alarms raised against the circuit pack.

—end—

Procedure 3-5
Replacing an OPTera Packet Edge circuit pack

Use this procedure to replace any of the following Packet Edge circuit packs:

- 4x100BT in slots 3 through 10
- 4x100FX in slots 3 through 10
- 2xGigE in slots 3, 5, 7, or 9

Requirements

To perform this procedure, you must

- obtain the required replacement Packet Edge circuit pack
- observe all safety requirements described in Safety requirements on page 3-3
- use an account with level 3 or higher user privilege code (UPC)

Step	Action
1	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Access the BCC CLI through a Terminal Telnet session. See 323-1059-302, Accessing the BCC CLI on page 2-37.
3	Disable the LAN ports on the Packet Edge circuit pack. For details about how to disable the LAN ports, see *OPTera Packet Edge System User Guide*, NTN465YG.
4	Disable the WAN ports on the Packet Edge circuit pack. For details about how to disable the WAN ports, see *OPTera Packet Edge System User Guide,* NTN465YG.
5	Save configuration data to non-volatile RAM for this circuit pack. For details about how to save configuration data, see *OPTera Packet Edge System User Guide*, NTN465YG.
6	Log out of the BCC CLI. See 323-1059-302, Logging out of the BCC CLI on page 2-39.
7	Detach the Packet Edge circuit pack from the ring. See 323-1059-320, Detaching an OPTera Packet Edge circuit pack from an RPR on page 5-24.
8	Disconnect any fibers or cables that are attached to the circuit pack. ***Note:*** For details on disconnecting fiber-optic cable from a 4x100FX or 2xGigE circuit pack, see *Installation*, 323-1059-201.

—continued—

Procedure 3-5 (continued)
Replacing an OPTera Packet Edge circuit pack

Step	Action
9	Replace the Packet Edge circuit pack. See Attaching or detaching a circuit pack from the back plane on page 3-94.
10	Connect any fibers or cables that you removed from the circuit pack in step 8. ***Note:*** For details on connecting fiber-optic cable to a 4x100FX or 2xGigE circuit pack, see *Installation*, 323-1059-201.
11	Ensure that the new Packet Edge circuit pack is recognized by the shelf processor in the Shelf Level View. ***Note:*** Ensure that the Circuit Pack Missing alarm clears.
12	Wait 13 minutes for the circuit pack to autoprovision.
13	Access the BCC CLI and enable the WAN ports of the Packet Edge circuit pack. See 323-1059-302, Accessing the BCC CLI on page 2-37 and *OPTera Packet Edge System User Guide*, NTN465YG.
14	Enable the LAN ports of the Packet Edge circuit pack. For details about how to enable the LAN ports, see *OPTera Packet Edge System User Guide*, NTN465YG.
15	Log out of the BCC CLI. See 323-1059-302, Logging out of the BCC CLI on page 2-39.
16	Attach the Packet Edge circuit pack to the ring. See 323-1059-320, Attaching an OPTera Packet Edge circuit pack to an RPR on page 5-22.
17	Select Active Alarms from the Faults drop-down menu to retrieve alarms. If there is any alarm, refer to the appropriate trouble clearing procedure. See Detailed procedures for active alarms on page 4-1.
18	Ensure that the alarms raised on the far end network element are cleared. ***Note:*** If there is a new alarm, refer to the appropriate trouble clearing procedure. See Detailed procedures for active alarms on page 4-1.

—end—

Procedure 3-6
Replacing a 2x100BT-P2P circuit pack

Use this procedure to replace a 2x100BT-P2P circuit pack.

CAUTION
Risk of traffic loss
There is no equipment protection for 2x100BT-P2P circuit packs. You lose all traffic when you replace a 2x100BT-P2P circuit pack that is carrying traffic.

Requirements

To perform this procedure, you must

- obtain the required replacement circuit pack
- observe all safety requirements described in Safety requirements on page 3-3
- use an account with level 3 or higher user privilege code (UPC)

Step	Action
1	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Disconnect any cables that are attached to the circuit pack.
3	Replace the circuit pack. See Attaching or detaching a circuit pack from the back plane on page 3-94.
4	Connect any cables that you removed from the circuit pack in step 2.
5	Select Active Alarms from the Faults menu. Ensure that the Circuit Pack Missing alarm is not raised by the circuit pack. Clear other alarms according to the appropriate procedure. See Detailed procedures for active alarms on page 4-1.
6	Select Shelf Level View from the Configuration menu. Ensure that the new circuit pack is recognized in the Shelf Level View window.
7	Ensure that alarms raised on the far end network element are cleared. If necessary, see Detailed procedures for active alarms on page 4-1.

—end—

Procedure 3-7
Replacing a 2xGigE/FC-P2P circuit pack

Use this procedure to replace a 2xGigE/FC-P2P circuit pack.

CAUTION
Risk of traffic loss
There is no equipment protection for 2xGigE/FC-P2P circuit packs. You lose all traffic when you replace a 2xGigE/FC-P2P circuit pack that is carrying traffic.

Requirements

To perform this procedure, you must

- obtain the required replacement circuit pack
- if you plan to use different SFP modules from those installed in the circuit pack you are removing, obtain two supported replacement SFP modules: Optical Communication Products TRP-G1 (multi-mode) or TRP-G1D (single mode). You must install an SX SFP module for multi-mode fiber-optic cable or an LX SFP module for single-mode fiber-optic cable.

ATTENTION
Ensure that you use the correct SFP module type. No alarm is raised to indicate a mismatch between the SFP module and the fiber-optic cable.

- obtain dust covers for any empty SFP slots. Dust covers are required to prevent damage to empty SFP slots.
- observe all safety requirements described in Safety requirements on page 3-3
- use an account with level 3 or higher user privilege code (UPC)

Step	Action
1	Place all facilities on the 2xGigE/FC-P2P circuit pack out-of-service (OOS). See 323-1059-350, Changing a facility state to Out of Service (OOS) on page 2-25. ***Note:*** To display the Facility details, you must first select the SFP equipment from the Equipment area of the Equipment & Facility Provisioning window.
2	Place the 2xGigE/FC-P2P equipment OOS. See 323-1059-350, Putting circuit pack equipment out of service (OOS) on page 2-15.

—continued—

Procedure 3-7 (continued)
Replacing a 2xGigE/FC-P2P circuit pack

Step	Action
3	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
4	Disconnect any cables that are attached to the 2xGigE/FC-P2P circuit pack. ***Note:*** For details on disconnecting fiber-optic cable, see *Installation*, 323-1059-201.
5	Disengage the circuit pack from the back plane. See Attaching or detaching a circuit pack from the back plane on page 3-94.
6	If you plan to use the same SFP modules that are currently installed in the 2xGigE/FC-P2P circuit pack you are removing, remove each SFP module from the circuit pack as follows: • Open the latch on the SFP module by pressing the latch to the left. • Carefully pull the SFP module out of its slot. • Install a dust cover into each empty SFP slot on the circuit pack. Dust covers are required to prevent damage to empty SFP slots.
7	Place the circuit pack you removed in a static protection envelope.
8	Install each SFP module into the replacement 2xGigE/FC-P2P circuit pack as follows: • With the label on the replacement SFP module facing to the right and the LC connectors facing away from the shelf, slide the SFP module into the receptacle on the 2xGigE/FC-P2P faceplate until the SFP module locks into place. See SFP module replacement on page 3-23. • Close the latch on the SFP module by pressing the latch to the right.
9	If you do not install an SFP in each available SFP slot, install a dust cover (if not already installed) in any empty SFP slot. Dust covers are required to prevent damage to empty SFP slots.
10	Engage the circuit pack in the back plane. See Attaching or detaching a circuit pack from the back plane on page 3-94.
11	Connect any cables that you removed from the circuit pack in step 4. ***Note:*** For details on connecting fiber-optic cable, see *Installation*, 323-1059-201.
12	Place the 2xGigE/FC-P2P equipment IS. See 323-1059-350, Putting circuit pack equipment in service (IS) on page 2-16.
13	Place the facilities on the 2xGigE/FC-P2P circuit pack IS. See 323-1059-350, Changing a facility state to In Service (IS) on page 2-26. ***Note:*** To display the Facility details, you must first select the SFP equipment from the Equipment area of the Equipment & Facility Provisioning window.

—continued—

Procedure 3-7 (continued)
Replacing a 2xGigE/FC-P2P circuit pack

Step	Action
14	Select Active Alarms from the Faults menu. Ensure that the Circuit Pack Missing alarm is not raised by the circuit pack. Clear other alarms according to the appropriate procedure. See Detailed procedures for active alarms on page 4-1.
15	Select Shelf Level View from the Configuration menu. Ensure that the new circuit pack is recognized in the Shelf Level View window.
16	Ensure that alarms raised on the far end network element are cleared. If necessary, see Detailed procedures for active alarms on page 4-1.

—end—

Procedure 3-8
Replacing a Small Form Factor Pluggable (SFP) optical transceiver module

Use this procedure to replace an SFP optical transceiver module installed in a a 2xGigE/FC-P2P circuit pack.

CAUTION
Risk of traffic loss
There is no equipment protection for 2xGigE/FC-P2P circuit packs. You lose all traffic when you replace an SFP module that is carrying traffic.

Note: If the Circuit Pack Failed or Intercard Failed alarm is raised against a 2xGigE/FC-P2P circuit pack, and you replace the SFPs on the circuit pack, the SFP inventory displayed in the Equipment & Facility Provisioning window is not updated. To correctly display the SFP inventory, clear the alarm first, then replace the SFPs.

Requirements

To perform this procedure, you must

- obtain a supported SFP module: Optical Communication Products TRP-G1 (multi-mode) or TRP-G1D (single mode). You must install an SX SFP module for multi-mode fiber-optic cable or an LX SFP module for single-mode fiber-optic cable.

ATTENTION
Ensure that you use the correct SFP module type. No alarm is raised to indicate a mismatch between the SFP module and the fiber-optic cable.

- observe all safety requirements described in Safety requirements on page 3-3
- use an account with level 3 or higher user privilege code (UPC)

—continued—

Procedure 3-8 (continued)
Replacing a Small Form Factor Pluggable (SFP) optical transceiver module

Step	Action

Removing the SFP optical tranceiver module from the 2xGigE/FC-P2P circuit pack

1 Place the corresponding LAN facility out-of-service (OOS). See 323-1059-350, Changing a facility state to Out of Service (OOS) on page 2-25.

Note: To display the Facility details, you must first select the SFP equipment from the Equipment area of the Equipment & Facility Provisioning window.

2 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

3 Disconnect the fiber-optic cable from the SFP module.

4 Open the latch on the SFP module by pressing the latch to the left.

5 Carefully pull the SFP module out of its slot.

Inserting a replacement SFP module into the 2xGigE/FC-P2P circuit pack

6 With the label on the replacement SFP module facing to the right and the LC connectors facing away from the shelf, slide the SFP module into the receptacle on the 2xGigE/FC-P2P faceplate until the SFP module locks into place. See SFP module replacement on page 3-23.

7 Close the latch on the SFP module by pressing the latch to the right.

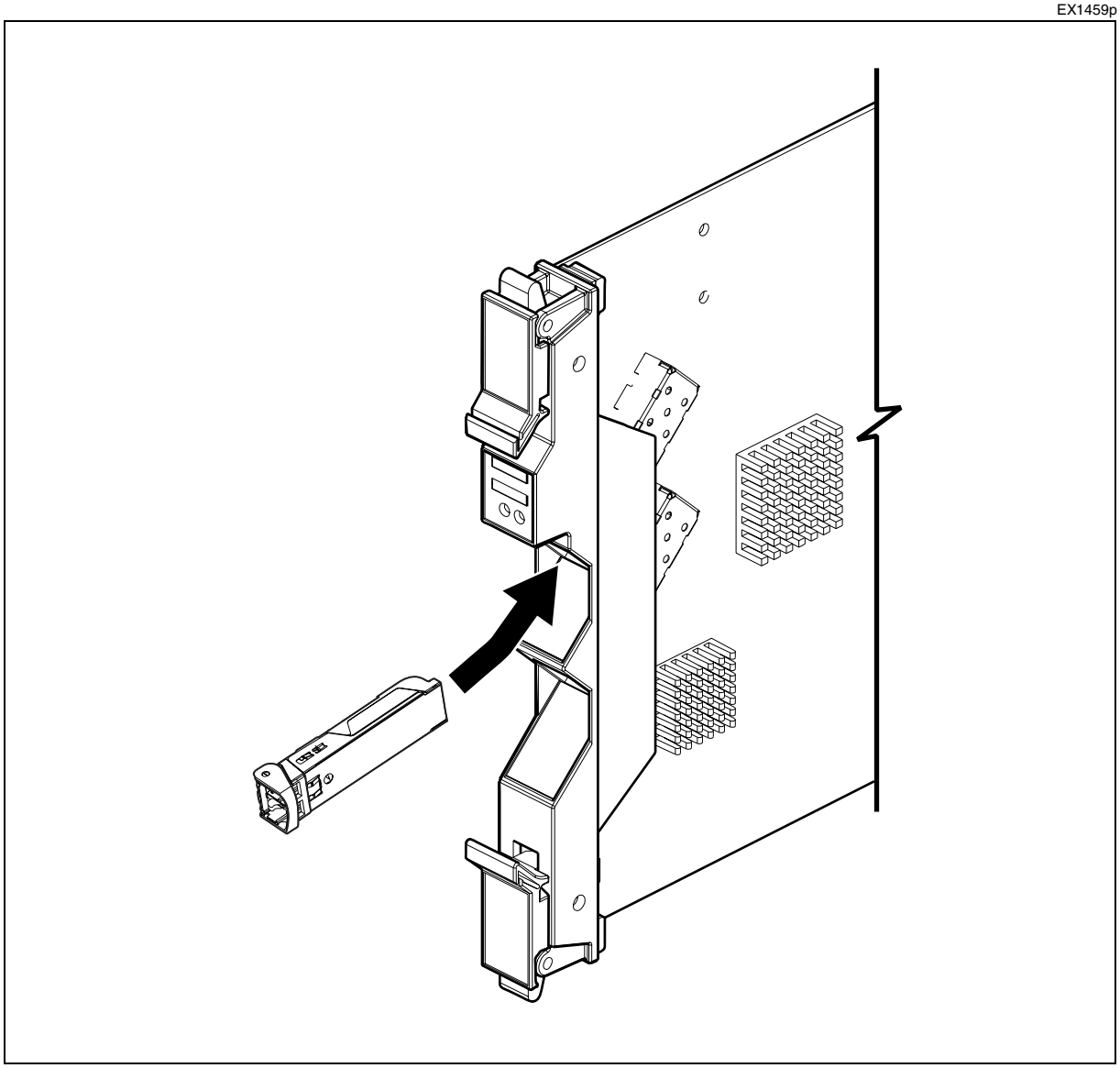
8 Reconnect the cable you removed in step 3.

9 Place the corresponding LAN facility in-service. See 323-1059-350, Changing a facility state to In Service (IS) on page 2-26.

—end—

SFP module replacement

EX1459p



Procedure 3-9
Replacing a DS1 mapper

Use this procedure to replace the DS1 mapper.

Note: Circuit packs are keyed to fit into specific slots and into specific types of shelves.

Requirements

To perform this procedure, you must

- obtain a replacement mapper
- observe all safety requirements described in Safety requirements on page 3-3
- ensure all alarms are enabled; See Enabling alarm points on page 2-29
- use an account with level 2 or higher user privilege code (UPC)

Step	Action
1	Select Active Alarms from the Faults drop-down menu to retrieve alarms.
2	Clear all alarms raised against the DS1 mapper, except those alarms that require DS1 mapper replacement. ***Note:*** Performing step 2 may clear the alarms that require DS1 mapper replacement. Do not continue this procedure if the mapper no longer requires replacing.
3	Switch DS1 traffic from the mapper to be replaced. See 323-1059-311, Operating a forced switch on a tributary circuit pack on page 1-18.
4	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

—continued—

Procedure 3-9 (continued)
Replacing a DS1 mapper

Step	Action
5	Replace the DS1 mapper. See Attaching or detaching a circuit pack from the back plane on page 3-94. ***Note 1:*** There is an automatic "Wait-to-Restore" period once the new mapper is inserted. By default, this period is 5 minutes. ***Note 2:*** If the upgrade fails, the Upgrade Fail alarm is activated.
6	Select Active Alarms from the Faults drop-down menu to retrieve alarms. Clear all alarms raised against the mapper. See Detailed procedures for active alarms on page 4-1.
7	Select Shelf Level View from the Configuration drop-down menu, and click Refresh in the Shelf Level View window.
8	Verify if the new mapper is recognized by the shelf processor in the Shelf Level View window. ***Note:*** A question mark (?) at the bottom of the circuit pack graphic indicates the circuit pack is not recognized.
9	**If** the new mapper — **Then** go to is recognized — step 10 is not recognized — step 11
10	Return DS1 traffic to the mapper. See 323-1059-311, Releasing a protection switch on a tributary circuit pack on page 1-21.
11	Select Active Alarms from the Faults drop-down menu to retrieve alarms. Clear all alarms raised against the mapper. See Detailed procedures for active alarms on page 4-1. If the new mapper was not recognized in step 9, return to step 8 after you have cleared all alarms against the mapper. Ensure that the shelf processor recognizes the new mapper before you return traffic to the mapper. If the mapper is not recognized even after you have cleared all alarms, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 3-10
Replacing the DSM DS1x84 termination module mapper

Use this procedure to replace a DSM DS1x84 termination module (TM) mapper.

Note: The host OC-3 port against which the DSM DS1x84TM will be provisioned must meet the following requirements.

— The OC-3 line facility and its SDCC are provisioned

— The OC-3 line facility is not already associated with a DS1 service module slot

— No cross-connects are provisioned on this line

— The line is not provisioned as a shelf timing reference

— The line is not a member of a facility fault protection (FFP) group pair.

— The OC-3 parameter REMOTE is set to OM3X00.

Also, the DSM DS1x84TM must be correctly fibered to the OC-3 circuit pack. If any one of these requirements are not met, the DSM will not autoprovision. Furthermore, an Autoprovisioning Mismatch alarm will not be raised.

Requirements

To perform this procedure, you must

- obtain a replacement mapper
- for protected scenarios, ensure that one DSM DS1x84 TM mapper is properly connected and alarm free
- observe all safety requirements described in Safety requirements on page 3-3
- ensure all alarms are enabled; see Enabling alarm points on page 2-29
- use an account with level 3 or higher user privilege code (UPC)

—continued—

Procedure 3-10 (continued)
Replacing the DSM DS1x84 termination module mapper

Step	Action
1	Select Active Alarms from the Faults drop-down menu to retrieve alarms.
2	Clear all LOS, LOP, SF, EBER, SD and equipment alarms raised against the host link optical interface circuit pack. ***Note 1:*** Performing step 2 may clear the alarms that require DSM DS1x84 TM mapper replacement. Do not continue this procedure if you do not need to replace the DSM DS1x84 TM mapper. ***Note 2:*** A user-initiated force switch away from a DSM DS1x84 TM mapper towards a protection DSM DS1x84 TM mapper will fail if the OCn line for the associated protection DSM DS1x84 TM mapper is faulty.
3	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
4	**If** you are replacing a DSM DS1x84 TM mapper — **Then** go to that is active and a protection DSM DS1x84 TM mapper is available — step 5 that is inactive and a protection DSM DS1x84 TM mapper is available — step 6 that is unprotected — step 17
5	Switch traffic away from the DSM DS1x84 TM mapper to be replaced by performing a forced switch. • Select Status from the Protection drop-down menu. • Select DS1 from the Equipment/Path Type list. • Select the mapper to be replaced under DS1 equipment protection. • Click Operate. • Select Forced Switch. • Click Operate. Click Yes in the confirmation dialog box.
6	Open the DSM front cover door.
7	Disconnect any fibers that are attached to the DSM DS1x84 TM mapper. ***Note:*** For details on disconnecting fiber-optic cable, see *Installation*, 323-1059-201.
8	Replace the DSM DS1x84 TM mapper. See Attaching or detaching a circuit pack from the back plane on page 3-94.
9	Connect any fibers that you removed from the DSM DS1x84 TM mapper in step 7. ***Note:*** For details on connecting fiber-optic cable, see *Installation*, 323-1059-201.
10	Wait 10 minutes for the system to upgrade and provision the mapper.

—continued—

Procedure 3-10 (continued)
Replacing the DSM DS1x84 termination module mapper

Step	Action
11	Select Inventory from the Configuration drop-down menu, and click Refresh in the Inventory window.
12	Verify if the new DSM DS1x84 TM mapper is present in the Inventory window.
13	If the new DSM DS1x84 TM mapper is present, go to step 15. If the new DSM DS1x84 TM mapper is not present, verify the fiber connections are correct, reseat the mapper, and ensure that SDCC is functioning. Go to step 14.
14	Verify the new DSM DS1x84 TM mapper is present in the Inventory window. If the mapper is not present, the DSM DS1x84 TM mapper is faulty. Use another DSM DS1x84 TM mapper and ensure it is present in the inventory window.
15	If you replaced a DSM DS1x84 TM mapper that was active before you started this procedure, release the forced switch as follows: • Select Status from the Protection drop-down menu. • Select DS1 from the Equipment/Path Type list. • Select the replaced mapper under DS1 equipment protection. • Click Release. Click Yes in the confirmation dialog box. • Go to step 18.
16	If you replaced a DSM DS1x84 TM mapper that was inactive before you started this procedure, and you want to switch traffic to the new mapper you installed: • Select Status from the Protection drop-down menu. • Select DSM DS1x84 TM from the Equipment/Path Type list. • Select the active mapper under DS1 equipment protection. • Click Operate. • Select Manual. • Click Operate. Click Yes in the confirmation dialog box. • Go to step 18.

—continued—

Procedure 3-10 (continued)
Replacing the DSM DS1x84 termination module mapper

Step	Action

17

CAUTION
Risk of traffic loss
You will lose all traffic while replacing an unprotected DSM DS1x84 TM mapper. You must perform the replacement as fast as possible to minimize the loss.

If the DSM DS1x84 TM mapper is not protected, perform the following:

For provisioning procedures, see 323-1059-350, Procedures for equipment provisioning on page 2-1 and Procedures for facility provisioning on page 2-1.

- Put the DS1 facilities out of service.
- Put the Host OCn facilities out of service.
- Put the DSM DS1x84 TM equipment out of service.
- Remove the fiber from the DSM DS1x84 TM mapper to be replaced.
- Remove and replace the DSM DS1x84 TM mapper. See Attaching or detaching a circuit pack from the back plane on page 3-94.
- Reconnect the fiber to the mapper. Allow time for the DSM DS1x84 TM mapper to restart.
- Put the host OCn facilities in service.
- Ensure that DS1 facilities and equipment are in service.

18 Select Active Alarms from the Faults menu to retrieve alarms. Clear all alarms raised against the mapper.

19 If the Circuit Pack Failed alarm was raised on the DSM DS1x84 TM mapper and does not clear, use a DS1 test set at the far-end network element to test the signal source.

If there is a loss of signal, the problem may be with the DS1 source. Perform troubleshooting on the source system according to your company procedures.

If there is no problem with the DS1 source, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 3-11
Replacing the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper

Use this procedure to replace the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper. You can also use this procedure to replace a DS3x12 mapper with a DS3x12e mapper. If this is the case, you must ensure that you do not have a mixed pair.

> ***Note:*** Circuit packs are keyed to fit into specific slots and into specific types of shelves.

Requirements

To perform this procedure, you must

- obtain a replacement mapper
- observe all safety requirements described in Safety requirements on page 3-3
- ensure all alarms are enabled; see Enabling alarm points on page 2-29
- use an account with level 2 or higher user privilege code (UPC)

Step	Action
1	Select Active Alarms from the Faults drop-down menu to retrieve alarms.
2	Clear all alarms raised against the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper, except the alarms that require DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper replacement. ***Note:*** Performing step 2 may clear the alarms that require DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper replacement. Do not continue this procedure if you do not need to replace the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper.
3	Switch traffic from the mapper to be replaced as follows: • Select Status from the Protection drop-down menu. • Select DS3 from the Equipment/Path Type list. • Select the mapper to be replaced under DS3 equipment protection. • Click Operate to open the Operate Protection Switch dialog box. • Select Forced Switch. • Click Operate. Click Yes in the confirmation dialog box. ***Note:*** If you are replacing a DS3x3, DS3x12, or DS3x12e mapper, ensure all the DS3 ports have successfully switched.

—continued—

Procedure 3-11 (continued)
Replacing the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper

Step	Action
4	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
5	Replace the mapper. See Attaching or detaching a circuit pack from the back plane on page 3-94.
6	Wait 5 minutes for the system to upgrade and provision the circuit pack. ***Note:*** If the upgrade fails, the Upgrade Failed alarm is activated.
7	Select Shelf Level View from the Configuration drop-down menu, and click Refresh in the Shelf Level View window.
8	Verify if the new DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper is recognized by the shelf processor in the Shelf Level View window. If the mapper is not recognized, go to step 9. ***Note:*** A question mark (?) at the bottom of the circuit pack graphic indicates the circuit pack is not recognized.
9	Select Active Alarms from the Faults drop-down menu to retrieve alarms. Clear all alarms raised against the mapper. See Detailed procedures for active alarms on page 4-1. If the new mapper was not recognized in step 8, return to step 7 after you have cleared all alarms against the mapper. Ensure that the shelf processor recognizes the new mapper. If the mapper is not recognized even after you have cleared all alarms, contact your next level of support or your Nortel Networks support group. **—end—**

Procedure 3-12
Replacing the EC-1x3 or EC-1x12 circuit pack

Use this procedure to replace the EC-1x3 or EC-1x12 circuit pack.

Note: Circuit packs are keyed to fit into specific slots and into specific types of shelves.

Requirements

To perform this procedure, you must

- obtain a replacement circuit pack
- observe all safety requirements described in Safety requirements on page 3-3
- ensure all alarms are enabled; see Disabling alarm points on page 2-28
- use an account with level 2 or higher user privilege code (UPC)

Step	Action
1	Select Active Alarms from the Faults drop-down menu to retrieve alarms.
2	Clear all alarms raised against the EC-1x3 or EC-1x12 circuit pack, except the alarms that require EC-1x3 or EC-1x12 circuit pack replacement. ***Note:*** Performing step 2 may clear the alarms that require EC-1x3 or EC-1x12 circuit pack replacement. Do not continue this procedure if you do not need to replace the EC-1x3 or EC-1x12 circuit pack.
3	Switch traffic from the circuit pack to be replaced as follows: • Select Status from the Protection drop-down menu. • Select EC-1from the Equipment/Path Type list. • Select the EC-1x3 or EC-1x12 to be replaced under EC-1x3 or EC-1x12 equipment protection. • Click Operate to open the Operate Protection Switch dialog box. • Select Forced. • Click Operate. Click Yes in the confirmation dialog box.
4	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
5	Replace the EC-1x3 or EC-1x12 circuit pack. See Attaching or detaching a circuit pack from the back plane on page 3-94.

—continued—

Procedure 3-12 (continued)
Replacing the EC-1x3 or EC-1x12 circuit pack

Step	Action
6	Wait 5 minutes for the system to upgrade and provision the circuit pack. ***Note:*** The Circuit Pack Missing alarm will clear once the circuit pack has finished upgrading.
7	Select Shelf Level View from the Configuration drop-down menu, and click Refresh in the Shelf Level View window.
8	Verify if the new EC-1x3 or EC-1x12 circuit pack is recognized by the shelf processor in the Shelf Level View window. ***Note:*** A question mark (?) at the bottom of the circuit pack graphic indicates the circuit pack is not recognized.
9	**If** the new circuit pack is — **Then** go to recognized — step 10 not recognized — step 11
10	Return traffic to the EC-1x3 or EC-1x12 circuit pack as follows: • Select Status from the Protection drop-down menu. • Select EC-1 from the Equipment/Path Type list. • Select the replaced circuit pack under EC-1x3 or EC-1x12 equipment protection. • Click Release. Click Yes in the confirmation dialog box.
11	Select Active Alarms from the Faults drop-down menu to retrieve alarms. Clear all alarms raised against the circuit pack. See Detailed procedures for active alarms on page 4-1. If the new circuit pack was not recognized in step 8, return to step 7 after you have cleared all alarms against the circuit pack. Ensure that the shelf processor recognizes the new circuit pack before you return traffic to the circuit pack. If the circuit pack is not recognized even after you have cleared all alarms, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 3-13
Replacing an optical interface circuit pack in a linear system

Use this procedure to replace the optical interface circuit packs in a linear system.

Note: Circuit packs are keyed to fit into specific slots.

Requirements

To perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- obtain a replacement circuit pack
- observe all safety requirements described in Safety requirements on page 3-3
- ensure all alarms are enabled; see Enabling alarm points on page 2-29
- use an account with level 2 or higher user privilege code (UPC)

Step	Action
1	Select Active Alarms from the Faults drop-down menu to retrieve alarms.
2	Clear all alarms raised against the circuit pack, except the alarms that require the circuit pack replacement. ***Note:*** Performing step 2 may clear the alarms that require the circuit pack replacement. Do not continue this procedure if you do not need to replace the circuit pack.

—continued—

Procedure 3-13 (continued)
Replacing an optical interface circuit pack in a linear system

Step	Action
3	Switch traffic from the optical interface circuit pack to be replaced as follows: • Select the network element from the Navigation tree that contains the optical interface to be replaced. • Select Status from the Protection drop-down menu. • Click Refresh. • Select the appropriate optical interface circuit pack type (for example, OC12) from the Equipment/Path Type list. • Select the circuit pack to be replaced under the Equipment list. • Perform a manual switch to verify the protection path. See 323-1059-311, Operating a manual optical line switch in a 1+1 linear system on page 1-26. If traffic switches back autonomously to the working path, contact your next level of support or your Nortel Networks support group. • If the circuit pack to be replaced is the working one, operate a forced switch. See 323-1059-311, Operating a forced optical line switch in a 1+1 linear system on page 1-27. If the circuit pack to be replaced is the protection one, operate a lockout. See 323-1059-311, Operating a lockout on an optical interface circuit pack in a 1+1 linear system on page 1-28.
4	Put the circuit pack equipment to be replaced out of service. See 323-1059-350, Putting circuit pack equipment out of service (OOS) on page 2-15.
5	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
6	Detach the fiber-optic cables on the optical interface circuit pack you are replacing. ***Note 1:*** If you are replacing an OC-3 or an OC-3x4 circuit pack that is connected to a DS1 service module (DSM), you must first disconnect the DSM. See *Installation,* 323-1059-201. ***Note 2:*** For details on disconnecting fiber-optic cable, see *Installation*, 323-1059-201.
7	Replace the optical interface circuit pack. See Attaching or detaching a circuit pack from the back plane on page 3-94. ***Note:*** Ensure that the replacement circuit pack is of the same type and reach.

—continued—

Procedure 3-13 (continued)
Replacing an optical interface circuit pack in a linear system

Step	Action
8	Measure the Transmit (Tx) power of the optical interface circuit pack. See 323-1059-222, Testing the power at the optical interface Tx port on page 2-8. ***Note:*** The value obtained from the test must comply with the Launch power minimum value found in the Technical specifications chapter of the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM.
9	**CAUTION** **Risk of damaging equipment** Ensure the received input power of the optical interface does not exceed the overload value. Otherwise, the equipment will be damaged. A variable optical attenuator or a fixed attenuator must be installed for each instance where the received power level exceeds the overload level. Measure the Received (Rx) power of the optical interface circuit pack. See 323-1059-222, Testing the power at the optical interface Rx port on page 2-10. ***Note:*** The value obtained from the test must be above the Receive sensitivity (min) value for the given unit and must not exceed the overload value found in the Technical specifications chapter of the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM.
10	Reattach the fiber-optic cables removed at step 6. **CAUTION** **Risk of signal degrade or loss of signal** When sliding the fiber tray back into an OC-3x4 circuit pack with SC connectors, ensure that the internal fibers are not kinked, twisted or snagged as they are routed into the fiber retainer. Visible signs of damage to primary coatings, buffers or jackets can cause signal degrade or loss of signal to the circuit pack. ***Note 1:*** If you disconnected the DSM in step 6, you must reconnect the DSM. See *Installation,* Connecting a DS1 service module to OPTera Metro 3500, 323-1059-201. ***Note 2:*** For details on connecting fiber-optic cable, refer to *Installation*, 323-1059-201.
11	Wait 5 minutes for the system to upgrade and provision the circuit pack.
12	Perform a cold restart of the circuit pack. See Restarting a circuit pack on page 2-45.

—continued—

Procedure 3-13 (continued)
Replacing an optical interface circuit pack in a linear system

Step	Action
13	Select Shelf Level View from the Configuration drop-down menu, and click Refresh in the Shelf Level View window.
14	Verify if the new circuit pack is recognized by the shelf processor in the Shelf Level View. ***Note:*** A question mark (?) at the bottom of the circuit pack graphic indicates the circuit pack is not recognized.
15	If the new circuit pack is recognized, go to step 17. If the new circuit pack is not recognized, go to step 16.
16	Select Active Alarms from the Faults drop-down menu to retrieve alarms. Clear all alarms raised against the circuit pack. Ensure the circuit pack is recognized by the shelf processor before you return the traffic.
17	Put the circuit pack equipment in service. See 323-1059-350, Putting circuit pack equipment in service (IS) on page 2-16.
18	Return traffic to the circuit pack by releasing the protection switch as follows: • Select Status from the Protection drop-down menu. • Select the appropriate optical interface circuit pack type (for example, OC12) from the Equipment/Path Type list. • Select the replaced circuit pack from the Equipment list. • Click Release. Click Yes in the confirmation dialog box. **—end—**

Procedure 3-14
Replacing an optical interface circuit pack in a UPSR

Use this procedure to replace the optical interface circuit pack in a unidirectional path-switched ring (UPSR).

Note: Circuit packs are keyed to fit into specific slots.

Requirements

To perform this procedure, you must

- ensure you have all the documentaton referenced in this procedure
- obtain a replacement circuit pack
- observe all safety requirements described in Safety requirements on page 3-3
- ensure all alarms are enabled; see Enabling alarm points on page 2-29
- use an account with level 2 or higher user privilege code (UPC)

Step	Action
1	Select Active Alarms from the Faults drop-down menu to retrieve alarms.
2	Clear all alarms raised against the circuit pack, except the alarms that require the circuit pack replacement. ***Note:*** Performing step 2 may clear the alarms that require the circuit pack replacement. Do not continue this procedure if you do not need to replace the circuit pack.
3	Put the circuit pack equipment to be replaced out of service. See 323-1059-350, Putting circuit pack equipment out of service (OOS) on page 2-15.
4	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
5	Detach the fiber-optic cables on the optical interface circuit pack you are replacing. ***Note 1:*** If you are replacing an OC-3 or an OC-3x4 circuit pack that is connected to a DS1 service module (DSM), you must first disconnect the DSM. See *Installation,* 323-1059-201. ***Note 2:*** For details on disconnecting fiber-optic cable, see *Installation*, 323-1059-201.

—continued—

Procedure 3-14 (continued)
Replacing an optical interface circuit pack in a UPSR

Step	Action
6	Replace the optical interface circuit pack. See Attaching or detaching a circuit pack from the back plane on page 3-94. ***Note:*** Ensure that the replacement circuit pack is of the same type and reach.
7	Measure the Transmit (Tx) power of the optical interface circuit pack. See 323-1059-222, Testing the power at the optical interface Tx port on page 2-8. ***Note:*** The value obtained from the test must comply with the Launch power minimum value found in the Technical specifications chapter of the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM.
8	**CAUTION** **Risk of damaging equipment** Ensure the received input power of the optical interface does not exceed the overload value. Otherwise, the equipment will be damaged. A variable optical attenuator or a fixed attenuator must be installed for each instance where the received power level exceeds the overload level. Measure the Received (Rx) power of the optical interface circuit pack. See 323-1059-222, Testing the power at the optical interface Rx port on page 2-10. ***Note:*** The value obtained from the test must be above the Receive sensitivity (min) value for the given unit and must not exceed the overload value found in the Technical specifications chapter of the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM.

—continued—

Procedure 3-14 (continued)
Replacing an optical interface circuit pack in a UPSR

Step	Action
9	Reattach the fiber-optic cables removed at step 5.

CAUTION
Risk of signal degrade or loss of signal
When sliding the fiber tray back into an OC-3x4 circuit pack with SC connectors, ensure that the internal fibers are not kinked, twisted or snagged as they are routed into the fiber retainer. Visible signs of damage to primary coatings, buffers or jackets can cause signal degrade or loss of signal to the circuit pack.

Note 1: If you disconnected the DSM in step 5, you must reconnect the DSM. See *Installation,* Connecting a DS1 service module to OPTera Metro 3500, 323-1059-201.

Note 2: For details on connecting fiber-optic cable, see *Installation*, 323-1059-201.

10 Wait 5 minutes for the system to upgrade and provision the circuit pack.

11 Perform a cold restart of the circuit pack. See Restarting a circuit pack on page 2-45.

12 Select Shelf Level View from the Configuration drop-down menu, and click Refresh in the Shelf Level View window.

13 Verify if the new circuit pack is recognized by the shelf processor in the Shelf Level View.

Note: A question mark (?) at the bottom of the circuit pack graphic indicates the circuit pack is not recognized.

14 If the new circuit pack is recognized, go to step 16. If the new circuit pack is not recognized, go to step 15.

15 Select Active Alarms from the Faults drop-down menu to retrieve alarms. Clear all alarms raised against the circuit pack. Ensure the circuit pack is recognized by the shelf processor before you return the traffic.

16 Put the circuit pack equipment in service. See 323-1059-350, Putting circuit pack equipment in service (IS) on page 2-16.

—end—

Procedure 3-15
Replacing an OC-48 or OC-192 optical interface circuit pack in a BLSR

Use this procedure to replace a double-width OC-48 or OC-192 optical interface circuit pack in a bidirectional line-switch ring (BLSR).

Note 1: Circuit packs are keyed to fit into specific slots.

Note 2: This procedure is not applicable to the OC-48 STS circuit pack. The OC-48 STS circuit pack does not support BLSR protection.

Requirements

To perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- obtain a replacement OC-48 or OC-192 circuit pack
- observe all safety requirements described in Safety requirements on page 3-3
- ensure all alarms are enabled; see Enabling alarm points on page 2-29
- use an account with level 2 or higher user privilege code (UPC)

Step	Action
1	Select Active Alarms from the Faults drop-down menu to retrieve alarms.
2	Clear all alarms raised against the circuit pack, except the alarms that require the circuit pack replacement. ***Note:*** Performing step 2 may clear the alarms that require the circuit pack replacement. Do not continue this procedure if you do not need to replace the circuit pack.

—continued—

Procedure 3-15 (continued)
Replacing an OC-48 or OC-192 optical interface circuit pack in a BLSR

Step	Action
3	Switch traffic from the optical interface circuit pack to be replaced: • Select the network element from the Navigation tree that contains the optical interface to be replaced. • Select Status from the Protection drop-down menu. • Click Refresh. • Select OC48 or OC192 under Protection summary. • Select the circuit pack to be replaced under OC48 equipment protection details or OC192 equipment protection details. • Perform a manual switch. See 323-1059-311, Operating a manual switch in a BLSR on page 1-31. If traffic switches back autonomously to the working path, contact your next level of support or your Nortel Networks support group. • Perform a forced switch. See 323-1059-311, Operating a forced switch in a BLSR on page 1-32. • Perform a manual switch. See 323-1059-311, Operating a manual switch in a BLSR on page 1-31. If traffic switches back autonomously to the working path, contact your next level of support or your Nortel Networks support group. • Perform a forced switch. See 323-1059-311, Operating a forced switch in a BLSR on page 1-32.
4	Put the circuit pack equipment to be replaced out of service. See 323-1059-350, Putting circuit pack equipment out of service (OOS) on page 2-15.
5	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
6	Detach the fiber-optic cables on the optical interface circuit pack you are replacing. ***Note:*** For details on diconnecting fiber-optic cable, see *Installation*, 323-1059-201.
7	Replace the optical interface circuit pack. See Attaching or detaching a circuit pack from the back plane on page 3-94. ***Note:*** Ensure that the replacement circuit pack is of the same type and reach.
8	Measure the Transmit (Tx) power of the optical interface circuit pack. See 323-1059-222, Testing the power at the optical interface Tx port on page 2-8 . ***Note:*** The value obtained from the test must comply with the Launch power minimum value found in the Technical specifications chapter of the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM.

—continued—

Procedure 3-15 (continued)
Replacing an OC-48 or OC-192 optical interface circuit pack in a BLSR

Step	Action
9	**CAUTION** **Risk of damaging equipment** Ensure the received input power of the optical interface does not exceed the overload value. Otherwise, the equipment will be damaged. A variable optical attenuator or a fixed attenuator must be installed for each instance where the received power level exceeds the overload level. Measure the Received (Rx) power of the optical interface circuit pack. See 323-1059-222, Testing the power at the optical interface Rx port on page 2-10. ***Note:*** The value obtained from the test must be above the Receive sensitivity (min) value for the given unit and must not exceed the overload value found in the Technical specifications chapter of the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM.
10	Reattach the fiber-optic cables removed at step 6. ***Note:*** For details on connecting fiber-optic cable, see *Installation*, 323-1059-201.
11	Wait 5 minutes for the system to upgrade and provision the circuit pack.
12	Perform a cold restart of the circuit pack. See Restarting a circuit pack on page 2-45.
13	Select Shelf Level View from the Configuration drop-down menu, and click Refresh in the Shelf Level View window.
14	Verify if the new circuit pack is recognized by the shelf processor in the Shelf Level View. ***Note:*** A question mark (?) at the bottom of the circuit pack graphic indicates the circuit pack is not recognized.
15	If the new circuit pack is recognized, go to step 17. If the new circuit pack is not recognized, go to step 16.
16	Select Active Alarms from the Faults drop-down menu to retrieve alarms. Clear all alarms raised against the circuit pack. Ensure the circuit pack is recognized by the shelf processor before you return the traffic. ***Note:*** If the circuit pack is not recognized by the shelf processor, contact your next level of support or your Nortel Networks support group.
17	Put the circuit pack equipment in service. See 323-1059-350, Putting circuit pack equipment in service (IS) on page 2-16.

—continued—

Procedure 3-15 (continued)
Replacing an OC-48 or OC-192 optical interface circuit pack in a BLSR

Step	Action
18	Return traffic to the circuit pack by releasing the protection switch as follows: • Select Status from the Protection drop-down menu. • Select OC48 or OC192 under Protection summary. • Select the circuit pack you replaced under OC48 equipment protection details or OC192 equipment protection details. • Click Release. Click Yes in the confirmation dialog box. **—end—**

Procedure 3-16
Replacing the PSC circuit pack

Use this procedure to replace a protection switch controller (PSC) circuit pack.

Note: Circuit packs are keyed to fit into specific slots.

Requirements

To perform this procedure, you must

- obtain a replacement circuit pack
- observe all safety requirements described in Safety requirements on page 3-3
- ensure all alarms are enabled; see Enabling alarm points on page 2-29

Step	Action
1	Select Active Alarms from the Faults drop-down menu to retrieve alarms.
2	Clear all alarms raised against the PSC circuit pack, except the alarms that require the PSC circuit pack replacement. ***Note:*** Performing step 2 may clear the alarms that require the PSC circuit pack replacement. Do not continue this procedure if you do not need to replace the PSC circuit pack.
3	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
4	**CAUTION** **Risk of traffic loss** Do not remove the PSC while a DS1 protection switch is active. Ensure that the PSC is not missing for an extended period of time. A shelf restart or a DS1 circuit pack insertion while the PSC is missing will affect DS1 traffic. Before removing the PSC, verify if there is an active DS1 protection switch, that is, the green LED is active on the PSC. If a switch is active, resolve the problem that caused the switch and ensure that traffic has switched back to the working DS1 mapper before continuing.
5	Replace the PSC circuit pack. See Attaching or detaching a circuit pack from the back plane on page 3-94.
6	Wait 5 minutes for the system to upgrade the circuit pack. ***Note:*** If the upgrade fails, the Upgrade Failed alarm is activated.
7	Select Shelf Level View from the Configuration drop-down menu, and click Refresh in the Shelf Level View window.

—continued—

Procedure 3-16 (continued)
Replacing the PSC circuit pack

Step	Action
8	Verify if the new PSC circuit pack is recognized by the shelf processor in the Shelf Level View window. ***Note:*** A question mark (?) at the bottom of the circuit pack graphic indicates the circuit pack is not recognized.
9	Select Active Alarms from the Faults drop-down menu to retrieve alarms. Clear all alarms raised against the mapper.

—end—

Procedure 3-17
Replacing the PSX circuit pack

Use this procedure to replace the protection switch extender (PSX) circuit pack.

Note: Circuit packs are keyed to fit into specific slots.

Requirements

To perform this procedure, you must

- obtain a replacement circuit pack
- observe all safety requirements described in Safety requirements on page 3-3
- ensure all alarms are enabled; see Enabling alarm points on page 2-29

Step	Action
1	Select Active Alarms from the Faults drop-down menu to retrieve alarms.
2	Clear all alarms raised against the PSX circuit pack, except the alarms that require the PSX circuit pack replacement. ***Note:*** Performing step 2 may clear the alarms that require the PSX circuit pack replacement. Do not continue this procedure if you do not need to replace the PSX circuit pack.
3	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
4	Replace the PSX circuit pack. See Attaching or detaching a circuit pack from the back plane on page 3-94.
5	Wait 5 minutes for the system to upgrade the circuit pack. ***Note:*** If the upgrade fails, the Upgrade Failed alarm is activated.
6	Select Shelf Level View from the Configuration drop-down menu, and click Refresh in the Shelf Level View window.
7	Verify if the new PSX circuit pack is recognized by the shelf processor in the Shelf Level View window. ***Note:*** A question mark (?) at the bottom of the circuit pack graphic indicates the circuit pack is not recognized.
8	Select Active Alarms from the Faults drop-down menu to retrieve alarms. Clear all alarms raised against the mapper.

—end—

Procedure 3-18
Replacing a VTX module

Use this procedure to replace the VTX-48 or VTX-48e circuit pack.

Note: Circuit packs are keyed to fit into specific slots.

Requirements

To perform this procedure, you must

- obtain a replacement circuit pack
- observe all safety requirements described in Safety requirements on page 3-3
- ensure all alarms are enabled; see Enabling alarm points on page 2-29
- use an account with level 3 or higher user privilege code (UPC)

CAUTION
Risk of OPE traffic congestion
Replacing a VTX module causes a ring segmentation in one direction through the resilient packet ring (RPR) path supported by that VTX module. This ring segmentation can result in the congestion of the RPR. OPE ring traffic must not exceed the bandwidth (STS-n) available for the ring.

Step	Action
1	Select Active Alarms from the Faults drop-down menu to retrieve alarms.
2	Clear all alarms raised against the VTX module, except the alarms that require the replacement of this circuit pack. ***Note:*** Performing step 2 may clear the alarms that require the VTX module replacement. Do not continue this procedure if replacing the VTX module is no longer required.

—continued—

Procedure 3-18 (continued)
Replacing a VTX module

Step	Action
3	Put the VTX module equipment out of service as follows: • Select Equipment & Facility Provisioning from the Configuration drop-down menu. • Select the equipment to be replaced under Equipment. • Click Edit under Equipment to open the Edit Equipment dialog box. • Select OOS from the Primary state drop-down list. • Click OK. Click Yes in the confirmation dialog box. ***Note 1:*** To put a VTX module in the OOS state, you must have an in-service VTX module in the mate slot. ***Note 2:*** Slot 13 and 14 must contain the same type of VTX module.
4	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
5	**CAUTION** **Risk of a traffic hit** A VTX module requires a time delay of one second while it is being removed from the shelf to allow time for the clocks to transfer without causing a traffic hit. Remove the VTX module as follows: • Pull the latches. • Wait one second. • Remove the circuit pack.
6	**CAUTION** **Risk of OPE traffic loss** When you insert a VTX module in the shelf, it can take up to 5 minutes to obtain the provisioning information. During that time, the circuit pack will be in service to respond to any protection switch from an optical interface or tributary circuit pack. For OPE traffic, the operating state of the affected WAN ports can be temporarily up during this time. When you perform a restart and put the VTX module in service, the WAN ports will remain up Insert the replacement VTX module into the empty slot. See Attaching or detaching a circuit pack from the back plane on page 3-94.
7	Wait 10 minutes for the system to upgrade the circuit pack.

—continued—

Procedure 3-18 (continued)
Replacing a VTX module

Step	Action
8	Perform a cold restart of the circuit pack. See Restarting a circuit pack on page 2-45.
9	Select Shelf Level View from the Configuration drop-down menu, and click Refresh in the Shelf Level View window.
10	Verify if the new circuit pack is recognized by the shelf processor in the Shelf Level View window. ***Note:*** A question mark (?) at the bottom of the circuit pack graphic indicates the circuit pack is not recognized.
11	If the new circuit pack is recognized, go to step 12. If the new circuit pack is not recognized, go to step 13.
12	Put the equipment in service for the VTX module as follows: • Select Equipment & Facility Provisioning from the Configuration drop-down menu. • Select the replaced equipment under Equipment. • Click Edit under Equipment to open the Edit Equipment dialog box. • Select IS from the Primary state drop-down list. • Click OK.
13	Select Active Alarms from the Faults drop-down menu to retrieve alarms. Clear all alarms raised against the VTX module. Ensure the circuit pack is recognized by the shelf processor before you put the equipment in service.

—end—

Procedure 3-19
Replacing an STX-192 circuit pack

Use this procedure to replace the STX-192 circuit pack.

Note: Circuit packs are keyed to fit into specific slots.

Requirements

To perform this procedure, you must

- obtain a replacement circuit pack
- observe all safety requirements described in Safety requirements on page 3-3
- ensure all alarms are enabled; see Enabling alarm points on page 2-29
- use an account with level 3 or higher user privilege code (UPC)

CAUTION
Risk of OPE traffic congestion
Replacing an STX-192 circuit pack causes a ring segmentation in one direction through the resilient packet ring (RPR) path supported by that STX-192 circuit pack. This ring segmentation can result in the congestion of the RPR. OPE ring traffic must not exceed the bandwidth (STS-n) available for the ring.

Step	Action
1	Select Active Alarms from the Faults drop-down menu to retrieve alarms.
2	Clear all alarms raised against the STX-192 circuit pack, except the alarms that require the replacement of this circuit pack. ***Note:*** Performing step 2 may clear the alarms that require the STX-192 circuit pack replacement. Do not continue this procedure if replacing the STX-192 circuit pack is no longer required.

—continued—

Procedure 3-19 (continued)
Replacing an STX-192 circuit pack

Step	Action
3	Put the STX-192 circuit pack equipment out of service as follows: • Select Equipment & Facility Provisioning from the Configuration drop-down menu. • Select the equipment to be replaced under Equipment. • Click Edit under Equipment to open the Edit Equipment dialog box. • Select OOS from the Primary state drop-down list. • Click OK. Click Yes in the confirmation dialog box. ***Note 1:*** To put an STX-192 circuit pack in the OOS state, you must have an in-service STX-192 circuit pack in the mate slot.
4	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
5	**CAUTION** **Risk of a traffic hit** An STX-192 circuit pack requires a time delay of one second while it is being removed from the shelf to allow time for the clocks to transfer without causing a traffic hit. Remove the STX-192 circuit pack as follows: • Pull the latches. • Wait one second. • Remove the circuit pack.
6	**CAUTION** **Risk of OPE traffic loss** When you insert an STX-192 circuit pack in the shelf, it can take up to 5 minutes to obtain the provisioning information. During that time, the circuit pack will be in service to respond to any protection switch from an optical interface or tributary circuit pack. For OPE traffic, the operating state of the affected WAN ports can be temporarily up during this time. When you perform a restart and put the STX-192 circuit pack in service, the WAN ports will remain up Insert the replacement STX-192 circuit pack into the empty slot. See Attaching or detaching a circuit pack from the back plane on page 3-94.
7	Wait 10 minutes for the system to upgrade the circuit pack.

—continued—

Procedure 3-19 (continued)
Replacing an STX-192 circuit pack

Step	Action
8	Perform a cold restart of the circuit pack. See Restarting a circuit pack on page 2-45.
9	Select Shelf Level View from the Configuration drop-down menu, and click Refresh in the Shelf Level View window.
10	Verify if the new circuit pack is recognized by the shelf processor in the Shelf Level View window. ***Note:*** A question mark (?) at the bottom of the circuit pack graphic indicates the circuit pack is not recognized.
11	If the new circuit pack is recognized, go to step 12. If the new circuit pack is not recognized, go to step 13.
12	Put the equipment in service for the STX-192 circuit pack as follows: • Select Equipment & Facility Provisioning from the Configuration drop-down menu. • Select the replaced equipment under Equipment. • Click Edit under Equipment to open the Edit Equipment dialog box. • Select IS from the Primary state drop-down list. • Click OK.
13	Select Active Alarms from the Faults drop-down menu to retrieve alarms. Clear all alarms raised against the STX-192 circuit pack. Ensure the circuit pack is recognized by the shelf processor before you put the equipment in service. ***Note:*** If the circuit pack is not recognized by the shelf processor, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 3-20
Replacing a fan module on the DS1 service module

Use this procedure to replace the fan module on the DS1 service module (DSM).

Requirement

To perform this procedure, you must

- obtain one fan module
- observe all safety requirements described in Safety requirements on page 3-3

Step	Action
1	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Open the DSM front cover door.
3	Verify that the Fan Fail LED is red.
4	Verify that the Minor LED is yellow, or that the Critical LED is red.
5	Loosen the thumbscrew on the front of the fan module.
6	Pull the fan module from the housing.
7	Insert the new fan module.
8	Verify the fan unit is seated properly.
9	Tighten the thumbscrew.
10	Verify that the Fan Failure alarm is cleared.

—end—

Procedure 3-21
Installing the power module and cooling unit upgrade kit

Use this procedure to install the power module and cooling unit upgrade kit.

Requirement

To perform this procedure, you must obtain one power module and cooling unit upgrade kit (NTN458MW).

Step	Action
1	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

Removing the shelf front cover

2	Rotate inward the two screws on the top, right, and left of the front cover.
3	Open the cover completely.
4	Push in the spring-loaded pins on the bottom left of the front cover. At the same time pull the left top of the cover just enough to disengage the pin from the shelf hole.
5	Push in the spring-loaded pins on the bottom right of the front cover. At the same time pull the right top of the cover just enough to disengage the pin from the shelf hole.
6	Pull out the front cover and store it in a safe place.

Removing the grill/air deflector

7	Open the front cover.
8	On the left side of the shelf, push in the spring-loaded pins of the grill/air deflector; at the same time pull the left end of the grill/air deflector just enough to disengage the pin from the shelf hole.
9	On the right side of the shelf, push in the spring-loaded pins of the grill/air deflector; at the same time pull the right end of the grill/air deflector just enough to disengage the pin from the shelf hole.
10	Pull out the grill/air deflector and store it in a safe place.

—continued—

Procedure 3-21 (continued)
Installing the power module and cooling unit upgrade kit

Step	Action

Removing the 12.5A power module

11 Switch the power A breaker of the network element to off.

12 Disconnect the -48V and Return power cable from the left side of the power A module.

13 Disconnect the fan power cable connector from power module A.

14 From the left side of the shelf, below the LOAM, remove the screw that secures the power module A to the shelf.

15 Using the tab handle of the power module A pull the power module out of the shelf.

Installing the new 20A power module

16 Slide the 20A power module into the shelf.

17 Insert and tighten the screw on the left side of the shelf, below the LOAM, to secure the power module to the shelf.

18 Connect the -48V and Return power cables to the power A module and switch the breaker to the on position.

19 Connect the fan power cable to the power module.

20 Repeat step 11 through step 19 to replace the power B module.

Replacing the cooling unit assembly

21 See Replacing the cooling unit assembly on page 3-57.

Installing the grill/air deflector

22 Push in the spring-loaded pins on the side of the grill/air deflector, insert the grill/air deflector into the shelf and release the pins.

23 Align the pins with the holes in the sides of the shelf and push the grill/air deflector until the pins enter the holes.

Installing the shelf front cover

24 Push in the spring-loaded pins on each side of the front cover.

25 Align the pins with the holes in the sides of the shelf, push the front cover into the shelf, and release the pins. Push the front cover gently until the spring-loaded pins enter the holes.

26 Close the front cover and rotate outward the two screws on the top, right, and left of the front cover.

—end—

Procedure 3-22
Replacing the cooling unit assembly

Requirements

To perform this procedure, you must obtain one cooling unit assembly kit (NTN458QA) for each network element in a bay. The kit includes three cooling unit fan modules, plenum assembly, and one power cable. The fan alarm cable is not included in the kit.

CAUTION
Risk of circuit pack failure
This procedure must be completed within 15 minutes to ensure that the circuit packs do not overheat and fail while there are no fans on the network element.

Step	Action
1	Clear all other alarms first using the appropriate procedure. See Detailed procedures for active alarms on page 4-1.
2	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
Opening the shelf front cover	
3	Rotate outward the two screws on the top, right and left of the shelf front cover.
4	Open the cover completely.
Removing the grill/air deflector	
5	Rotate the fiber storage tray toward the front of the shelf.
6	On the left side of the shelf, push in the spring-loaded pins of the grill/air deflector; at the same time pull the left end of the grill/air deflector just enough to disengage the pin from the shelf hole. See Installing and removing the grill/air deflector on page 3-65.
7	On the right side of the shelf, push in the spring-loaded pins of the grill/air deflector; at the same time pull the right end of the grill/air deflector just enough to disengage the pin from the shelf hole.
8	Pull out the grill/air deflector and store it in a safe place.

—continued—

Procedure 3-22 (continued)
Replacing the cooling unit assembly

Step	Action

Removing the cooling unit assembly from the shelf

9 Remove the fan assembly attaching screws. See Cooling unit assembly (NTN458QA) on page 3-61.

10 If applicable remove the grounding cable from the cooling unit. See Grounding the shelf on page 3-63.

Note: This step applies only when upgrading from an older cooling unit assembly. A grounding cable is not required for the new cooling unit assembly.

11 Disconnect the fan alarm cable connector from the cooling unit.

Note: The new cooling unit will reuse the fan alarm cable.

12 Disconnect the fan power cable connectors from power module A and power module B.

Note: When installing the power module and cooling unit upgrade kit (NTN458MW) remove the cable from the network element and replace it with the NTN458MJ power cable.

13 Lift out the cooling unit assembly from the top of the shelf.

Installing the new cooling unit assembly

14 Position the cooling unit assembly in respect to the front of the shelf.

15 Set down the cooling unit assembly on the top of the shelf.

16 If required, route the power cables to the top, left side of the shelf.

Note: Only one plug must go through the hole at a time.

17 Plug the cooling fan power cables into the cooling fan connectors and to the power modules A and B. See Power cable connections on page 3-59 and Fan power cable on page 3-64.

18 Attach the cooling unit assembly to the shelf using two attaching screws provided. See Cooling unit assembly (NTN458QA) on page 3-61.

Connecting the alarm cable to the LOAM connectors

19 Plug the alarm cable into the alarm connector on the left, front side of the cooling unit plenum. See Cooling unit plenum on page 3-62 and Fan alarm cable on page 3-64.

20 Use a tie wrap to attach the alarm and power cables to the cable tie lances on the left edge of the shelf.

Connecting the cooling fan power cables

21 Ensure the green LED in front of each fan module is ON.

—continued—

Procedure 3-22 (continued)
Replacing the cooling unit assembly

Step	Action

Installing the grill/air deflector

22 Push in the spring-loaded pins on the sides of the grill/air deflector, insert the grill/air deflector into the shelf and release the pins. See Installing and removing the grill/air deflector on page 3-65.

23 Align the pins with the holes in the sides of the shelf and push the grill/air deflector until the pins enter the holes.

Closing the front cover

24 Close the front cover and rotate inward the two screws on the top, right, and left of the front cover.

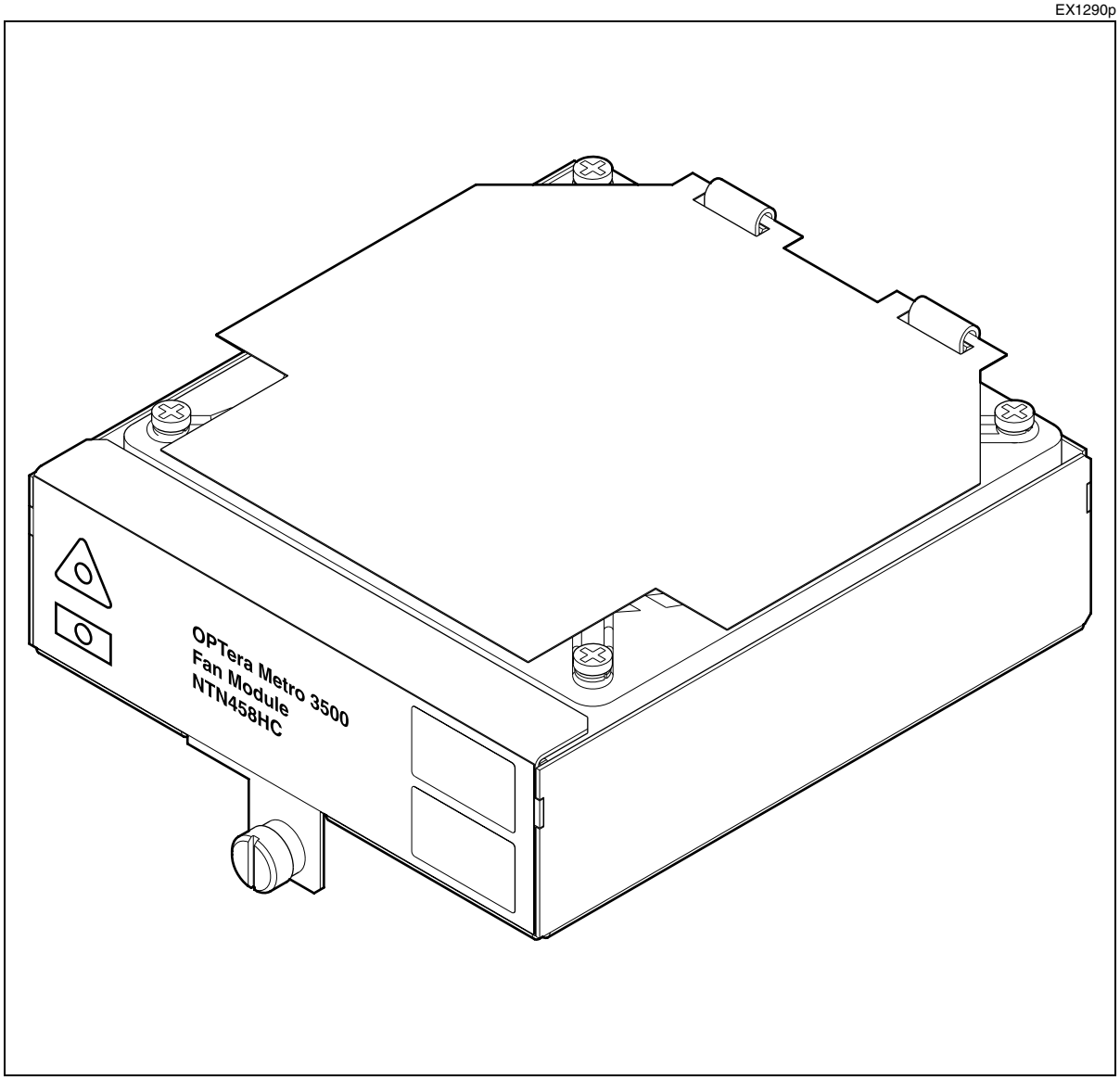
—end—

Power cable connections

Power cable lead	Power supply
Red	-48V A
White/red strip	A return
Red/blue strip	-48V B
White/blue strip	B return

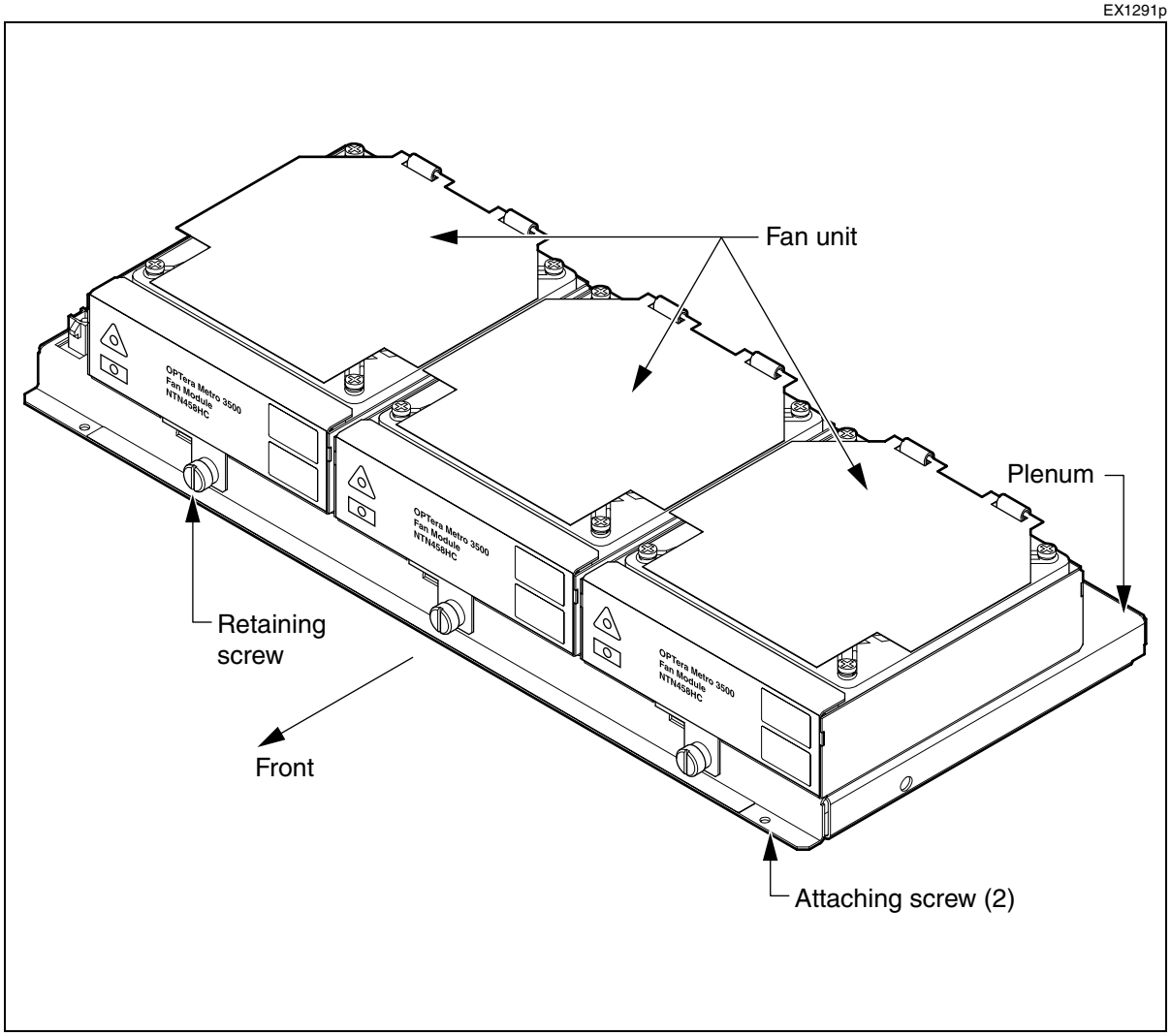
Cooling unit fan module (NTN458HC)

EX1290p



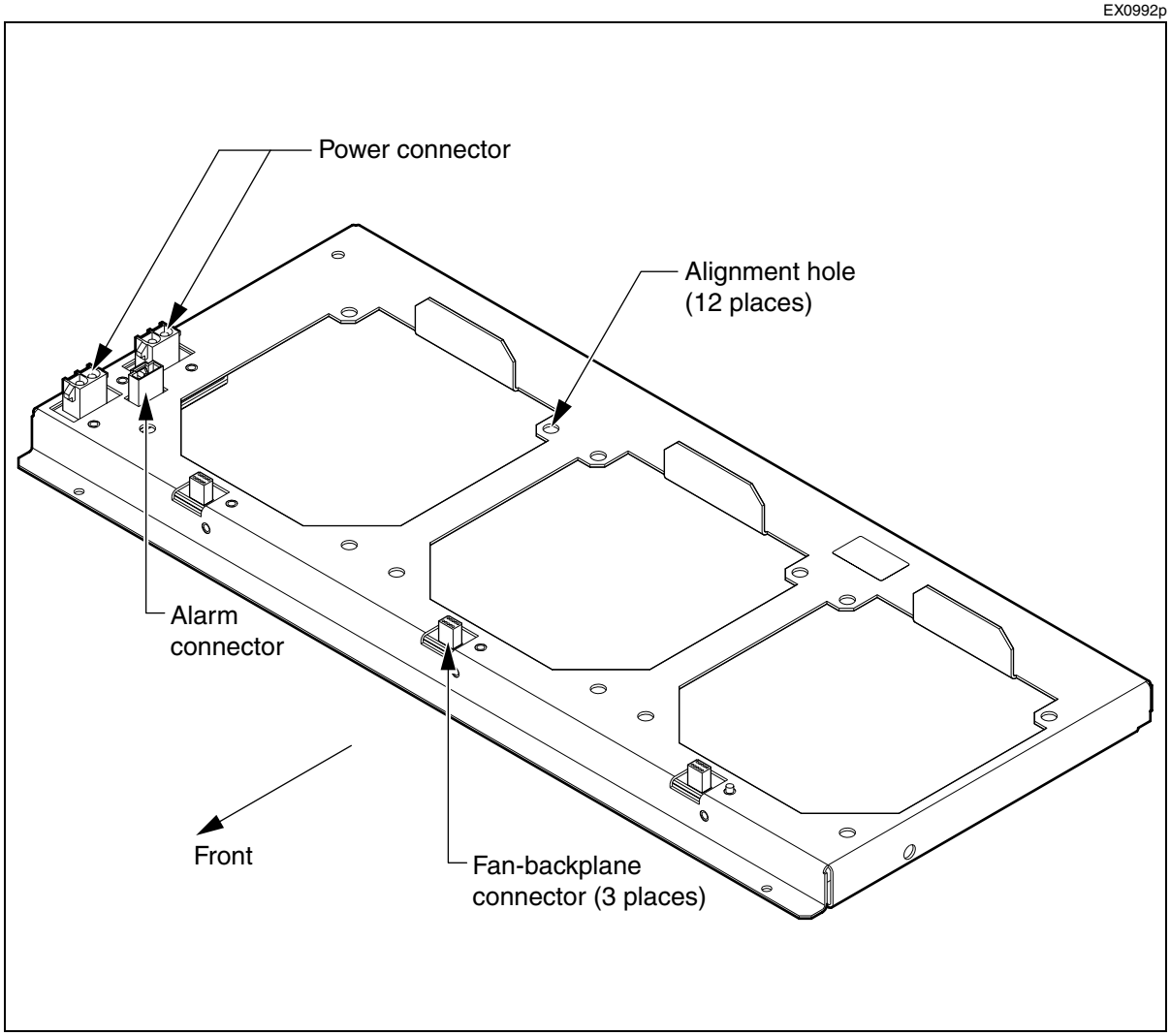
Cooling unit assembly (NTN458QA)

EX1291p



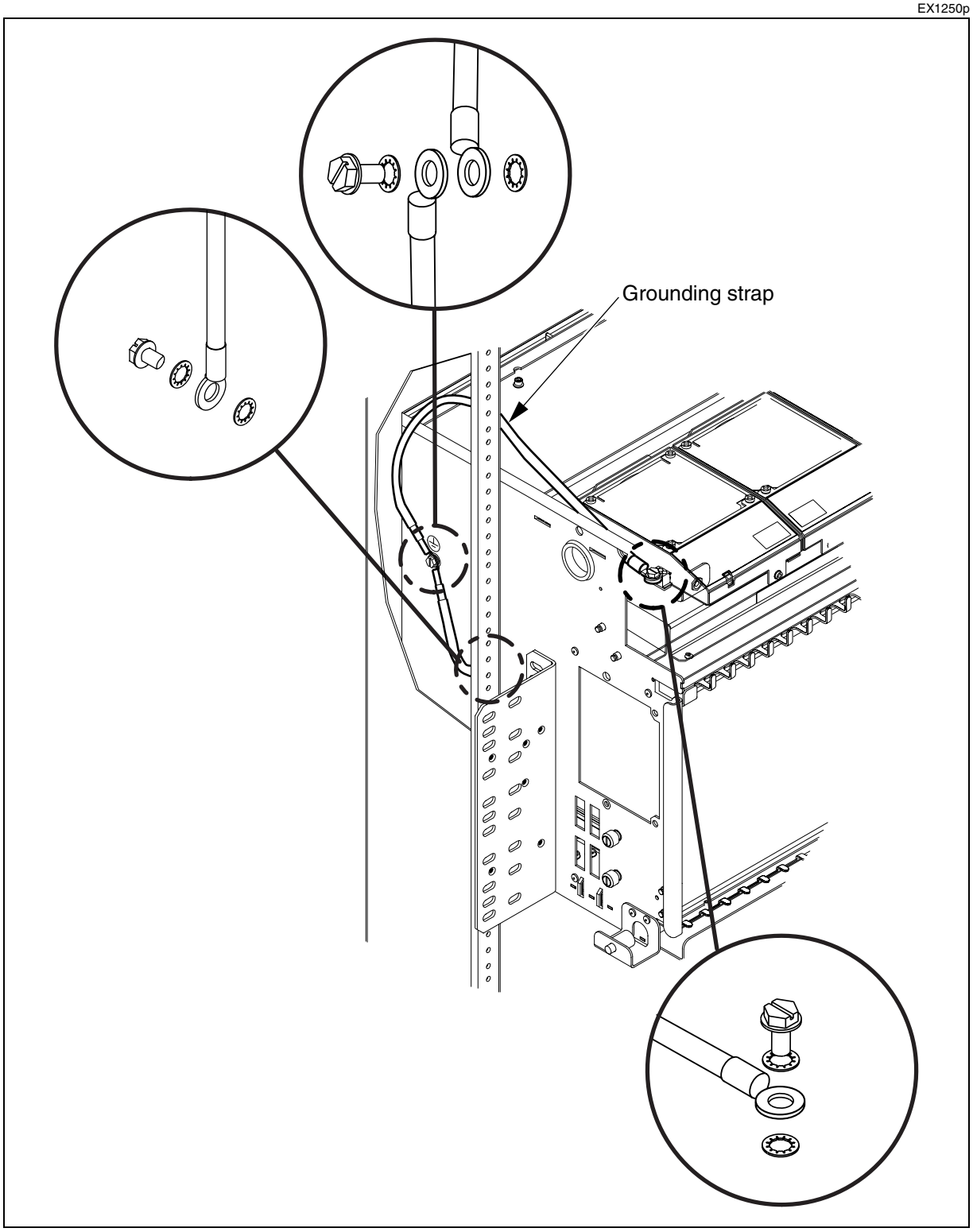
Cooling unit plenum

EX0992p



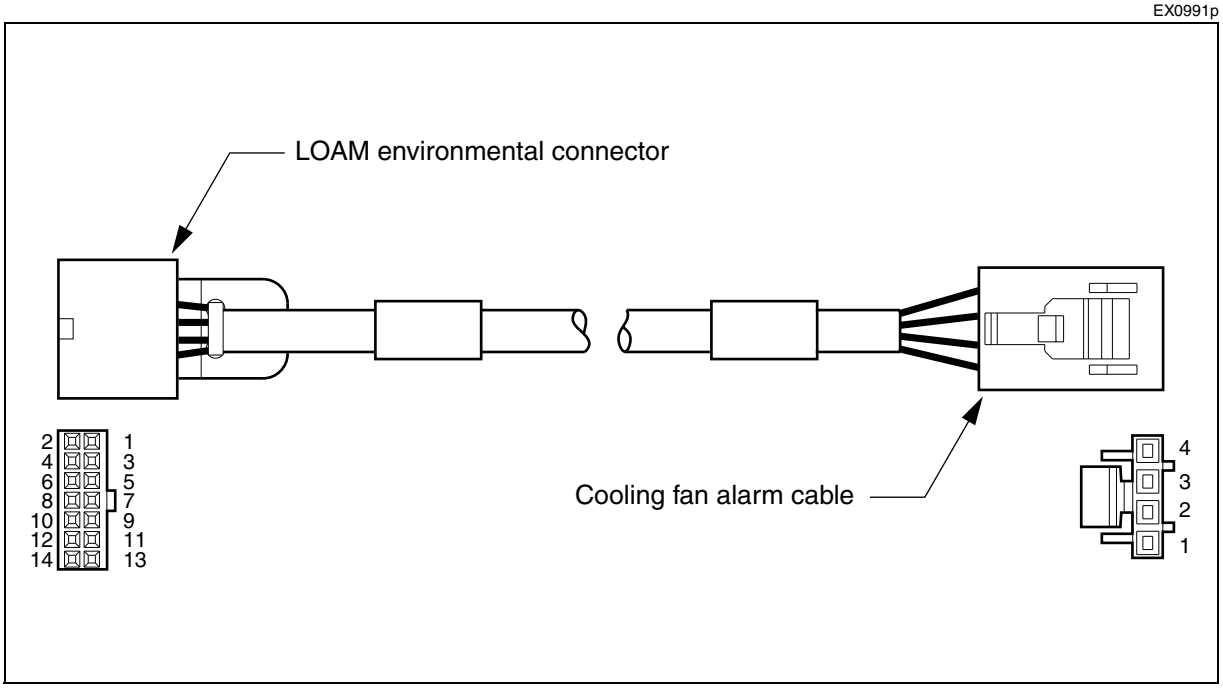
Grounding the shelf

EX1250p



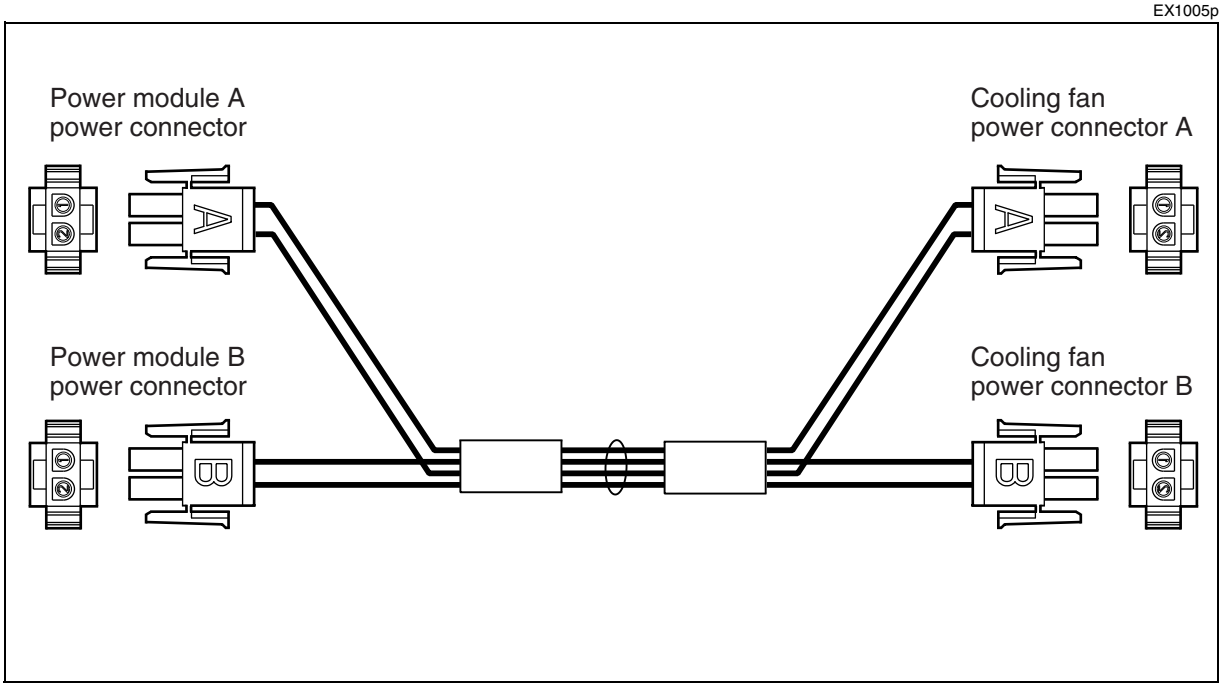
Fan alarm cable

EX0991p



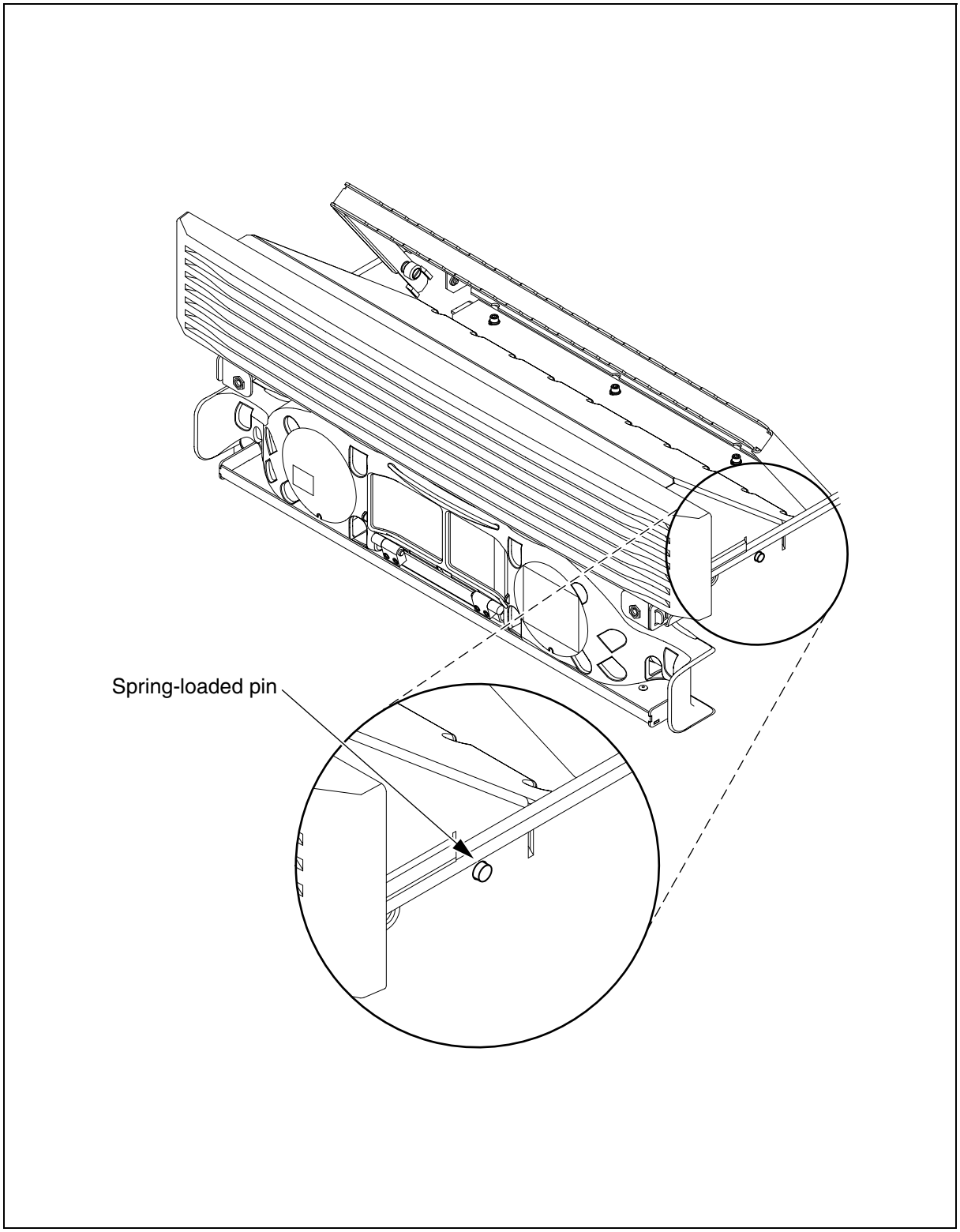
Fan power cable

EX1005p



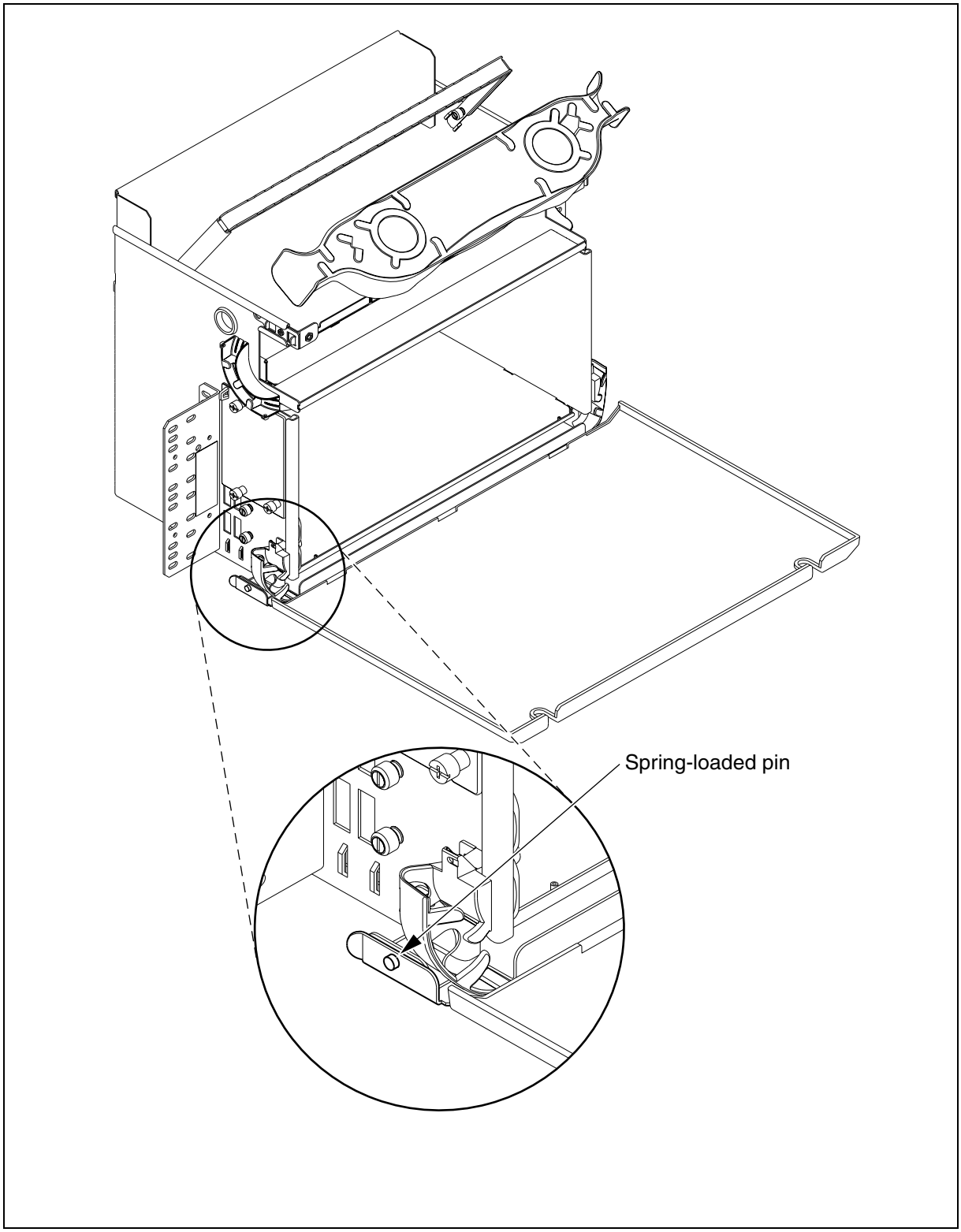
Installing and removing the grill/air deflector

EX0828t



Installing and removing the shelf front cover

EX0829t



Procedure 3-23
Replacing a cooling unit fan module

Use this procedure to replace a cooling unit fan module (NTN458HC).

Requirement

To perform this procedure, you must obtain one cooling unit fan module (NTN458HC) for cooling unit assembly (NTN458QA).

Step	Action
1	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

Opening the front cover

2	Rotate outward the two screws on the top, right and left of the front cover.
3	Open the cover completely.

Removing the grill/air deflector

4	Rotate the fiber storage tray toward the front of the shelf.
5	On the left side of the shelf, push in the spring-loaded pins of the grill/air deflector; at the same time pull the left end of the grill/air deflector just enough to disengage the pin from the shelf hole. See Installing and removing the grill/air deflector on page 3-65.
6	On the right side of the shelf, push in the spring-loaded pins of the grill/air deflector; at the same time pull the right end of the grill/air deflector just enough to disengage the pin from the shelf hole.
7	Pull out the grill/air deflector and store it in a safe place.
8	Rotate the fiber-optic cable tray forward.

Removing the cooling unit fan module

9	Hold the front and back of the damaged cooling unit fan module and pull the cooling unit fan module up until the retaining screw at the bottom front of the cooling unit is released.

Replacing the cooling unit fan module

10	Place a replacement cooling unit over the cooling unit opening in the top of the plenum so that the back of the cooling unit touches the vertical flange at the back of the opening.
11	Align the pins at the bottom of the new cooling unit with the four holes at the corners of the plenum opening.
12	Press the cooling unit down.
13	Insert and tighten the retaining screw.

—continued—

Procedure 3-23 (continued)
Replacing a cooling unit fan module

Step	Action
	Installing the grill/air deflector
14	Push in the spring-loaded pins on the sides of the grill/air deflector, insert the grill/air deflector into the shelf and release the pins. See Installing and removing the grill/air deflector on page 3-65.
15	Align the pins with the holes in the sides of the shelf and push the grill/air deflector until the pins enter the holes.
	Closing the front cover
16	Close the front cover and rotate inward the two screws on the top, right, and left of the front cover.

—end—

Procedure 3-24
Replacing the Universal cooling unit assembly

Requirements

To perform this procedure, you must obtain one Universal cooling unit assembly kit (NTN458QH) for each network element in a bay. The kit includes three Universal cooling unit fan modules, a plenum assembly, two power cables and one fan alarm cable.

CAUTION
Risk of circuit pack failure
This procedure must be completed within 15 minutes to ensure that the circuit packs do not overheat and fail while there are no fans on the network element.

Step	Action
1	Clear all other alarms first using the appropriate procedure. See Detailed procedures for active alarms on page 4-1.
2	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
	Opening the front cover
3	Rotate outward the two screws on the top, right and left of the front cover.
4	Open the cover completely.
	Removing the grill/air deflector
5	Rotate the fiber storage tray toward the front of the shelf.
6	On the left side of the shelf, push in the spring-loaded pins of the grill/air deflector; at the same time pull the left end of the grill/air deflector just enough to disengage the pin from the shelf hole. See Installing and removing the grill/air deflector on page 3-65.
7	On the right side of the shelf, push in the spring-loaded pins of the grill/air deflector; at the same time pull the right end of the grill/air deflector just enough to disengage the pin from the shelf hole.
8	Pull out the grill/air deflector and store it in a safe place.

—continued—

Procedure 3-24 (continued)
Replacing the Universal cooling unit assembly

Step	Action
	Removing the Universal cooling unit assembly from the shelf
9	Remove the fan assembly attaching screws. See Universal cooling unit assembly (NTN458QH) on page 3-72.
10	Disconnect the fan alarm cable connector from the LOAM. ***Note:*** The new cooling unit will reuse the fan alarm cable.
11	Disconnect the fan power cable connectors from power module A and power module B.
12	Lift out the cooling unit assembly from the top of the shelf.
	Installing the new Universal cooling unit assembly
13	Position the cooling unit assembly in respect to the front of the shelf.
14	Hold the Universal cooling unit assembly and pass the fan alarm cable and power cables through the hole on the left side of the shelf.
15	Set down the cooling unit assembly on the top of the shelf.
16	Plug the cooling fan power cables into the power modules A and B. See Power cable connections on page 3-71 and Fan power cable on page 3-64.
17	Attach the cooling unit assembly to the shelf using two attaching screws provided. See Universal cooling unit assembly (NTN458QH) on page 3-72.
	Connecting the alarm cable to the LOAM connectors
18	Plug the alarm cable into the alarm connector of the LOAM on the left side of the shelf. See Universal cooling unit plenum on page 3-74 and Fan alarm cable on page 3-64.
19	Use a tie wrap to attach the alarm and power cables to the cable tie lances on the left edge of the shelf.
	Connecting the cooling fan power cables
20	Ensure the green LED in front of each fan module is ON.

—continued—

Procedure 3-24 (continued)
Replacing the Universal cooling unit assembly

Step	Action

Installing the grill/air deflector

21 Push in the spring-loaded pins on the sides of the grill/air deflector, insert the grill/air deflector into the shelf and release the pins. See Installing and removing the grill/air deflector on page 3-65.

22 Align the pins with the holes in the sides of the shelf and push the grill/air deflector until the pins enter the holes.

Closing the front cover

23 Close the front cover and rotate inward the two screws on the top, right, and left of the front cover.

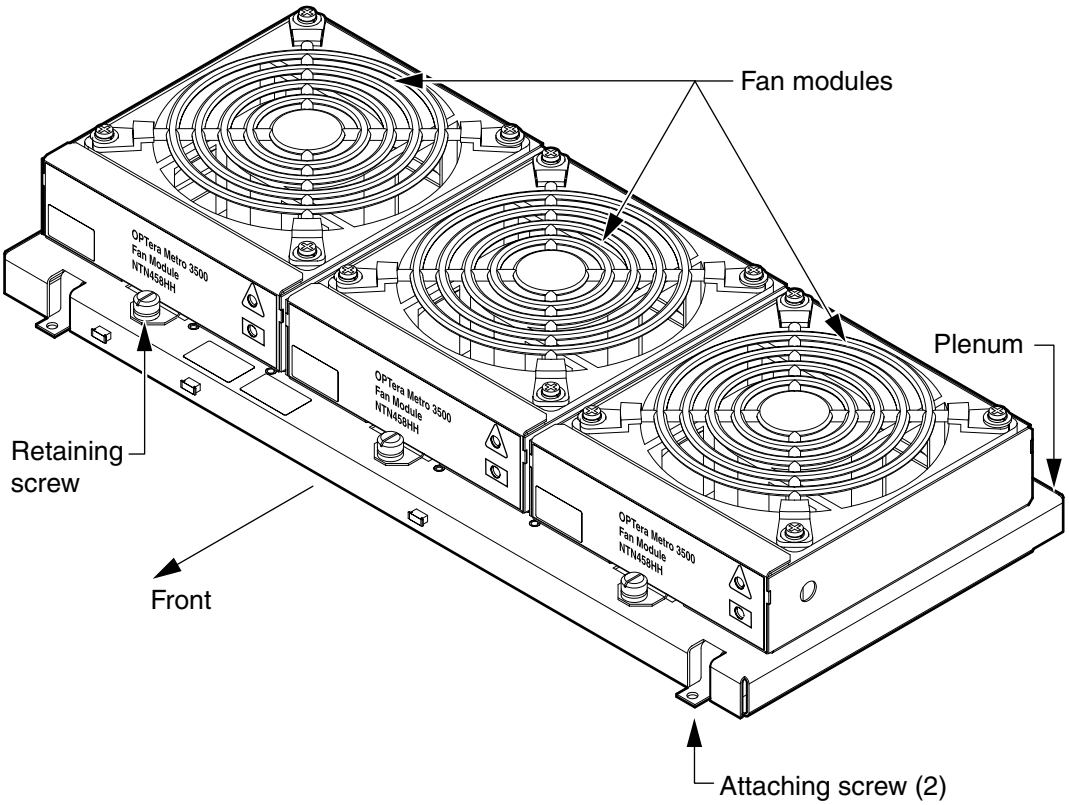
—end—

Power cable connections

Power cable lead	Power supply
Red	-48V A
White/red strip	A return
Red/blue strip	-48V B
White/blue strip	B return

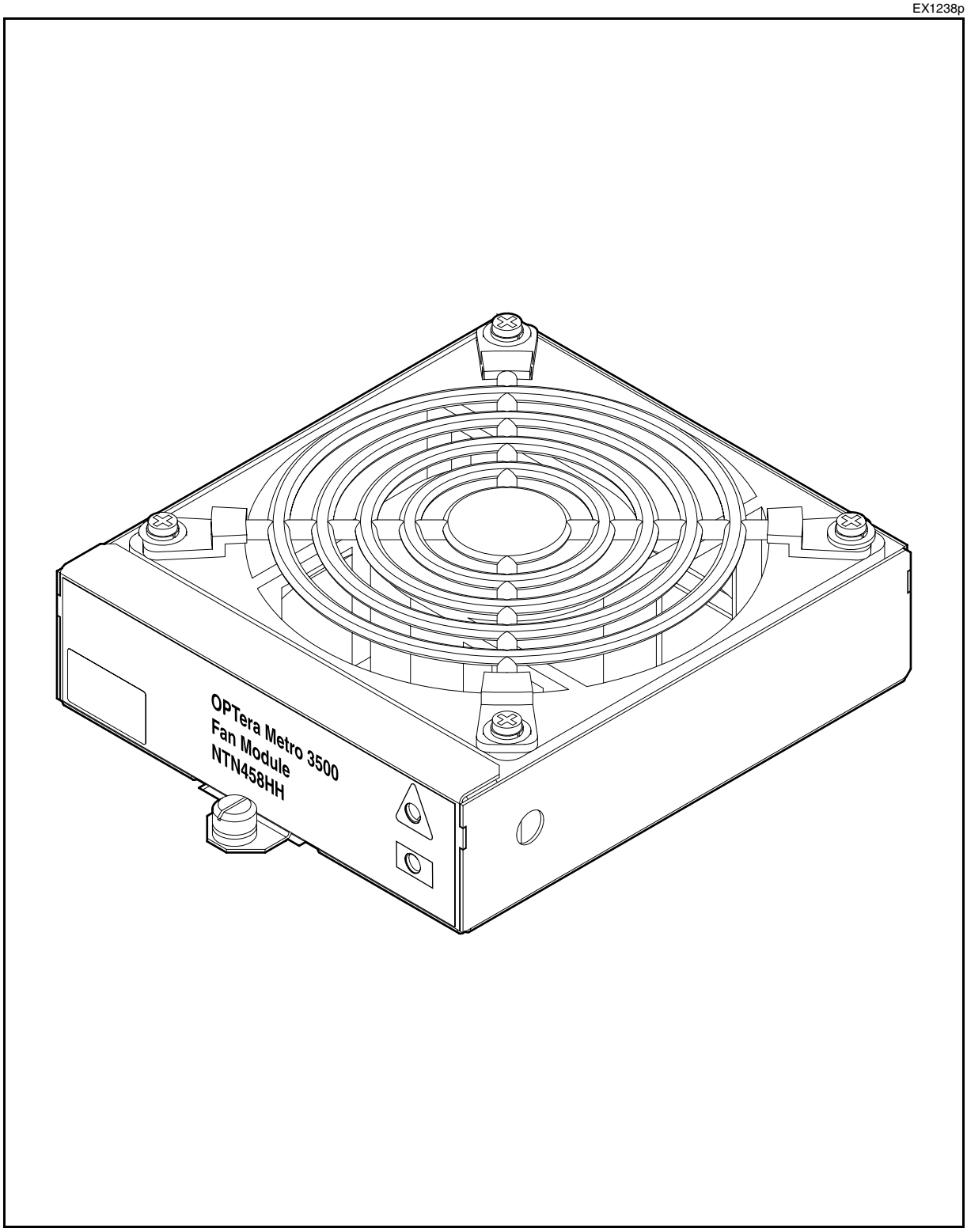
Universal cooling unit assembly (NTN458QH)

EX1239p



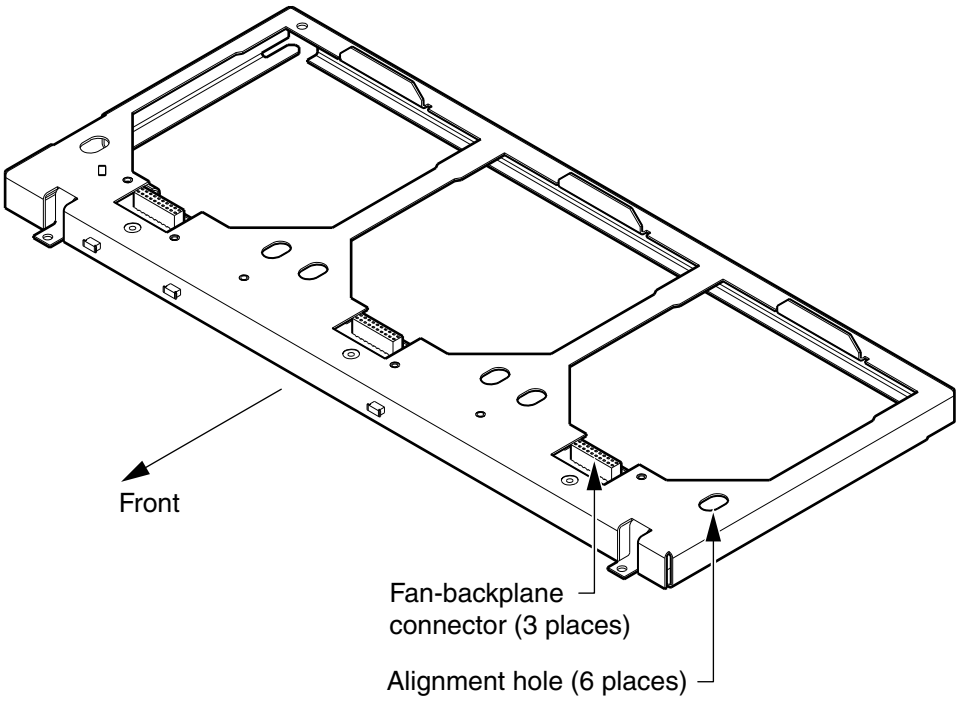
Universal cooling unit fan module (NTN458HH)

EX1238p



Universal cooling unit plenum

EX1240p



Procedure 3-25
Replacing a Universal cooling unit fan module

Use this procedure to replace a Universal cooling unit fan module (NTN458HH).

Requirement

To perform this procedure, you must obtain one Universal cooling unit fan module (NTN458HH) for Universal cooling unit assembly (NTN458QH).

Step	Action
1	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

Opening the front cover

2	Rotate outward the two screws on the top, right and left of the front cover.
3	Open the cover completely.

Removing the grill/air deflector

4	Rotate the fiber storage tray toward the front of the shelf.
5	On the left side of the shelf, push in the spring-loaded pins of the grill/air deflector; at the same time pull the left end of the grill/air deflector just enough to disengage the pin from the shelf hole. See Installing and removing the grill/air deflector on page 3-65.
6	On the right side of the shelf, push in the spring-loaded pins of the grill/air deflector; at the same time pull the right end of the grill/air deflector just enough to disengage the pin from the shelf hole.
7	Pull out the grill/air deflector and store it in a safe place.
8	Rotate the fiber-optic cable tray forward.

Removing the Universal cooling unit fan module

9	Untighten the retaining screw at the front of the module. Hold the back of the damaged Universal cooling unit fan module and pull front of the Universal cooling unit fan module up until the unit is released.

Replacing the cooling unit fan module

10	Place a replacement cooling unit over the cooling unit opening in the top of the plenum so that the back of the cooling unit touches the vertical flange at the back of the opening.
11	Align the pins at the bottom of the new cooling unit with the two holes at the front corners of the plenum opening.
12	Press the cooling unit down.
13	Insert and tighten the retaining screw.

—continued—

Procedure 3-25 (continued)
Replacing a Universal cooling unit fan module

Step	Action
	Installing the grill/air deflector
14	Push in the spring-loaded pins on the sides of the grill/air deflector, insert the grill/air deflector into the shelf and release the pins. See Installing and removing the grill/air deflector on page 3-65.
15	Align the pins with the holes in the sides of the shelf and push the grill/air deflector until the pins enter the holes.
	Closing the front cover
16	Close the front cover and rotate inward the two screws on the top, right, and left of the front cover.

—end—

Procedure 3-26
Replacing the power A and power B modules

Use this procedure to replace the power A and power B modules on the network element.

Requirements

To perform this procedure, you must

- obtain a replacement power module
- observe all safety requirements described in Safety requirements on page 3-3

Step	Action

Replacing the power A module

1 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

2 Switch the power A breaker of the network element to off.

Note 1: When the power A breaker is turned off the power B module becomes the sole source.

Note 2: When the power A breaker is turned off, the Power Failure - A alarm is raised. This alarm clears when the breaker is turned on.
See Power failure - A or Power failure - B on page 5-135.

3 Disconnect the -48V and Return power cables from the left side of the power A module.

4 From the left side of the shelf, below the LOAM, remove the screw that secures the power module A to the shelf.

5 From the left side of the power A module pull the power module out of the shelf.

6

DANGER
Risk of electrical shock and short circuit
Ensure there is no chance of any conductive material coming in contact with the circuit board on the right side of the power modules. Electrical shock or short circuit can result when the power is returned.

Slide the new power A module into the shelf.

7 Insert and tighten the screw on the left side of the shelf, below the LOAM, to secure the power module to the shelf.

8 Connect the -48V and Return power cables to the power A module and switch the breaker to the on position.

—continued—

Procedure 3-26 (continued)
Replacing the power A and power B modules

Step	Action

Replacing the power B module

9 Switch the power B breaker of the network element to off.

Note: When the power B breaker is turned off, the Power Failure - B alarm is raised. This alarm clears when the breaker is turned on.
See Power failure - A or Power failure - B on page 5-135.

10 Disconnect the -48V and Return power cables from the left side of the power B module.

11 From the left side of the shelf, below the LOAM, remove the screw that secures the power module B to the shelf.

12 From the left side of the power B module pull the power module out of the shelf.

13

DANGER
Risk of electrical shock and short circuit
Ensure there is no chance of any conductive material coming in contact with the pins on the right side of the power modules. Electrical shock or short circuit can result when the power is returned.

Slide the new power B module into the shelf.

14 Insert and tighten the screw on the left side of the shelf, below the LOAM, to secure the power module to the shelf.

15 Connect the -48V and Return power cable to the power B module and switch the breaker to the on position.

—end—

Procedure 3-27
Replacing the LIF and/or the LOAM

Use this procedure to replace the left interface (LIF), the left OAM (LOAM), or both on the network element without removing traffic from the network element.

Note: You should perform this procedure only during a maintenance window.

Requirements

To perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- obtain a replacement LIF and/or a replacement LOAM (as required)
- observe all safety requirements described in Safety requirements on page 3-3 and in *Installation*, 323-1059-201

Step	Action
1	Log in to the network element using a direct cable connection. See 323-1059-302, Logging in to a network element using a direct cable connection on page 2-32.
2	Take note of all active alarms on the network element. See Retrieving active alarms for a network element on page 2-3.
3	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
4	Disconnect all cables and remove all the wire-wrap pins from the LOAM. ***Note:*** Several alarms are raised when you disconnect the cables from the LOAM. The alarms raised depend on the LOAM connections and can include the following: • "Fan missing" alarms raised (although the fans should continue to function correctly) • loss of BITS timing (IN and OUT) • loss of visibility to network elements through the LAN ports • loss of surveillance of environmental and office alarms • loss of surveillance through TBOS • loss of X.25 connectivity • loss of RS-232 connectivity though the LOAM. RS-232 connectivity through the shelf processor is available.
5	Unscrew the two hinged screws and the two unit mount screws on the LOAM. See LOAM connectors on page 3-81.

—continued—

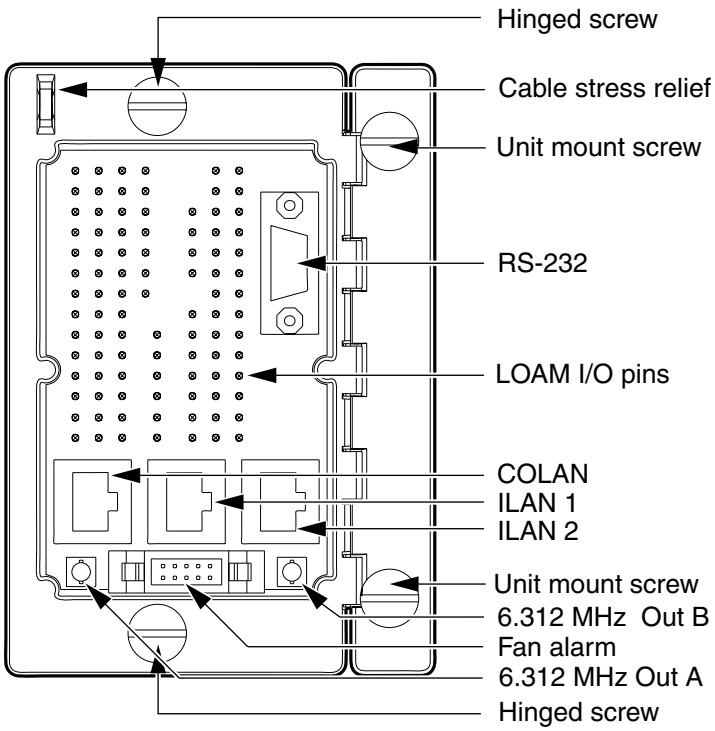
Procedure 3-27 (continued)
Replacing the LIF and/or the LOAM

Step	Action
6	Unplug the LOAM from the LIF.
7	**If** you are replacing the — **Then** go to LOAM and the LIF — step 8 LOAM only — step 14
8	Unlatch and lift the LIF faceplate until it it horizontal.
9	Hold the LIF and pull the circuit pack forward until it disengages from the backplane.
10	Pull the circuit pack out of the slot.
11	Lift the faceplate of the replacement LIF until it is horizontal.
12	Carefully guide the back end of the circuit pack into subslot 1 in slot 1. Make sure that the top and bottom edges of the circuit pack enter the slot guides.
13	Carefully close and latch the LIF faceplate until the connector at the back of the circuit pack mates with the backplane.
14	Insert the LOAM connector into the socket on the LIF.
15	Fasten the LOAM to the LIF with the two unit mount screws on the LOAM. ***Note:*** Do not overtighten the screws.
16	Reconnect all the cables and wire-wrap pins to the LOAM.
17	Retrieve the active alarms on the network element. See Retrieving active alarms for a network element on page 2-3. If any alarms are raised as a result of the LIF replacement, check the connection between the LIF and the LOAM.
18	Test the connection by logging in to the network element through the COLAN port or the RS-232 port on the LOAM. See 323-1059-302, Starting a remote login session from an OPTera Metro 3500 network element on page 2-17 or Connecting a terminal or modem to the shelf in *Installation*, 323-1059-201.
19	Tighten the remaining screws on the LOAM.

—end—

LOAM connectors

EX0792p



Procedure 3-28
Replacing the DSM-OAM adapter module

Use this procedure to replace the OAM adapter module on the DS1 service module (DSM).

Requirements

To perform this procedure, you must

- ensure the DSM is powered down
- obtain a replacement DSM-OAM adapter module
- observe all safety requirements described in Safety requirements on page 3-3

Step	Action
1	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	**CAUTION** **Risk of traffic loss** All DS1 traffic on the DSM is lost if the traffic is not rerouted to another DSM. Perform an in-service traffic rollover for all traffic on both DSM DS1x84 TM circuit packs to the circuit packs of another DSM. See 323-1059-320, Procedures for in-service traffic rollovers in a linear configuration on page 2-1, Procedures for in-service traffic rollovers in UPSR networks on page 3-2, or Procedures for in-service traffic rollovers in a BLSR on page 4-1.
3	Switch the Power A and Power B breakers of the DSM to off.
4	Switch the appropriate breaker to off at the BIP.
5	Untighten the two screws on the front of the DSM cover.
6	Open the DSM cover.
7	Disconnect the power cables from the DSM-OAM adapter module.
8	Remove the alarm control cable from the wire wrap pins of the DSM-OAM adapter module. The alarm control cable can be connected to the environmental I/O and OAM alarm pins. For a description of the wire pin assignments, refer to the OAM interface matrix pinout in *Installation*, 323-1059-201.
9	Disconnect the communication cables including the intershelf LAN and RS-232 cables, if present.

—continued—

Procedure 3-28 (continued)
Replacing the DSM-OAM adapter module

Step	Action
10	From the back of the DSM-OAM adapter module, unscrew the two screws that secure the module to the DSM.
11	Lift the DSM-OAM adapter module off the DSM.
12	Position the DSM-OAM adapter module on top of the DSM and tighten the two screws to secure the module in place.
13	Connect the power cable to the DSM-OAM adapter module.
14	Connect the alarm control and communication cables. For more information on connecting those cables, see *Installation*, 323-1059-201.
15	Switch the Power A breakers and the Power B breakers of the DSM to the on position.
16	Switch the BIP breaker to the on position.
17	Perform an in-service traffic rollover to return the traffic to the DSM.
18	Close the DSM cover.
19	Tighten the two screws on the front of the DSM cover.

—end—

Procedure 3-29
Replacing the DS1-I/O module on the DS1 service module

Use this procedure to replace a DS1-I/O module on the DS1 service module (DSM).

CAUTION
Risk of traffic loss
All traffic on this DS1 I/O module is lost when you remove it from the DSM. Perform this procedure as quickly as possible to minimize traffic loss.

Requirements

To perform this procedure, you must

- obtain a replacement DS1-I/O module
- observe all safety requirements described in Safety requirements on page 3-3

Step	Action
1	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Open the DSM front cover door.
3	Ensure the DS1 cables are disconnected from the DS1-I/O module in the DSM.
4	Pull the two spring-loaded brackets on top of the DS1-I/O apart and disconnect the cables from the DS1-I/O.
5	From the front of the DSM, unscrew the two thumbscrews that secure the DS1-I/O module in the DSM.
6	Pull the DS1-I/O module from the DSM.
7	Insert the replacement DS1-I/O module.
8	Reconnect the cables that you diconnected in step 3.
9	Tighten the two thumbscrews to secure the module in place.

—end—

Procedure 3-30
Replacing the shelf air filter

Requirement

To perform this procedure, you must obtain one new shelf air filter.

Note: The shelf air filter must be replaced every six months.

Step	Action
1	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

Removing the shelf front cover

2	Rotate inward the two screws on the top, right, and left of the front cover.
3	Open the cover completely.
4	Push in the spring-loaded pins on the bottom left of the front cover. At the same time pull the left top of the cover just enough to disengage the pin from the shelf hole.
5	Push in the spring-loaded pins on the bottom right of the front cover. At the same time pull the right top of the cover just enough to disengage the pin from the shelf hole.
6	Pull out the front cover and store it in a safe place.

Removing the grill/air deflector

7	Rotate the fiber storage tray toward the front of the shelf.
8	On the left side of the shelf, push in the spring-loaded pins of the grill/air deflector; at the same time pull the left end of the grill/air deflector just enough to disengage the pin from the shelf hole. See Installing and removing the grill/air deflector on page 3-65.
9	On the right side of the shelf, push in the spring-loaded pins of the grill/air deflector; at the same time pull the right end of the grill/air deflector just enough to disengage the pin from the shelf hole.
10	Pull out the grill/air deflector and store it in a safe place.
11	Rotate the fiber-optic cable tray forward.

Removing the shelf air filter

12	Locate the shelf air filter. See Installing the shelf air filter on page 3-87.
13	Press the air filter towards the front of the shelf and pull the back of the air filter down and out of the shelf.

—continued—

Procedure 3-30 (continued)
Replacing the shelf air filter

Step	Action

Installing the shelf air filter

14 Insert the new air filter into the retaining springs on the shelf and push the air filter into position. See Installing the shelf air filter on page 3-87.

Note: Ensure the grill side of the air filter faces out.

Installing the grill/air deflector

15 Push in the spring-loaded pins on the sides of the grill/air deflector, insert the grill/air deflector into the shelf and release the pins. See Installing and removing the grill/air deflector on page 3-65.

16 Align the pins with the holes in the sides of the shelf and push the grill/air deflector until the pins enter the holes.

Installing the shelf front cover

17 Push in the spring-loaded pins on each side of the front cover.

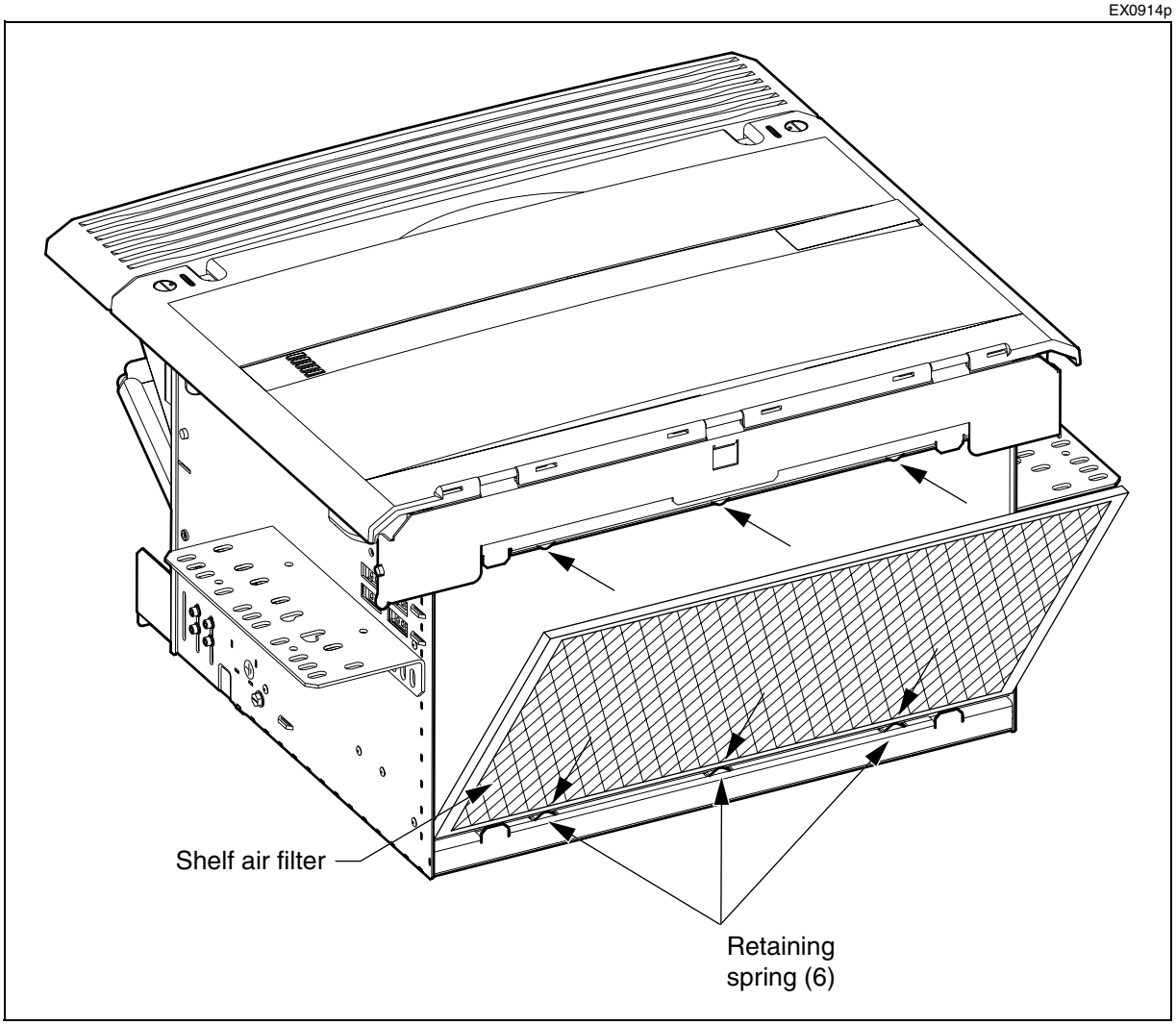
18 Align the pins with the holes in the sides of the shelf, push the front cover into the shelf, and release the pins. Push the front cover gently until the spring-loaded pins enter the holes.

19 Close the front cover and rotate outward the two screws on the top, right, and left of the front cover.

—end—

Installing the shelf air filter

EX0914p



Procedure 3-31
Replacing the I/O modules on the NTN476AA or NTN476DA shelf

Use this procedure to replace one of the following front I/O modules on the NTN476AA or NTN476DA shelf:

- DS1 1-28
- DS1 29-56
- DS1 29-84
- BNC 12-port
- 8xRJ-45

CAUTION
Risk of traffic loss
All traffic on the I/O module is lost when you remove it from the shelf. Perform this procedure as quickly as possible to minimize traffic loss.

Requirements

To perform this procedure, you must

- obtain a replacement I/O module as required
- observe all safety requirements described in Safety requirements on page 3-3

Step	Action
1	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Record the position of each cable on the I/O module to facilitate reconnection of the cables.
3	Add a terminal loopback on each facility for the affected circuit pack, individually. See 323-1059-222, Provisioning a software loopback on page 2-56.
4	Select the next facility and add a terminal loopback until all the facilities on the affected circuit pack have loopbacks.
5	Disconnect the cables on the I/O module.
6	Lift the lock/eject lever on the I/O module and remove the module.

—continued—

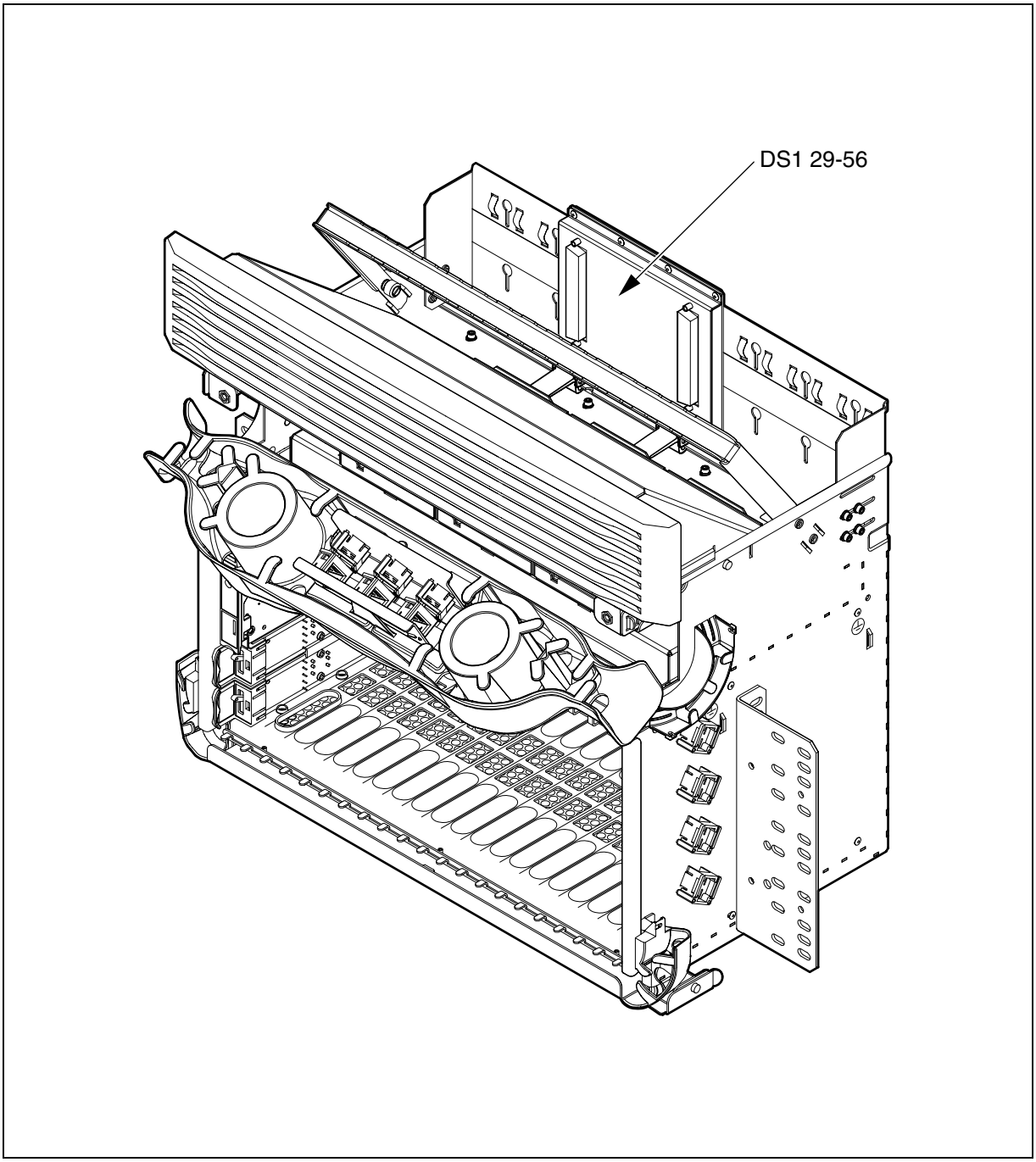
Procedure 3-31 (continued)
Replacing the I/O modules on the NTN476AA or NTN476DA shelf

Step	Action
7	Install the new module. See Installing an I/O module on the NTN476DA shelf on page 3-90. **a.** Loosen the thumbscrew shoulder rivet on the I/O module. **b.** Position the I/O module so that the connectors face forward. **c.** Insert the thumbscrew shoulder rivet on the back of the I/O module into the keyhole slots on the back top of the shelf. **d.** Push the module down until the locking tabs lock into place on the backplane. **e.** Lock the module in position by pushing down the lock/eject lever; push until the lever latches on the base of the backplane connector. **f.** Tighten the thumbscrews.
8	Reconnect the cables to the module as they were connected before the replacement.
9	Release the loopback on each of the facilities, individually. See 323-1059-222, Releasing a software loopback on page 2-58.
10	Select the next facility and release the loopback until all the loopbacks have been released.
11	Put each facility in service, individually. See 323-1059-350, Changing a facility state to In Service (IS) on page 2-26.

—end—

Installing an I/O module on the NTN476DA shelf

EX0889t



Procedure 3-32
Replacing the I/O modules on the NTN476AH Universal shelf

Use this procedure to replace one of the following front or rear I/O module on the NTN476AH Universal shelf:

- DS1 1-28
- DS1 29-56
- DS1 29-84
- BNC 12-port
- 8xRJ-45

CAUTION
Risk of traffic loss
All traffic on the I/O module is lost when you remove it from the shelf. Perform this procedure as quickly as possible to minimize traffic loss.

Requirements

To perform this procedure, you must

- obtain a replacement I/O module as required
- observe all safety requirements described in Safety requirements on page 3-3

Step	Action
1	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Record the position of each cable on the I/O module to facilitate reconnection of the cables.
3	Add a terminal loopback on each facility for the affected circuit pack, individually. See 323-1059-222, Provisioning a software loopback on page 2-56.
4	Select the next facility and add a terminal loopback until all the facilities on the affected circuit pack have loopbacks.
5	Disconnect the cables on the I/O module.
6	Pull the lock/eject lever towards the front of the shelf while lifting the lock/eject lever to remove the module.

—continued—

Procedure 3-32 (continued)
Replacing the I/O modules on the NTN476AH Universal shelf

Step	Action
7	Install the new front or rear I/O module. See Installing an I/O module on the NTN476AH Universal shelf on page 3-93.
	a. Ensure the lock/eject lever on the I/O module is in the up position.
	b. Identify the mating connector on the shelf.

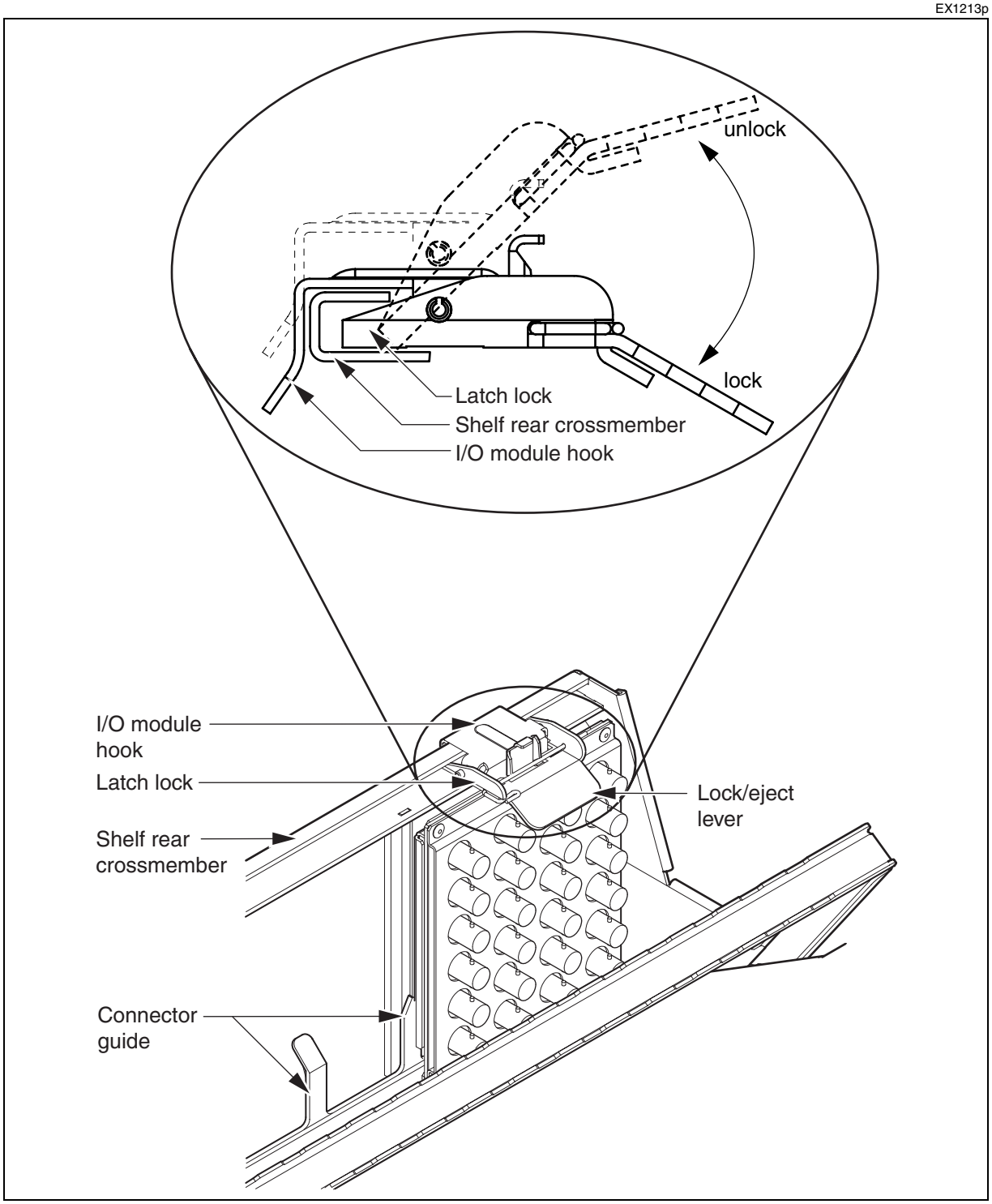
If you are installing the	**Then**
front I/O module	go to substep c
rear I/O module	go to substep d

	c. From the front of the shelf, align the alignment tabs on the I/O module with the connector guides on the shelf. Go to substep e.
	d. From the back of the shelf, align the alignment tabs on the I/O module with the connector guides on the shelf.
	e. Hang the I/O module hook on the shelf rear crossmember and insert the latch lock into the rear crossmember slot.
	f. Push the lock/eject lever down to connect and attach the I/O module to the shelf.
8	Reconnect the cables to the module as they were connected before the replacement.
9	Release the loopback on each of the facilities, individually. See 323-1059-222, Releasing a software loopback on page 2-58.
10	Select the next facility and release the loopback until all the loopbacks have been released.
11	Put each facility in service, individually. See 323-1059-350, Changing a facility state to In Service (IS) on page 2-26.

—end—

Installing an I/O module on the NTN476AH Universal shelf

EX1213p



Procedure 3-33
Attaching or detaching a circuit pack from the back plane

This is not a stand-alone procedure.

Requirements

To perform this procedure, you must

- use an account with level 1 or higher user privilege code (UPC)
- obtain a replacement circuit pack
- if the circuit pack is an OC-48 ER, OC-48 ELR, OC-48 STS, or OC-192 circuit pack, have an optical power meter with the same optical connectors as the circuit pack
- observe all safety requirements described in Safety requirements on page 3-3

Step	Action
1	Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Select Active Alarms from the Faults drop-down menu to retrieve alarms.
3	**If** you are / **Then** go to replacing a circuit pack from the back plane — step 4 detaching a circuit pack from the back plane — step 4 attaching a circuit pack from the back plane — step 7

Detaching the circuit pack from the back plane

4	Pull the locking levers of the failed circuit pack to unlock and detach the circuit pack from the backplane. The locking levers are at each end of the circuit pack.
5	Remove the circuit pack from the slot by pulling on the locking levers. Place the circuit pack in a static protection envelope. ***Note 1:*** The Circuit Pack Missing alarm is raised, except when you are replacing the shelf processor or the LIF. ***Note 2:*** The Circuit Pack Missing alarm is cleared when the replacement circuit pack is inserted in to the shelf and the card software is fully initialized. ***Note 3:*** The Circuit Pack Missing alarm masks any alarms raised against the circuit pack you are replacing.

—continued—

Procedure 3-33 (continued)
Attaching or detaching a circuit pack from the back plane

Step	Action

Note 4: If OPE traffic is present, an STS Rx AIS,STS3c Rx AIS, or STS12c Rx AIS minor alarm is raised at adjacent network elements containing OPE circuit packs.

Note 5: If you are replacing the LIF, then the Fan Missing and the ILAN Port Failure alarms are raised. Also, the Power A and Power B slots are displayed as “Empty” in the inventory. Traffic is not affected.

6

If	Then
you also want to attach a circuit pack	go to step 7
you wanted to detach a circuit pack only	you have completed this procedure

Attaching a circuit pack on the back plane

7

If you are	**Then** go to
attaching an optical interface circuit pack	step 8
not attaching an optical interface circuit pack	step 17

8

If the optical interface circuit pack you are attaching	**Then** go to
is not equipped with any optical connectors but optical connectors are required	step 9
is equipped with optical connectors of the wrong type	step 9
is equipped with optical connectors of the right type	step 17
does not require optical connectors	step 17

9 Open the lower latch of the circuit pack.

10 On the side of the circuit pack faceplate, insert the end of a flat-head screwdriver into the slotted groove between the adapter retainer and the faceplate.

11 Twist the screwdriver until the adapter retainer becomes loosened.

12 Slide the adapter retainer downward and away from the circuit pack.

13 If your circuit pack is currently equipped with connectors that do not match your fiber connector type, remove the connectors from the circuit pack’s fiber-optic connectors by individually pulling the connectors downward and away from the circuit pack.

14 Insert the required type of connectors into each fiber-optic connector of the circuit pack.

a. With one hand, hold the internal side (circuit board side) of the fiber-optic connector to brace the fiber and plug.

b. With your other hand, insert the connector adapter into the external side (faceplate side) of the fiber-optic connector.

—continued—

Procedure 3-33 (continued)
Attaching or detaching a circuit pack from the back plane

Step	Action
15	Repeat step 14 for all connectors.
16	Re-attach the adapter retainer to the circuit pack by sliding it upward and into place on the faceplate. ***Note 1:*** Firmly snap the adapter retainer into place. ***Note 2:*** The connectors should slide through the holes of the adapter retainer as you slide the retainer into place.
17	Lift the replacement circuit pack by the edges of the faceplate where the locking levers are located and insert it carefully into the slot guide grooves. ***Note 1:*** The circuit pack is right side up when the printed labels on the front faceplate are right side up. ***Note 2:*** All the LEDs on the circuit pack illuminate when you insert the circuit pack into the slot. The top Status LED turns red and the next, Status LED turns green. These LEDs indicate that the optical interface circuit pack software is initializing. ***Note 3:*** Software initialization time is complete when the top Status LED turns yellow. If the top Status LED remains red, the optical interface circuit pack is damaged and must be returned to Nortel Networks. ***Note 4:*** Do not wait for software initialization time to be complete. Install the next optical interface circuit pack.
18	Push the circuit pack all the way in.
19	Lock the circuit pack into its slot by pushing the locking levers toward the faceplate at the same time. ***Note:*** Do not force the locking levers. If the levers do not close properly, remove the circuit pack and examine the connectors on the back of the circuit pack. Look for bent pins or damage to the module or shelf keys. The shelf keys are the colored inserts near the top and bottom of the shelf connector.
20	Wait 10 minutes or until the circuit pack reboots. ***Note:*** If you are replacing an OPE circuit pack, it can take up to 13 minutes for the circuit pack to autoprovision.
21	For each optical interface circuit pack you installed, perform step 22.
22	**If** the optical interface circuit pack you installed — **Then** go to is an ER or ELR circuit pack — step 23 is not an ER or ELR circuit pack — step 25
23	Ensure you are logged into the network element in which you installed the optical interface circuit pack. See login procedures in *Security and Administration*, 323-1059-302.

—continued—

Procedure 3-33 (continued)
Attaching or detaching a circuit pack from the back plane

Step	Action
	Note: Before continuing this procedure, you must ensure the circuit pack is receiving a signal. Measure the receive power to ensure that it is within the correct range for the circuit pack.
24	In Site Manager, select this network element in the navigation tree.
25	Select Facility PM Thresholds in the Performance menu.
26	In the Type box, select the line rate of your ER or ELR circuit pack.
27	In the Facility box, select the circuit pack you installed.
28	In the Location box, select Near end.
29	In the Direction box, select Receive.
30	Click Retrieve.
31	In the Monitor Type column of the PM Thresholds list, select OPR.
32	Click Edit.
33	In the Edit Threshold Values dialog box, under Physical PM, select Reset baseline power level.
34	Click OK.

—end—

Alarm clearing A-K

Detailed procedures for active alarms

A

B

C

D

E

F

I

L

P

R

S

Alarm hierarchies

Alarm severity

The levels of severity for alarms are critical (C), major (M), and minor (m). Alarm reports always contain a notification code that identifies the alarm severity, or the code CL to indicate that the fault has been cleared. The W code indicates a warning. The A code indicates an alert.

Critical alarms (C)

Critical alarms are the most severe. Critical alarms always indicate a service-affecting fault. For example, unprotected facility losses and unprotected facility-carrying equipment failures raise critical alarms.

Major alarms (M)

Major alarms are less severe than critical alarms but can be service-affecting or non-service-affecting. Major alarms are raised when something has an effect on a low-speed facility. For example, a major alarm is raised when tributary signals fail or unprotected provisioned circuit packs are missing.

Minor alarms (m)

Minor alarms are less severe but can be service-affecting or non-service-affecting. For example, a non-service-affecting minor alarm is raised when a protected circuit fails. However, an STS Rx AIS service-affecting minor alarm raises when a 1+1 protected linear configuration does not have protection available.

Cleared alarm notification (CL)

The cleared notification code indicates that the fault no longer exists. Two seconds after a fault clears, a cleared alarm report goes to all active sessions. The automatic output cache stores the cleared alarm reports.

Warning (W)

Warning alarms are less severe than minor alarms and are not accompanied by an alarm clearing procedure. A Warning is an indication that a problem may exist on the network element which could eventually escalate into an alarm of higher severity. As well, some alarms have a Warning severity rather than a minor severity when the affected traffic is protected.

Alert (A)

Threshold-crossing alerts are less severe than alarms. An alert can indicate that the threshold crossed does not affect service but requires further investigation.

Safety requirements

CAUTION
Loss of functionality
When you replace a circuit pack, the circuit pack can take up to 5 minutes to auto-upgrade. If you remove the circuit pack before the auto-upgrade process is complete, the circuit pack does not function properly.

CAUTION
Loss of functionality
All system functionality is lost when the shelf processor is removed. Only traffic is maintained.

CAUTION
Risk of circuit pack damage
Avoid touching any components on the printed circuit board. Electrostatic discharge can damage electrostatic-sensitive devices. Always connect yourself to ground before handling any circuit pack.

CAUTION
Risk of circuit pack damage
Do not force a circuit pack all the way to the back of a slot if it resists insertion. Before installing any of the circuit packs, make sure you know the detailed procedure for insertion of circuit packs.

CAUTION
Risk of service interruption
Electrostatic discharge can corrupt traffic. Severe discharges can cause temporary service interruptions.

CAUTION
Risk of service interruption
If you use radio communication devices like cellular telephones, service interruptions can occur. For example, a North American cellular telephone of approximately 1 W must not be used within 30 cm of a system with an open service access front cover.

Procedure 4-1
Alarm and Event Throttling Active

Probable cause

This alarm is raised when the generation of alarms surpasses an average of four alarms per second over a ten minute period.

If this alarm is raised, other alarms can still be raised and retrieved, but their output to the alarm banner is stopped. Once this alarm is cleared, the output of other alarms to the alarm banner resumes.

Impact

Minor, non-service-affecting (m, NSA) alarm

Step	Action
1	Reduce the generation of alarms to less than four alarms per second.
2	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-2
All Provisioned VTs Rx AIS

Probable cause

This alarm is raised when the network element detects VT AIS (alarm indication signal) in all of the VT1.5 cross-connects provisioned within an STS. The Rx AIS indicates that an upstream network element cannot transmit the correct VT signal for some reason.

One of the following conditions at the far-end or pass-through network elements causes this alarm:

- incoming signal missing or errored (DS1 Rx Loss of Signal, Loss of Frame, or AIS) at the far end
- circuit pack failed (tributary) at the far end
- DS1 facility out of service at the far end
- STS Rx Unequipped alarm at a pass-through connection
- a test access session is in progress (no action is required if this is the cause)

Impact

Minor, service-affecting (m, SA) alarm, if on active path
Minor, non-service-affecting (m, NSA) alarm, if on inactive path

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- ensure that no STS Rx AIS, OC3 Rx line AIS, OC12 Rx line AIS, OC-48 Rx Line AIS, or OC-192 Rx Line AIS alarms are active in the network. Clear all alarms that can prevent the correct transmission of traffic before you start this procedure. The only alarms on the system should be VT Rx AIS or VT Rx RFI
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

  Note: Perform this procedure for all VT1.5 cross-connects provisioned within the STS.

—continued—

Procedure 4-2 (continued)
All Provisioned VTs Rx AIS

Step	Action
1	Retrieve alarms from the network element. See Retrieving active alarms for a network element on page 2-3.
2	**If** the circuit pack is / **Then** go to OCn — step 3 EC-1x3 or EC-1x12 — step 17
3	Verify if there are alarms of higher order from the alarm hierarchy. See Alarm hierarchies on page 4-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
4	Retrieve alarms to determine if the Rx AIS alarm cleared.
5	If the alarm does not clear, identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
6	Use the optical fiber connection information to identify the receive and transmit sites of the alarmed signal: • If the network element you identified at the remote end is not an OPTera Metro 3500 network element, go to step 7. • If the network element you identified at the remote end is an OPTera Metro 3500 network element, go to step 8.
7	If this network element is part of a mid-span meet and the remote network element is from another vendor, use the alarm system of the other vendor to find the problem.
8	Log in to the alarmed remote network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
9	Retrieve all alarms from the transmit end.
10	Clear the loss of signal, loss of frame, AIS, or circuit pack failed alarm on the DS1 circuit pack at the transmit end if they exist.
11	If the alarm does not clear, log in to each of the pass-through network elements and retrieve alarms. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
12	Look for a VT Rx Unequipped alarm for the optical interface on the VT path. If there is a VT Rx Unequipped alarm, clear the alarm. See VT Rx Unequipped on page 5-281.
13	Retrieve alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
14	If the alarm does not clear, verify the DS1 facility state at the transmit end, if applicable. If the DS1 facility is out of service, put it in service. See 323-1059-350, Changing a facility state to In Service (IS) on page 2-26.

—continued—

Procedure 4-2 (continued)
All Provisioned VTs Rx AIS

Step	Action
15	Retrieve alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
16	If the alarm does not clear, contact your next level of support or your Nortel Networks support group. You have completed this procedure.
17	Use an EC-1 test set to determine if a valid EC-1 signal is on the EC-1 cross-connect for that facility. • If the signal contains VT-AIS, the problem is in the EC-1 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. You have completed this procedure. • If the signal has no VT-AIS, go to the next step.
18	Operate a manual switch on the EC-1x3 or EC-1x12 circuit pack raising the alarm. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16.
19	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
20	Wait 30 seconds. If the alarm clears, the working EC-1x3 or EC-1x12 circuit pack is faulty. Replace the circuit pack that is detecting AIS. See Replacing the EC-1x3 or EC-1x12 circuit pack on page 3-32.
21	If the alarm does not clear, contact your next level of support or your Nortel Networks support group. **—end—**

Procedure 4-3
All Provisioned VTs Rx Excessive BIP Error Rate

Probable cause

This alarm is raised when all of the received VT1.5 signals in all VT1.5 cross-connects provisioned within an STS are degraded to the point where they are unusable.

One of the following conditions causes this alarm:

- excessive attenuation
- dirty optical fibers
- dirty connectors
- improper connector seating
- transmit laser degrade

Perform this procedure for all VT1.5 cross-connects provisioned within the STS.

CAUTION
Risk of outage
This procedure assumes that no OC-n, or STS-1 signal degrade alarms are active. Performing this procedure before clearing any OC-n signal degrade or signal failure alarms; or STS signal degrade or excessive BIP error rate alarms is not effective and can cause an outage.

Impact

Major, service-affecting (M, SA) alarm, if on active path
Minor, non-service-affecting (m, NSA) alarm, if on inactive path

Note: The status is major because the VT section is unprotected. The system cannot determine if path protection will be successful because that occurs where the path terminates. If the protection path is available, the path terminating network element switches to that path to protect traffic.

—continued—

Procedure 4-3 (continued)
All Provisioned VTs Rx Excessive BIP Error Rate

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- clear all higher level OC-n, or STS Rx Signal Degrade alarms, OC-n Rx Signal Failure or STS Rx Excessive BIP Error Rate alarms on the system
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Retrieve alarms from the network element. See Retrieving active alarms for a network element on page 2-3.
2	Verify if there are alarms of higher order from the alarm hierarchy. See Alarm hierarchies on page 4-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the Rx Excessive BIP Error Rate alarm cleared.
4	If the alarm does not clear, identify the optical interface circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
5	Use the optical fiber connection information to identify the transmit and the receive sites of the alarmed signal.
6	Retrieve all alarms from the transmit end: • If you retrieve alarms of higher order, clear the alarms by following the appropriate procedure. • If Rx RFI is the only alarm, go to the next step.
7	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

—continued—

Procedure 4-3 (continued)
All Provisioned VTs Rx Excessive BIP Error Rate

Step	Action

8

CAUTION
Risk of traffic loss
Ensure that the correct module is identified. Removing the wrong optical fiber drops all traffic on the local shelf.

DANGER
Risk of laser radiation exposure
Laser radiation is present on the optical fiber. Do not look into the optical fiber.

Remove the optical fiber from the circuit pack raising the alarm.

9 Measure the receive power using an optical power meter.

10 If the power is below the receiver sensitivity for this circuit pack, perform the following steps for All Provisioned VTs Rx excessive BIP error rate:

Note: For information about circuit pack technical specifications, see the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM.

a. Adjust the local attenuation, if equipped, to try to get the receive power above the receiver sensitivity level.

b. If you cannot get the receive power above the receiver sensitivity level, remove the Tx optical fiber from the far-end circuit pack.

c. Measure the transmit power at the far end.

d. If the power is above the launch power (minimum), the optical fiber attenuation is too high, the optical fiber connections are dirty or the optical fiber is damaged. Use your company procedure to determine the location of the problem.

—continued—

Procedure 4-3 (continued)
All Provisioned VTs Rx Excessive BIP Error Rate

Step	Action
	e. If the power is below the launch power (minimum), replace the required circuit pack at the transmit end. See Replacing an optical interface circuit pack in a linear system on page 3-34, Replacing an optical interface circuit pack in a UPSR on page 3-38, or Replacing an OC-48 or OC-192 optical interface circuit pack in a BLSR on page 3-41.
	f. Retrieve all alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
	g. If the alarm does not clear, replace the optical interface circuit pack reporting the alarm.
	h. Clean and reattach both optical fibers. See *Installation*, 323-1059-201.Retrieve all alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
	i. If the alarm does not clear, contact your next level of support or your Nortel Networks support group.
11	If the power is above the receiver sensitivity for this circuit pack, clean all connections at both ends of the optical fiber link following your company standards and reattach the optical fibers.
12	If the alarm does not clear, clean the receive optical fibers and connections.
13	If the alarm does not clear, replace the circuit pack raising the alarm. See Replacing an optical interface circuit pack in a linear system on page 3-34, Replacing an optical interface circuit pack in a UPSR on page 3-38, or Replacing an OC-48 or OC-192 optical interface circuit pack in a BLSR on page 3-41.
14	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-4
All Provisioned VTs Rx Loss of Pointer

Probable cause

This alarm is raised when the network element detects an invalid pointer sequence in the VT line overhead for all VT1.5 cross-connects provisioned within an STS.

One of the following conditions causes this alarm:

- incoming EC-1 signal is improperly formatted
- improper network synchronization
- connection rate mismatch (for example, VT1.5 connects to STS-1)

  Note: Perform this procedure for all VT1.5 cross-connects provisioned within the STS.

- squelching in a BLSR

Impact

Major, service-affecting (M, SA) alarm, if on active path
Minor, non-service-affecting (m, NSA) alarm, if on inactive path

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Retrieve alarms from the network element. See Retrieving active alarms for a network element on page 2-3.
2	**If** the circuit pack is … **Then** go to …
	OCn — step 3
	EC-1x3 or EC-1x12 — step 16
3	Verify if there are alarms of higher order from the alarm hierarchy including the Traffic Squelched alarm. See Alarm hierarchies on page 4-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.

—continued—

Procedure 4-4 (continued)
All Provisioned VTs Rx Loss of Pointer

Step	Action
4	Retrieve alarms to determine if the Rx Loss of Pointer alarm cleared.
5	If the alarm does not clear, identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
6	Use the optical fiber connection information to identify the receive and transmit sites of the alarmed signal.
7	Log in to the remote network element at the transmit end. See 323-1059-302, Procedures for logging in to a network element on page 2-1. ***Note:*** If you cannot log in, you may have to travel to the remote site.
8	Retrieve alarms from the transmit end. See Retrieving active alarms for a network element on page 2-3.
9	Look for an alarm message for the optical interface circuit pack that connects to the original shelf: • Clear any higher order alarms using the appropriate procedures. • If there is Rx RFI, or if there are no alarms, go to the next step.
10	Retrieve alarms from the original network element to determine if the alarm cleared.
11	If the alarm does not clear, ensure that the network synchronization is correct. See 323-1051-310, Procedures for provisioning system synchronization on page 1-1.
12	Retrieve alarms from the original network element to determine if the alarm cleared.
13	If the alarm does not clear, verify the connection rate for the entire VT path to ensure that it is correct. See 323-1059-320, Procedures for end-to-end connection management on page 1-1.
14	Retrieve alarms from the original network element to determine if the alarm cleared.
15	If the alarm does not clear, contact your next level of support or your Nortel Networks support group. You have completed this procedure.
16	Use an EC-1 test set to determine if a valid EC-1 signal is on the EC-1 cross-connect for that facility. • If the signal has no valid pointer, the problem is in the EC-1 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. You have completed this procedure. • If the signal has a valid pointer, go to the next step.

—continued—

Procedure 4-4 (continued)
All Provisioned VTs Rx Loss of Pointer

Step	Action
17	Operate a manual switch on the EC-1x3 or EC-1x12 circuit pack raising the alarm. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16.
18	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
19	Wait 30 seconds. If the alarm clears, the working EC-1x3 or EC-1x12 circuit pack is faulty. Replace the circuit pack that is detecting loss of pointer. See Replacing the EC-1x3 or EC-1x12 circuit pack on page 3-32.
20	If the alarm does not clear, inspect the cabling around the input connector of the affected port. Look for misconnected, damaged or loose cables. Repair any damage.
21	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-5
All Provisioned VTs Rx RFI

Probable cause

This alarm is raised when the optical interface circuit pack circuit pack receives a signal with a remote fault indicator (RFI). The RFI is attached to the signal because of the following:

- an alarm of higher order raised on the remote network element
- the far end detects VT signal failures in all VT1.5 cross-connects provisioned within an STS

  Note: Perform this procedure for all VT1.5 cross-connects provisioned within the STS.

Impact

Minor, non-service-affecting (m, NSA) alarm

Note: The alarm status is minor, non-service-affecting (m, NSA) because it is a secondary alarm. Another fault causes the remote terminal to send this signal out. The problem that prevents the reception of the signal has a separate alarm raised.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- clear all alarms that can prevent the correct transmission of traffic before you start this procedure. The only alarms on the system could be VT Rx AIS or VT Rx RFI.
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

—continued—

Procedure 4-5 (continued)
All Provisioned VTs Rx RFI

Step	Action
1	Identify the circuit pack that raised the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Use the optical fiber connection information to identify the receive and transmit ends of the alarmed signal.
3	Log in to the network element at the transmit end. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
	Note: If you cannot log in, you may have to travel to the remote site.
4	Retrieve alarms from the transmit end.
5	Look for an alarm message for the optical interface circuit pack that connects to the original shelf. Clear any alarms using the appropriate procedure.
6	Retrieve alarms from the original network element to determine if the alarm cleared.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-6
All Provisioned VTs Rx Signal Degrade

Probable cause

This alarm is raised when the received signals on all VT1.5 cross-connects provisioned within an STS are significantly degraded.

One of the following conditions causes this alarm:

- excessive attenuation
- dirty optical fibers
- dirty connectors
- improper connector seating
- transmit laser degrade
- path signal degrade
- threshold set too high

Perform this procedure for all VT1.5 cross-connects provisioned within the STS-1.

CAUTION
Risk of outage
This procedure assumes that no OC-n, or STS signal degrade alarms are active. Performing this procedure before clearing any OC-n signal degrade or signal failure alarms; or STS signal degrade or excessive BIP error rate alarms is not effective and can cause an outage.

Impact

Minor, service-affecting (m, SA) alarm, if on active path
Minor, non-service-affecting (m, NSA) alarm, if on inactive path

Note: The alarm status is minor because the VT is degraded and not completely failed. If the protection path is available, the path terminating network element switches to that path to protect traffic.

—continued—

Procedure 4-6 (continued)
All Provisioned VTs Rx Signal Degrade

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- clear all higher level OC-n or STS Rx Signal Degrade alarms, OC-n Rx Signal Failure or STS Rx Excessive BIP Error Rate alarms on the system
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Retrieve alarms from the network element. See Retrieving active alarms for a network element on page 2-3.
2	Verify if there are alarms of higher order from the alarm hierarchy. See Alarm hierarchies on page 4-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the Rx Signal Degrade alarm cleared.
4	If the alarm does not clear, identify the optical interface circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
5	Use the optical fiber connection information to identify the transmit and the receive sites of the alarmed signal.
6	Retrieve all alarms from the transmit end: • If you retrieve alarms of higher order, clear the alarms by following the appropriate procedure. • If Rx RFI is the only alarm, go to the next step.
7	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

—continued—

Procedure 4-6 (continued)
All Provisioned VTs Rx Signal Degrade

Step	Action

8

CAUTION
Risk of traffic loss
Ensure that the correct module is identified. Removing the wrong optical fiber drops all traffic on the local shelf.

DANGER
Risk of laser radiation exposure
Laser radiation is present on the optical fiber. Do not look into the optical fiber.

Remove the optical fiber from the circuit pack raising the alarm.

9 Measure the receive power using an optical power meter.

10 If the power is below the receiver sensitivity for this circuit pack, perform the following steps for All Provisioned VTs Rx signal degrade:

Note: For information about circuit pack technical specifications, see the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM.

a. Adjust the local attenuation, if equipped, to try to get the receive power above the receiver sensitivity level.

b. If you cannot get the receive power above the receiver sensitivity level, remove the Tx optical fiber from the far-end circuit pack.

c. Measure the transmit power at the far end.

d. If the power is above the launch power (minimum), the optical fiber attenuation is too high, the optical fiber connections are dirty or the optical fiber is damaged. Use your company procedure to determine the location of the problem.

e. If the power is below the launch power (minimum), replace the required circuit pack at the transmit end.
See Replacing an optical interface circuit pack in a linear system on page 3-34, Replacing an optical interface circuit pack in a UPSR on page 3-38, or Replacing an OC-48 or OC-192 optical interface circuit pack in a BLSR on page 3-41.

f. Retrieve all alarms to determine if the alarm cleared.
See Retrieving active alarms for a network element on page 2-3.

g. If the alarm does not clear, replace the optical interface circuit pack reporting the alarm.

h. Clean and reattach both optical fibers. See *Installation*, 323-1059-201.

—continued—

Procedure 4-6 (continued)
All Provisioned VTs Rx Signal Degrade

Step	Action
	i. Retrieve all alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
	j. If the alarm does not clear, contact your next level of support or your Nortel Networks support group.
11	If the power is above the receiver sensitivity for this circuit pack, clean all connections at both ends of the optical fiber link following your company standards and reattach the optical fibers.
12	If the alarm does not clear, replace the optical interface circuit pack raising the alarm.
13	If the alarm does not clear, clean the receive optical fibers and connectors.
14	Verify the signal degrade threshold (SDTH). Ensure that the SDTH is set to the value that you must be using. See 323-1059-311, Editing the line SDTH of an optical facility on page 1-37 or Editing the path SDTH of a signal on page 1-39.
15	If the alarm does not clear, replace the optical interface circuit pack raising the alarm. See Replacing an optical interface circuit pack in a linear system on page 3-34, Replacing an optical interface circuit pack in a UPSR on page 3-38, or Replacing an OC-48 or OC-192 optical interface circuit pack in a BLSR on page 3-41.
16	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-7
All Provisioned VTs Rx Signal Label Mismatch

Probable cause

This alarm is raised when the network element detects that all of the signal labels in the VT overhead do not match the expected signal labels on all VT1.5 cross-connects provisioned within an STS.

For most VTs, the expected signal label depends on the type of mapping that is used to place the DS1s into the VT1.5 bit asynchronous mapping or VT1.5 byte synchronous mapping.

The usual causes of this alarm are as follows:

- mapping a DS1 to the wrong VT1.5
- incorrect setting for the mapping of a DS1 facility

Note: Perform this procedure for all VT1.5 cross-connects provisioned within the STS-1.

Impact

Major, service-affecting (M, SA) alarm if on active path
Minor, non-service-affecting (m, NSA) alarm if on inactive path

Note: The alarm status is major, service-affecting (M, SA) because the DS1 mapper is unable to demultiplex the correct DS1 and will output DS1 AIS. A DS1 Tx AIS alarm is raised.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

—continued—

Procedure 4-7 (continued)
All Provisioned VTs Rx Signal Label Mismatch

Step	Action
1	Retrieve alarms from the network element. See Retrieving active alarms for a network element on page 2-3.
2	Verify if there are alarms of higher order from the alarm hierarchy. See Alarm hierarchies on page 4-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the Rx Signal Label Mismatch alarm cleared.
4	If the alarm does not clear, identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
5	Use the optical fiber connection information to identify the transmit and receive sites of the alarmed signal.
6	If the network element is part of a mid-span meet and the remote network element is from another vendor, use the alarm system of the other vendor to find the problem.
7	Log in to each of the network elements on the VT path. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
8	Retrieve all cross-connects from the remote network element. See 323-1059-320, Retrieving end-to-end connections on page 1-2.
9	Verify cross-connects for the entire path to ensure an end-to-end connection exists. If an end-to-end connection does not exist, provision the necessary cross-connects. See 323-1059-320, Procedures for end-to-end connection management on page 1-1.
10	Retrieve the alarms from the remote network element to determine if the alarm cleared.
11	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-8
All Provisioned VTs Rx Unequipped

Probable cause

This alarm is raised when the network element detects unequipped signal labels in the VT path overhead on all VT1.5 cross-connects provisioned within an STS.

One or more of the following conditions cause this alarm:

- incoming EC-1 Rx signal contains unequipped VTs
- improper connection (for example, no cross-connect is provisioned at the far end)
- far-end DS1 facility out of service with cross-connect provisioned

Note 1: Unequipped alarms can be raised while provisioning. Correct completion of provisioning should clear the alarms.

Note 2: This procedure assumes provisioning is not being done, the system has been running for some time without VT unequipped errors, and all fail LEDs are cleared.

Note 3: Perform this procedure for all VT cross-connects provisioned within the STS-1.

Impact

Major, service-affecting (M, SA) alarm, if on active path
Minor, non-service-affecting (m, NSA) alarm, if on inactive path

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

—continued—

Procedure 4-8 (continued)
All Provisioned VTs Rx Unequipped

Step	Action
1	Retrieve alarms from the network element. See Retrieving active alarms for a network element on page 2-3.
2	**If** the circuit pack is / **Then** go to OCn — step 3 EC-1x3 or EC-1x12 — step 14
3	Verify if there are alarms of higher order from the alarm hierarchy. See Alarm hierarchies on page 4-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
4	Retrieve alarms to determine if the Rx Unequipped alarm cleared.
5	If the alarm does not clear, identify the optical interface circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
6	Use the optical fiber connection information to identify the transmit and receive ends for the alarmed signal.
7	If the network element is part of a mid-span meet and the remote network element is from another vendor, use the alarm system of the other vendor to find the problem.
8	Log in to each of the network elements on the VT path. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
9	Retrieve all cross-connects from the remote network element. See 323-1059-320, Retrieving end-to-end connections on page 1-2.
10	Verify cross-connects for the entire path to ensure an end-to-end connection exists. If an end-to-end connection does not exist, provision the necessary cross-connects. See 323-1059-320, Procedures for end-to-end connection management on page 1-1.
11	Retrieve alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
12	If the alarm does not clear, verify the DS1 facility state to ensure that the facility is in service. See 323-1059-350, Retrieving equipment and facility details on page 2-2.
13	If the alarm does not clear, contact your next level of support or your Nortel Networks support group. You have completed this procedure.

—continued—

Procedure 4-8 (continued)
All Provisioned VTs Rx Unequipped

Step	Action
14	Use a SONET test set to determine if a valid EC-1 signal is on the EC-1 cross-connect for that facility. • If the signal contains unequipped VT1.5s (V5 payload label is 0), the problem is in the EC-1 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. You have completed this procedure. • If the signal contains equipped VT1.5s, go to the next step.
15	Operate a manual switch on the EC-1x3 or EC-1x12 circuit pack raising the alarm. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16.
16	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
17	Wait 30 seconds. If the alarm clears, the working EC-1x3 or EC-1x12 circuit pack is faulty. Replace the circuit pack that is detecting unequipped. See Replacing the EC-1x3 or EC-1x12 circuit pack on page 3-32.
18	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-9
APS Channel Match Fail

Probable cause

This alarm is raised when

- the received channel ID on the protection optical interface circuit pack is not as expected. This is normally because of a failure in the optical interface circuit pack.
- the K-byte communications protocol between the two optical interfaces is not working because the optical fiber is not connected to the correct slot at either end
- the protection engine does not receive K-bytes from the far-end
- the protection engine receives invalid K-bytes from the far-end

Note: This alarm is only raised on 1+1 linear protected configurations.

Impact

Major, non-service-affecting (M, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201.

Step	Action
1	Identify the optical interface circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Identify the protection provisioning on the circuit pack raising the alarm. Ensure that the protection scheme is 1+1 linear. See 323-1059-311, Retrieving protection scheme and protection switch mode for a pair of optical facilities on page 1-3. If the protection is not 1+1 linear, contact your next level of support or your Nortel Networks support group.
3	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
4	Verify that the optical fibers are connected to the correct slots on each node.
5	If the alarm does not clear, replace the optical interface circuit pack raising the alarm. See Replacing an optical interface circuit pack in a linear system on page 3-34.
6	Wait 30 seconds.

—continued—

Procedure 4-9 (continued)
APS Channel Match Fail

Step	Action
7	If the alarm does not clear, use company records to determine the network element and optical interface circuit pack on the far end of the optical fiber link that is raising the alarm.
8	Replace the remote optical interface circuit pack. See Replacing an optical interface circuit pack in a linear system on page 3-34.
9	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-10
Automatic Protection Switch Byte Fail

Probable cause

This alarm is raised when the received channel protection switching control bytes (K1/K2) on the protection optical interface circuit pack are not valid codes. This is normally because of a failure in the optical interface circuit pack.

Note: This alarm is only raised on 1+1 linear protected configurations.

Impact

Major, non-service-affecting (M, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201.

Step	Action
1	Identify the optical interface circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Identify the protection provisioning on the circuit pack raising the alarm. Ensure that the protection scheme is 1+1 linear. See 323-1059-311, Retrieving protection scheme and protection switch mode for a pair of optical facilities on page 1-3. If the protection is not 1+1 linear, contact your next level of support or your Nortel Networks support group.
3	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
4	Replace the optical interface circuit pack raising the alarm. See Replacing an optical interface circuit pack in a linear system on page 3-34.
5	Wait 30 seconds.
6	If the alarm does not clear, use company records to determine the network element and optical interface circuit pack on the far end of the optical fiber link.
7	Replace the remote optical interface circuit pack. See Replacing an optical interface circuit pack in a linear system on page 3-34.
8	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-11
Autoprovisioning Mismatch

Probable cause

This alarm is raised when

- a circuit pack is inserted into a shelf that does not support that specific type of circuit pack
- a Packet Edge 2xGigE has been inserted into an OPTera Metro 3500 shelf that contains a shelf processor
- a Packet Edge 2xGigE has been inserted into a slot other than 3, 5, 7, or 9
- a circuit pack has been tampered with or damaged and inserted into the wrong slot

Impact

Minor, non-service-affecting (m, NSA) alarm

Note: There is no effect on shelf operations.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

Step	Action
1	Identify the circuit pack that is in the wrong slot or shelf. See Circuit pack slot assignments for OPTera Metro 3500 on page 4-38.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	If a Packet Edge 2xGigE circuit pack has been inserted into an even slot, remove the circuit pack and place it into an odd slot.
4	Remove the incorrect circuit pack and replace it with the correct circuit pack. See Procedures for equipment replacement on page 3-1. ***Note:*** The circuit pack raises a Circuit Pack Mismatch alarm if the circuit pack is the correct type, but is not in the correct position. To clear the alarm, see Circuit Pack Mismatch on page 4-70.

—end—

Procedure 4-11 (continued)
Autoprovisioning Mismatch

Circuit pack slot assignments for OPTera Metro 3500

Circuit pack	OPTera Metro 3500 slots	Description
LIF	1a	Left interface
LOAM	1a	Left OAM
Power mod.	1b	Power module
Power mod.	1c	Power module
DS1	3 to 10	DS1 mapper
DSM DS1x84 termination module	DS1 service module only	DS1 service module DS1x84 terminal module (TM) mapper
DS3x3, DS3x12, DS3x12e, DS3VTx12	3 to 10	DS3x3 mapper, DS3x12 mapper, DS3x12e mapper, DS3VTx12 mapper
EC-1x3, EC-1x12	3 to 10	EC-1x3 circuit pack, EC-1x12 circuit pack
ILAN	16	Intershelf LAN (optional)
4x100BT or 4x100FX	3 to 10	OPTera Packet Edge circuit pack
2xGigE	3, 5, 7, 9	OPTera Packet Edge 2xGigE circuit pack
2xGigE/FC-P2P-P2P	3 to 10	Dual port Gigabit Ethernet/Fibre Channel circuit pack
2x100BT-P2P	3 to 10	2x100BT-P2P circuit pack
NPx	16	Extended network processor
OC-3	3 to 10	Optical interface circuit pack
OC-3x4	3 to 10	Optical interface circuit pack
OC-12	3 to 12	Optical interface circuit pack
OC-12x4 STS STS	3 to 10	Optical interface circuit pack
OC-48 STS	3 to 12	Optical interface circuit pack
OC-48	11 and 12	Optical interface circuit pack
OC-48 DWDM	11 and 12	Optical interface circuit pack
OC-192	11 and 12	Optical interface circuit pack
OC-192 DWDM	11 and 12	Optical interface circuit pack
PSC	2	Protection switch controller
PSX	17	Protection switch extender

SPx	15	Extended shelf processor
VTX-48 and VTX-48e	13 and 14	Virtual tributary cross-connect circuit pack
STX-192	13 and 14	STS cross-connect circuit pack

Procedure 4-12
Auto Switch Complete

Probable cause

This alarm is raised when traffic is switched away from a DS1, DSM DS1x84 TM, DS3x3, DS3x12, DS3x12e, DS3VTx12, EC-1x3, EC-1x12, OC-3, OC-3x4, OC-12, OC-12x4 STS STS, OC-48 STS, OC-48, OC-192 circuit pack.

This alarm is notification that a protection switch has occurred.

The related conditions that can cause a protection switch include the following:

- excessive BIP error rate
- equipment or facility out of service
- equipment failure
- signal degrade
- signal failure

If the Auto Switch Complete-Oscillation autonomous event is also active, then oscillation control has been activated to prevent oscillating protection switches (repeated protection switches). Oscillation control, applicable to OC-n circuit packs in a 1+1 configuration, is activated after 6 protection switches occur within a 2 minute interval. Further protection switches are prevented for 2 minutes. After the 2 minute lockout period expires, the protection switches are re-enabled.

Impact

Warning, non-service-affecting (w, NSA) alarm

> ***Note:*** The non-alarm status of this alarm indicates that this is a standing condition which needs to be cleared. This condition has been caused by a protection switch.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

—continued—

Procedure 4-12 (continued)
Auto Switch Complete

Step	Action
1	Retrieve alarms from the network element. See Retrieving active alarms for a network element on page 2-3.
2	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
3	Determine the cause for the switch and use the appropriate alarm clearing procedure to clear the alarm. ***Note 1:*** This alarm is cleared 10 seconds after the failure condition is corrected. ***Note 2:*** For 1:n revertive protection the alarm will clear 5 seconds after the wait to restore timer has timed out. ***Note 3:*** For 1+1 nonrevertive protection traffic does not automatically switch back to the original circuit pack. You must move traffic between the circuit packs of the protected pair by performing a manual switch.
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-13
Bandwidth Incompatible

Probable cause

This alarm is raised by the shelf when tributary or high-speed circuit packs are not supported by the clock and cross-connect modules (VTX or STX) paired in slots 13 and 14.

Note 1: The Bandwidth Incompatible alarm is raised against the shelf, not the equipment. However, it masks and is masked by other STX or VTX equipment alarms. See Equipment alarm hierarchy on page 5-288.

Note 2: You cannot provision additional cross-connects until you clear this alarm.

Note 3: This alarm can be raised during VTX or STX configuration or reconfiguration.

The following table lists the incompatible conditions that raise this alarm:

Module installed in slot 13	Module installed in slot 14	Circuit packs in tributary or high-speed slots	Details
VTX-48	VTX-48	• OC-192 (slots 11, 12) • OC-48 STS (slots 3-10) • OC-12x4 STS STS (slots 3-10)	The Bandwidth Incompatible alarm is raised against the shelf. The Circuit Pack Incompatible alarm is also raised against the circuit packs in the tributary or high-speed slots.
VTX-48e	VTX-48e		
Note: Refer to the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM, for the list of compatible clock and cross-connect module and circuit pack combinations.			

Impact

Major, service-affecting (M, SA) alarm, if active with cross-connects
Minor, non-service-affecting (m, NSA) alarm, if unprotected or with no provisioned cross-connects

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

—continued—

Procedure 4-13 (continued)
Bandwidth Incompatible

Step	Action
1	Clear the associated Circuit Pack Incompatible alarm. See Circuit Pack Incompatible on page 4-66.
2	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-14
BITSin-A Rx AIS or BITSin-B Rx AIS

Probable cause

This alarm is raised when a VTX or STX module detects an alarm indication signal (AIS) on the incoming BITS timing reference signal. The upstream equipment generates an AIS signal to tell downstream equipment that a failure occurred. This alarm indicates that the BITS for this shelf has a failure.

Impact

Minor, service-affecting (m, SA) alarm, if active and unprotected
Minor, non-service-affecting (m, NSA) alarm, if inactive

Note: The Timing Source BITSin is not available to the shelf. If this is the active source, a timing protection switch occurs if a secondary source is provisioned and available. Otherwise, the shelf enters timing holdover mode.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Use a DS1 test set with clip-on leads to determine if the BITSin pins have a valid DS1 signal. The BITSin pins are on the LOAM of the shelf raising the alarm. • If there is an AIS, the problem is in the BITS source equipment and the shelf is reporting a valid condition. Perform troubleshooting on the BITS source equipment according to your company procedure. • If there is no AIS, go to the next step.
2	Identify the timing references in use on the network element. See 323-1051-310, Retrieving synchronization data for a network element on page 1-2.
3	Look for the alarmed BITSin in the Synchronization dialog box and note the corresponding primary or secondary reference.
4	Go to the site. Look at the VTX or STX modules in slots 13 and 14. Look at the reference fail LEDs that correspond to the reference you determined.

—continued—

Procedure 4-14 (continued)
BITSin-A Rx AIS or BITSin-B Rx AIS

Step	Action
5	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
6	If the LEDs are not off on both VTX or STX modules, replace the circuit pack that has the reference fail LED on. See Replacing a VTX module on page 3-48 or Replacing an STX-192 circuit pack on page 3-51.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-15
BITSin-A Rx BPV exceeds 10E-3 or BITSin-B Rx BPV exceeds 10E-3

Probable cause

This alarm is raised when the VTX or STX module detect a bipolar violation (BPV) on the incoming BITS timing reference signal. This alarm indicates that the signal from an outside BITS source is degraded. If this timing source is the active timing reference, the VTX or STX module will switch to the alternate reference if it is available.

A bipolar violation refers to two consecutive positive or negative pulses without an opposite polarity pulse in between. The alarm is raised when this error occurs at a rate greater than 10^{-3}.

Note: This procedure assumes that the signal has been in service and is alarm free. Ensure that line coding provisioning for the shelf and Remote Timing source is correct.

Impact

Minor, non-service-affecting (m, NSA) alarm

Note: The Timing Source BITSin is not available to the shelf. If this is the active source, a timing protection switch occurs if a secondary source is provisioned and available, or the shelf enters timing holdover mode.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

—continued—

Procedure 4-15 (continued)
BITSin-A Rx BPV exceeds 10E-3 or BITSin-B Rx BPV exceeds 10E-3

Step	Action
1	Use a DS1 test set with clip-on leads to determine if the BITSin pins have a valid DS1 signal. The BITSin pins are on the LOAM of the shelf raising the alarm. • If there are BPVs, the problem is in the BITS source equipment and the shelf is reporting a valid condition. Perform troubleshooting on the BITS source equipment according to your company procedure. • If there are no BPVs, go to the next step.
2	Identify the timing references in use on the network element. See 323-1051-310, Retrieving synchronization data for a network element on page 1-2.
3	Look for the alarmed BITSin in the Synchronization dialog box and note the corresponding primary or secondary reference.
4	Go to the site. Look at the VTX or STX modules in slots 13 and 14. Look at the reference fail LEDs that correspond to the reference you determined.
5	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
6	If the LEDs are not off on the VTX or STX module, replace the circuit pack that has the reference fail LED on. See Replacing a VTX module on page 3-48 or Replacing an STX-192 circuit pack on page 3-51.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-16
BITSin-A Rx Loss of Frame or BITSin-B Rx Loss of Frame

Probable cause

This alarm is raised when the VTX or STX module detects a loss of frame on the incoming BITS timing reference signal.

> ***Note:*** This procedure assumes that the signal has been in service and is alarm free. Ensure that frame provisioning for the shelf and Remote Timing source is correct.

Impact

Minor, non-service-affecting (m, NSA) alarm

> ***Note:*** The Timing Source BITSin is not available to the shelf. If this is the active source, a timing protection switch occurs when a secondary source is provisioned and available. Otherwise, the shelf enters timing holdover mode.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Use a DS1 test set with clip-on leads to determine if the BITSin pins have a valid DS1 signal. • If there is LOF, the problem is in the BITS source equipment and the shelf is reporting a valid condition. Perform troubleshooting on the BITS source equipment according to your company procedure. • If there is no LOF, go to the next step.
2	Identify the timing references in use on the network element. See 323-1051-310, Retrieving synchronization data for a network element on page 1-2.
3	Look for the alarmed BITSin in the Synchronization dialog box and note the corresponding primary or secondary reference.
4	Click Close in the Synchronization dialog box.

—continued—

Procedure 4-16 (continued)
BITSin-A Rx Loss of Frame or BITSin-B Rx Loss of Frame

Step	Action
5	Go to the site. Look at the VTX or STX module in slots 13 and 14. Look at the reference fail LEDs that correspond to the reference you determined.
6	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
7	If the LEDs are not off on the VTX or STX module, replace the circuit pack that has the reference fail LED on. See Replacing a VTX module on page 3-48 or Replacing an STX-192 circuit pack on page 3-51.
8	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-17
BITSin-A Rx Loss of Signal or BITSin-B Rx Loss of Signal

Probable cause

This alarm is raised when the VTX or STX module cannot detect a signal on the incoming BITS timing reference.

Impact

Minor, non-service-affecting (m, NSA) alarm

> ***Note:*** The Timing Source BITSin is not available to the shelf. If this is the active reference, a timing protection switch occurs when a secondary source is provisioned and available. Otherwise, the shelf enters timing holdover mode.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201.

Step	Action
1	Use a DS1 test set with clip-on leads to determine if the BITSin pins have a valid DS1 signal. The BITSin pins are on the LOAM of the shelf raising the alarm. • If there is LOS, the problem is in the BITS source equipment and the shelf is reporting a valid condition. Perform troubleshooting on the BITS source equipment according to your company procedure. • If there is no LOS, go to the next step.
2	Identify the timing references in use on the network element. See 323-1051-310, Retrieving synchronization data for a network element on page 1-2.
3	Look for the alarmed BITSin in the Synchronization dialog box and note the corresponding primary or secondary reference.

—continued—

Procedure 4-17 (continued)
BITSin-A Rx Loss of Signal or BITSin-B Rx Loss of Signal

Step	Action
4	Go to the site. Look at the VTX or STX module in slots 13 and 14. Look at the reference fail LEDs that correspond to the reference you determined.
5	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
6	If the LEDs are not off on both VTX or STX modules replace the circuit pack that has the reference fail LED on. See Replacing a VTX module on page 3-48 or Replacing an STX-192 circuit pack on page 3-51.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-18
BLSR Configuration Audit Fail

Probable cause

This alarm is raised when a discrepancy is detected between the master ring configuration file on the NPx and the copy residing on the SPx.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

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

Step	Action
1	Log in to the network processor. See 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Perform a force audit on the ring. See 323-1059-320, Performing a BLSR audit and retrieving diagnostics on page 6-45.
3	Retrieve the ring diagnostics to verify if the network processor or the network element has the correct ring configuration. **a.** Select BLSR Ring Management from the Configuration menu. **b.** Click on the Rings Diagnostics tab. **c.** Select the BLSR from the Ring drop-down list. **d.** Click Refresh.
4	**If** the ring configuration is correct on the — **Then** go to: network element — step 5 network processor — step 6

—continued—

Procedure 4-18 (continued)
BLSR Configuration Audit Fail

Step	Action
5	Load the ring configuration from the network element to the network processor: **a.** Select BLSR Ring Management, from the Configuration menu. **b.** Click on the Rings Commissioning tab. **c.** Click Remote Load [NE -> NP] to open the Remote load of ring map to NP dialog box. **d.** Select the BLSR ring name from the Ring drop-down list. **e.** Select the network element that has the correct ring configuration from the Remote source drop-down list. **f.** Click OK.
6	Perform the ring commissioning: **a.** Select BLSR Ring Management, from the Configuration menu. **b.** Click on the Rings Commissioning tab. **c.** Select the network processor from the NE drop-down list box. **d.** Select the BLSR ring name from the Ring drop-down list. **e.** Select the Temporary Configuration radio button. **f.** Click Check. ***Note:*** Allow enough time for the check to run. **g.** Click Load [NP -> SP]. ***Note:*** Allow enough time for the load to run. **h.** Click Invoke. Click Yes in the warning dialog box. ***Note:*** Allow enough time for the invoke to run. **i.** Click Commit. **j.** Click OK in the confirmation dialog box.
7	Perform a force audit on the ring. See 323-1059-320, Performing a BLSR audit and retrieving diagnostics on page 6-45.
8	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-19
BLSR Configuration in Progress

Probable cause

The user is attempting to provision a new BLSR configuration on the network element.

This alarm is raised in response to the successful execution of the following actions performed by accessing the BLSR Ring Management menu item in Site Manager:

- creating a ring in the ring list
- changing the ring name
- deleting a ring from the ring list
- adding a node to the ring included in the BLSR configuration list
- deleting a node from the ring included in the BLSR configuration list
- loading the BLSR configuration

Impact

Minor, non-service-affecting (m, NSA) alarm

Before you perform this procedure, you must

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

Step	Action
1	Perform commissioning of the BLSR configuration. See 323-1059-320, Provisioning a BLSR configuration on page 6-34.
2	To clear the alarm you need to do one of the following: • commit the ring commissioning. See 323-1059-320, Provisioning a BLSR configuration on page 6-34 • cancel the ring commissioning

—end—

Procedure 4-20
BLSR Connection Audit Fail

Probable cause

This alarm is raised when a nodal cross-connect in the bidirectional line-switched ring (BLSR) has an incorrect End NE A and End NE Z provisioned.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

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

Step	Action
1	Retrieve alarms from the network element. See 323-1059-543, Retrieving active alarms for a network element on page 2-3.
2	From the Active Alarms window, record the network element and unit (STS path) against which the BLSR Connection Audit Fail alarm is raised. ***Note:*** If the STS path is a pass-through connection, then two alarms will be raised, one against the STS path on each OC-48 or OC-192 optical interface circuit pack.
3	Retrieve end-to-end connections. See 323-1059-320, Retrieving end-to-end connections on page 1-2.
4	Record the NE A and NE Z for the network element and the unit (STS path) that you recorded in step 2.
5	Retrieve the nodal cross-connects for the network element on which the alarm is raised. See 323-1059-320, Retrieving cross-connects on page 6-3.
6	Edit the nodal cross-connect for the STS path against which the alarm is raised. The End NE A and End NE Z must be the same as the ones you recorded in step 4. See 323-1059-320, Editing a 2WAY cross-connect (BLSR networks) on page 6-29.
7	Perform a forced audit on the ring. See 323-1059-320, Performing a BLSR audit and retrieving diagnostics on page 6-45.
8	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-21
Bridge port not in forwarding state

Probable cause

This alarm is raised when a LAN port is not in service. If the service is a bridge with spanning tree functionality, the subscriber spanning-tree-protocol (STP) may have selected and disabled this path (LAN path). The system detected a redundant path.

Impact

Minor, service-affecting (m, SA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201.

Step	Action
1	Verify the system configuration for network loops.
2	Verify that the far end network element has no redundant connections. Remove any redundant connections. ***Note:*** If the network is intentionally configured with redundant paths, you can ignore or disable the alarm. See Disabling alarm points on page 2-28.
3	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-22
Circuit Pack Failed

Probable cause

CAUTION
Risk of circuit pack damage
Avoid touching any components on the printed circuit board. Electrostatic discharge can damage electrostatic-sensitive devices. Always connect yourself to ground before handling any circuit pack.

CAUTION
Risk of circuit pack damage
Do not force a circuit pack all the way to the back of a slot if there is resistance during insertion. Circuit packs are keyed to fit into specific slots. Ensure that each slot is correctly equipped to receive the circuit pack.

CAUTION
Risk of false failures being reported
The BNC 12 port I/O modules must be installed prior to insertion of the tributary circuit packs that use them.

This alarm is raised in the following situations:

- the trouble detection circuits of a circuit pack detect a failure on the module
- the shelf processor detects a major failure on another circuit pack
- on the shelf processor co-located with the network processor when the communication channel between the shelf processor and the network processor is down for 10 minutes
- on the shelf processor co-located with the network processor if the network processor resets twice in 1 minute

—continued—

- on the shelf processor co-located with the network processor if the shelf processor cannot read the network processor circuit pack identification
- on the DS3x3, DS3x12, DS3x12e, DS3VTx12, EC-1x3, or EC-1x12 circuit packs if the BNC 12 port I/O module or module connections are faulty

  Note 1: Both the alarm and LED alarm indicators should report the failure at the same time. If not, verify that there is not a shelf processor problem. The status LED comes on (red indicates a failure) after a circuit pack is inserted until it is completely booted. The circuit pack is not failed in this case. This LED should clear 1 minute after insertion.

  Note 2: If the Circuit Pack Failed alarm is raised against a 2xGigE/FC-P2P circuit pack, and you replace the SFPs on the circuit pack, the SFP inventory displayed in the Equipment & Facility Provisioning window is not updated. To correctly display the SFP inventory, clear the alarm first, then replace the SFPs.

Impact

Critical, service-affecting (C, SA) alarm, BLSR, unprotected circuit pack
Critical, service-affecting (C, SA) alarm, UPSR ring with cross-connects
Critical, service-affecting (C, SA) alarm, if active linear or unprotected with cross-connects
Minor, non-service-affecting (m, NSA) alarm, BLSR, protected circuit pack
Minor, non-service-affecting (m, NSA) alarm, if inactive linear, protected linear, or without cross-connects

Alarm severity depends on the circuit pack and the following conditions:

- alarms with critical, service-affecting severity occur when the circuit pack is active but unprotected, and the cross-connects are provisioned

  Note 1: If both VTX or STX modules fail, two C, SA alarms are raised.

  Note 2: An OCn UPSR raises critical, service-affecting alarms whether protected or unprotected.
- alarms with critical, service-affecting severity are raised when an OPTera Packet Edge circuit pack fails while attached to a ring
- alarms with critical, service-affecting severity occur when the DS3x3, DS3x12, DS3x12e, DS3VTx12, EC-1x3, EC-1x12, 2xGigE/FC-P2P, or 2x100BT-P2P circuit pack is faulty
- alarms with minor, non-service-affecting (m, NSA) severity occur when the circuit pack is protected or when the circuit pack is unprotected and there are no provisioned cross-connects, or when the circuit pack is unprotected and inactive

—continued—

Procedure 4-22 (continued)
Circuit Pack Failed

The following table lists expected severities for each circuit pack if any cross-connects are provisioned.

Module	Inactive	Active	Unprotected Mode
DS1, DSM DS1x84 termination module	m, NSA	C, SA	C, SA
DS3x3, DS3x12, DS3x12e, DS3VTx12	m, NSA	C, SA	C, SA
EC-1x3, EC-1x12	m, NSA	C, SA	C, SA
ILAN	NA	m, NSA	NA
NPx	NA	m, NSA	NA
VTX-48, VTX-48e, STX-192 (see Note 1)	m, NSA	C, SA	C, SA
OC-3, OC-3x4 as host for DS1 service module	C, SA	C, SA	C, SA
linear (OC-3, OC-3x4, OC-12, OC-12x4 STS, OC-48 STS, OC-48, OC-192)	m, NSA	C, SA	C, SA
BLSR (OC-48, OC-192) (see Note 2)	m, NSA	C, SA	C, SA
UPSR (OC-3, OC-3x4, OC-12, OC-12x4 STS, OC-48 STS, OC-48, OC-192) (see Note 3)	C, SA	C, SA	C, SA
OPTera Packet Edge (see Note 4)	C, SA	C, SA	NA
2x100BT-P2P	m, NSA	C, SA	NA
2xGigE/FC-P2P	m, NSA	C, SA	NA
PSC	NA	M, NSA	NA
PSX	NA	m, NSA	NA
SPx (see Note 5)	NA	M, NSA	NA

Note 1: If the VTX or STX modules are removed, the alarm severity is C, SA on both slots.

Note 2: In a BLSR configuration, both circuit packs are active.

Note 3: If the circuit pack is inactive the alarm severity is m, NSA, except in the case of an OC-3, OC-3x4, OC-12, OC-12x4 STS, OC-48, OC-48 STS, or OC-192 UPSR ring configuration.

Note 4: If the alarmed OPTera Packet Edge circuit pack is attached to a ring, the alarm severity is C, SA. If the alarmed OPTera Packet Edge circuit pack is not attached to a ring, the alarm severity is m, NSA.

Note 5: A major audible alarm is the only indication if the shelf processor is missing.

—continued—

Procedure 4-22 (continued)
Circuit Pack Failed

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- get a replacement circuit pack for the failed circuit pack
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

Step	Action
1	If the failed circuit pack is the network processor, see Circuit Pack Failed (network processor) on page 4-61. If the failed circuit pack is not the network processor, go to step 2.
2	If the circuit pack has fiber-optic cables attached, then disconnect the cables.
3	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
4	Replace the circuit pack. See Procedures for equipment replacement on page 3-1.
5	Reattach the fiber-optic cables if you removed them in step 2.
6	Retrieve all alarms and ensure the system is restored to its original state. See Retrieving active alarms for a network element on page 2-3.
7	Select Shelf Level View from the Configuration menu. Ensure that the shelf processor recognizes the new circuit pack in the Shelf Level View.

—end—

Procedure 4-23
Circuit Pack Failed (network processor)

Probable cause

CAUTION
Risk of circuit pack damage
Avoid touching any components on the printed circuit board. Electrostatic discharge can damage electrostatic-sensitive devices. Always connect yourself to ground before handling any circuit pack.

CAUTION
Risk of circuit pack damage
Do not force a circuit pack all the way to the back of a slot if there is resistance during insertion. Circuit packs are keyed to fit into specific slots. Ensure that each slot is correctly equipped to receive the circuit pack.

Use this procedure to clear a Circuit Pack Failed alarm.

This alarm is raised in the following situations:

- the on-board trouble detection circuits of a circuit pack detect a failure on the module and fail the circuit pack
- on the shelf processor co-located with the network processor when the communication channel between the shelf processor and the network processor is down for 10 minutes
- on the shelf processor co-located with the network processor if the network processor resets twice in 1 minute
- on the shelf processor co-located with the network processor if the shelf processor cannot read the network processor circuit pack identification

  Note 1: Both the alarm and LED alarm indicators should report the failure at the same time. If not, verify that there is not a shelf processor problem.

  Note 2: The status LED comes on (red indicates a failure) after a circuit pack is inserted until it is completely booted. The circuit pack is not failed in this case. This LED should clear in 1 minute after insertion.

  Note 3: Circuit packs are keyed to fit into specific slots. Ensure each slot is correctly equipped to receive the circuit pack.

—continued—

Procedure 4-23 (continued)
Circuit Pack Failed (network processor)

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201
- use an account with level 3 or higher user privilege code (UPC)

Step	Action
1	Retrieve the manual area address provisioned on the shelf processor. **a.** Open the Node Information window for the network element. **b.** Click Upper Layer SDCC to open the Upper Layer SDCC dialog box for the network element. **c.** Click Cancel.
2	Retrieve the manual area address provisioned on the network processor. See 323-1059-520, Retrieving the manual area addresses of the network processor on page 3-16.
3	If the network processor and shelf processor do not share a common manual area address, change the network processor or shelf processor address.
4	Modify the manual area address on the shelf processor. See 323-1059-520, Adding or editing a manual area address on page 3-17.
5	Modify the manual area address on the network processor. See 323-1059-520, Adding or editing a manual area address on page 3-17.
6	If the alarm does not clear, go to the next step.
7	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
8	Reseat the network processor. The network processor can take 5 minutes to become available. See Reseating a circuit pack on page 3-4.
9	If the alarm does not clear, reseat the shelf processor. This can take 5 minutes. See Reseating a circuit pack on page 3-4.
10	If the alarm does not clear, replace the network processor circuit pack. See Replacing the network processor on page 3-10.
11	If the alarm does not clear, replace the shelf processor circuit pack. See Replacing the shelf processor on page 3-7.
12	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-24
Circuit Pack Failed - BWM and Circuit Pack Failed - Sync

Use this procedure to clear a virtual tributary cross-connect (VTX) or STS tributary cross-connect (STX) double fault scenario. If the VTX/STX double fault conditions do not exist, follow the circuit pack fail procedure. See Circuit Pack Failed on page 4-57.

Probable cause

This alarm indicates that the VTX or STX modules failed in their bandwidth management or synchronization.

If a VTX or STX double fault scenario exists, follow this procedure to replace the VTX or STX module. Both circuit packs are partially functioning. If you remove either circuit pack, you will cause shelf traffic loss.

Note 1: Use this procedure to clear a virtual tributary cross-connect (VTX) or STS tributary cross-connect (STX) double fault scenario. If the VTX/STX double fault conditions do not exist, follow the circuit pack fail procedure. See Circuit Pack Failed on page 4-57.

Note 2: Use this procedure if on one VTX or STX module, the Circuit Pack Failed - Sync alarm is indicated by the red LED and the green LED being ON; and on the other VTX or STX module, the Circuit Pack Failed - BWM alarm is indicated by the red LED being ON.

Impact

CAUTION
Traffic loss
The procedure to clear the VTX or STX double fault scenario will result in a 90 second traffic loss. This traffic loss may be up to 5 minutes if the replacement circuit pack needs to be auto-upgraded. It is recommended that this procedure be performed during a maintenance window (when traffic is lightest), or that all traffic be routed away from the affected network element before performing this procedure.

Critical, service-affecting (C, SA) alarm (unprotected)
Major, non-service-affecting (M, NSA) alarm (protected)

—continued—

Procedure 4-24 (continued)
Circuit Pack Failed - BWM and Circuit Pack Failed - Sync

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Determine that a VTX or STX double fault scenario exists. See Probable cause.
2	Wait for an appropriate maintenance window when traffic is minimal. ***Note:*** Perform step 4 through step 6 as quickly as possible to minimize traffic loss.
3	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
4	Replace the VTX or STX module raising the Circuit Pack Failed - Sync alarm. See Replacing a VTX module on page 3-48 or Replacing an STX-192 circuit pack on page 3-51.
5	Wait for the green active LED to come on. This normally takes 10 seconds, but can take 5 minutes if the circuit pack needs to be auto-upgraded.
6	Replace the VTX or STX module raising the Circuit Pack Failed - BWM alarm. See Replacing a VTX module on page 3-48 or Replacing an STX-192 circuit pack on page 3-51. ***Note:*** Removing both VTX or STX modules can cause the shelf processor to raise alarms against other circuit packs, such as the Intercard fail or Circuit pack failed alarms. If this occurs, remove the alarmed circuit pack for 5 seconds and then insert it.

—end—

Procedure 4-25
Circuit Pack Failed - Pluggable

Probable cause

This alarm is raised when a Small Form Factor Pluggable (SFP) optical transceiver module provisioned on a 2xGigE/FC-P2P circuit pack fails.

Impact

Critical, service-affecting (C, SA) alarm for a 2xGigE/FC-P2P circuit pack with cross-connects
Minor, non-service-affecting (m, NSA) alarm for a 2xGigE/FC-P2P circuit pack without cross-connects

Requirements

Before you perform this procedure, ensure you

- have all the documentation referenced in this procedure
- obtain a supported SFP optical transceiver module
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify the 2xGigE/FC-P2P circuit pack and SFP port raising the alarm. The Unit field in the Active Alarms window specifies the circuit pack and port using the following format: GEFC-slot#-port#. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Replace the SFP optical transceiver module you identified in step 1. See Replacing a Small Form Factor Pluggable (SFP) optical transceiver module on page 3-21. ***Note:*** Refer to the Hardware feature descriptions chapter of the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM for the list of PECs of supported SFP optical transceiver modules.
3	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-26
Circuit Pack Incompatible

Probable cause

This alarm is raised when one of the following conditions occurs:

- the clock and cross-connect modules (VTX or STX) paired in slots 13 and 14 do not provide the same bandwidth switching capacity or synchronization modes. The Circuit Pack Incompatible alarm is raised against the modules in slots 13 and 14.

  Note 1: Slot 13 and 14 must contain the same type of clock and cross-connect module (VTX or STX), with the same PEC.

  Note 2: This alarm can be the result of an incorrect VTX or STX module replacement or installation, and is raised during VTX or STX configuration or reconfiguration.

- a circuit pack installed in a tributary or high-speed slot is incompatible with the clock and cross-connect modules (VTX or STX). The Circuit Pack Incompatible alarm is raised against the tributary circuit pack.
- an STX and a VTX circuit pack are installed in the same system creating an unsupported set up
- OC-48 STS circuit packs are installed in slots where OC-48 circuit packs were pre-provisioned, and BLSR protection is provisioned. The Circuit Pack Incompatible alarm is raised against the OC-48 STS circuit packs. In this case, no clock and cross-connect modules are installed in slots 13 and 14.

  Note: The OC-48 STS circuit pack does not support BLSR protection.

—continued—

Procedure 4-26 (continued)
Circuit Pack Incompatible

The following table lists the incompatible conditions that raise this alarm:

Module installed in slot 13	Module installed in slot 14	Circuit packs in tributary or high-speed slots	Details
VTX-48	VTX-48	• OC-192 (slots 11, 12) • OC-48 STS (slots 3-10) • OC-12x4 STS (slots 3-10)	Circuit Pack Incompatible alarm is raised against the circuit packs in the tributary or high-speed slots. The Bandwidth Incompatible alarm is also raised.
VTX-48e	VTX-48e		
VTX-48	VTX-48	• OC-48 STS (slots 11, 12)	Circuit Pack Incompatible alarm is raised against the circuit packs in the high-speed slots.
VTX-48e	VTX-48e		
STX-192	STX-192	• DS1 (slots 3-10) • DS3VTx12 (slots 3-10) • Double-width OC-48 (slots 11, 12)	Alarm raised against the circuit packs in the tributary or high-speed slots.
STX-192	VTX-48 or VTX-48e	—	Alarm raised against both modules in slots 13 and 14. Intercard Suspect alarm is also raised if there is a tributary card in the system that is not compatible with VTX or STX..
VTX-48 or VTX-48e	STX-192	—	Alarm raised against both modules in slots 13 and 14. Intercard Suspect alarm is also raised if there is a tributary card in the system that is not compatible with VTX or STX..
VTX-48	VTX-48e	—	Alarm raised against both VTX modules in slots 13 and 14.
VTX-48e	VTX-48	—	Alarm raised against both VTX modules in slots 13 and 14.
Note: Refer to the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM, for the list of compatible clock and cross-connect module and circuit pack combinations.			

Impact

Critical, service-affecting (C, SA) alarm, if active with cross-connects
Minor, non-service-affecting (m, NSA) alarm, if unprotected or with no provisioned cross-connects

—continued—

Procedure 4-26 (continued)
Circuit Pack Incompatible

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	**If** the alarm is raised against — **Then** go to an OC-48 STS circuit packs in slot 11 and 12, and BLSR protection is provisioned — step 3 VTX or STX modules in slots 13 and 14 — step 6 any other circuit pack — step 15
3	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
4	Replace the OC-48 STS circuit packs installed in slot 11 and 12 with OC-48 circuit packs. See on page 3-94.
5	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.
6	Select Shelf Level View from the Configuration menu.
7	In the Shelf Level View window, click the VTX or STX module in slot 13 to view the Selected circuit pack details.
8	Record the PEC for the VTX or STX module.
9	Click the other VTX or STX module in slot 14 to view the Selected circuit pack details.
10	Record the PEC for the other VTX or STX module.
11	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
12	Replace one of the modules so that slot 13 and 14 contain the same type of module, both VTX or both STX, with the same PEC. See Replacing a VTX module on page 3-48 or Replacing an STX-192 circuit pack on page 3-51.
13	Wait 30 seconds for the new circuit pack to provision.
14	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—continued—

Procedure 4-26 (continued)
Circuit Pack Incompatible

Step	Action
15	Replace the circuit pack in the tributary or high-speed slot with a circuit pack that is compatible with the installed clock and cross-connect modules (VTX or STX). Alternatively, you can replace both clock and cross-connect modules to support the installed tributary or high-speed circuit packs. See Procedures for equipment replacement on page 3-1. ***Note:*** Refer to the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM, for the list of compatible clock and cross-connect module and circuit pack combinations.
16	If the alarm does not clear, contact your next level of support or your Nortel Networks support group. **—end—**

Procedure 4-27
Circuit Pack Mismatch

Probable cause

This alarm is raised when one of the following conditions apply:

- circuit pack is in a slot provisioned for a circuit pack of another type
- PSX is inserted before the PSC

Note: During provisioning, a slot is assigned a specific facility and circuit pack type. The assignments are recorded in the provisioning database.

Impact

Critical, service-affecting (C, SA) alarm, BLSR, unprotected circuit pack
Critical, service-affecting (C, SA) alarm, UPSR with cross-connects
Critical, service-affecting (C, SA) alarm, if active linear or unprotected with cross-connects
Minor, non-service-affecting (m, NSA) alarm, BLSR, protected circuit pack
Minor, non-service-affecting (m, NSA) alarm, if inactive linear, protected linear, or without cross-connects

Note: An equipment protection switch occurs if protection is available. If the circuit pack is unprotected, shelf functions may be disrupted.

—continued—

Procedure 4-27 (continued)
Circuit Pack Mismatch

The following table lists expected severities for each circuit pack if any cross-connects are provisioned.

Module	Inactive	Active	Unprotected Mode
DS1, DSM DS1x84 termination module	m, NSA	C, SA	C, SA
DS3x3, DS3x12, DS3x12e, DS3VTx12	m, NSA	C, SA	C, SA
EC-1x3, EC-1x12	m, NSA	C, SA	C, SA
ILAN	NA	m, NSA	NA
NPx	NA	m, NSA	NA
VTX-48, VTX-48e, STX-192 (see Note 1)	m, NSA	C, SA	C, SA
OC-3, OC-3x4 as host for DS1 service module	C, SA	C, SA	C, SA
linear (OC-3, OC-3x4, OC-12, OC-12x4 STS, OC-48 STS, OC-48, OC-192)	m, NSA	C, SA	C, SA
BLSR (OC-48, OC-192) (see Note 2)	m, NSA	C, SA	C, SA
UPSR (OC-3, OC-3x4, OC-12, OC-12x4 STS, OC-48 STS, OC-48, OC-192) (see Note 3)	C, SA	C, SA	C, SA
OPTera Packet Edge (see Note 4)	C, SA	C, SA	NA
2x100BT-P2P	m, NSA	C, SA	NA
2xGigE/FC-P2P	m, NSA	C, SA	NA
PSC	NA	M, NSA	NA
PSX	NA	m, NSA	NA
SPx (see Note 5)	NA	M, NSA	NA

Note 1: If the VTX or STX modules are removed, the alarm severity is C, SA on both slots.

Note 2: In a BLSR configuration, both circuit packs are active.

Note 3: If the circuit pack is inactive the alarm severity is m, NSA, except in the case of an OC-3, OC-3x4, OC-12, OC-12x4 STS, OC-48, OC-48 STS, or OC-192 UPSR ring configuration.

Note 4: If the alarmed OPTera Packet Edge circuit pack is attached to a ring, the alarm severity is C, SA. If the alarmed OPTera Packet Edge circuit pack is not attached to a ring, the alarm severity is m, NSA.

Note 5: A major audible alarm is the only indication if the shelf processor is missing.

—continued—

Procedure 4-27 (continued)
Circuit Pack Mismatch

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 1 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Select the network element, then click Shelf Level View from the Configuration drop-down menu to open the network element Shelf Level View.
2	Compare slot assignments shown in the Shelf Level View with the actual circuit packs in the shelf until you identify the incorrect circuit pack.
3	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
4	Replace the incorrect circuit pack with a correct circuit pack. See Procedures for equipment replacement on page 3-1.
5	If the PSX has been inserted before the PSC: **a.** pull both the PSX and PSC out of their slots **b.** insert the PSC first and wait 5 minutes **c.** insert the PSX second
6	If all circuit packs appear to be the correct type, retrieve all alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
7	If the alarm does not clear, identify the circuit pack issuing the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
8	Replace the circuit pack you identified in step 7. See Procedures for equipment replacement on page 3-1.
9	If the alarm clears, the circuit pack you identified in step 7 is damaged. If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-28
Circuit Pack Mismatch - Pluggable

Probable cause

This alarm is raised when an unsupported Small Form Factor Pluggable (SFP) optical transceiver module is installed in a provisioned port on a 2xGigE/FC-P2P circuit pack.

Impact

Critical, service-affecting (C, SA) alarm for a 2xGigE/FC-P2P circuit pack with cross-connects
Minor, non-service-affecting (m, NSA) alarm for a 2xGigE/FC-P2P circuit pack without cross-connects

Requirements

Before you perform this procedure, ensure you

- have all the documentation referenced in this procedure
- obtain a supported SFP optical transceiver module
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify the 2xGigE/FC-P2P circuit pack and SFP port raising the alarm. The Unit field in the Active Alarms window specifies the circuit pack and port using the following format: GEFC-slot#-port#. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	Replace the SFP optical transceiver module you identified in step 1 with a supported SFP optical transceiver module. See Replacing a Small Form Factor Pluggable (SFP) optical transceiver module on page 3-21. ***Note:*** Refer to the Hardware feature descriptions chapter of the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM for the list of PECs of supported SFP optical transceiver modules.
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-29
Circuit Pack Missing

Probable cause

This alarm is raised when the following occurs:

- circuit pack is not in the designated slot
- circuit pack failure makes the circuit pack undetectable
- a replacement circuit pack is being initialized

  Note: Software initalization can delay the removal of the Circuit Pack Missing alarm for a few minutes. The delay may vary depending upon the amount of SPx activity at the time of the CP replacment and the size of the tributary load.

- PSX is inserted before the PSC
- DSM DS1x84 termination module (TM) mapper indicates that its mate is missing

  Note: Loss of an OAM link to a provisioned DSM DS1x84 TM mapper while the OAM link of the mate remains intact masks all alarms against the circuit pack except the Circuit Pack Missing alarm. A Circuit Pack Missing alarm against a DSM DS1x84 TM mapper masks the OAM not available alarm provided it has a mate with an OAM link (the mate informs the shelf processor that the circuit pack is missing).

—continued—

Procedure 4-29 (continued)
Circuit Pack Missing

Impact

Critical, service-affecting (C, SA) alarm, BLSR, unprotected circuit pack
Critical, service-affecting (C, SA) alarm, UPSR, with cross-connects
Critical, service-affecting (C, SA) alarm, if active linear or unprotected with cross-connects
Minor, non-service-affecting (m, NSA) alarm, BLSR, protected circuit pack
Minor, non-service-affecting (m, NSA) alarm, if inactive linear, protected linear, or without cross-connects

Alarm severity depends on the following conditions:

- alarms with critical, service-affecting severity are raised when both circuit packs in a protection group are pulled out of their slots. In this case you would have one m, NSA and one C, SA.

  Note 1: An OCn UPSR ring raises critical, service-affecting circuit pack missing alarms whether protected or unprotected.

  Note 2: If both VTX or STX modules are removed, two C, SA alarms are raised.

- alarms with critical, service-affecting severity are raised when the DS3x3, DS3x12, DS3x12e, DS3VTx12, EC-1x3, EC-1x12, 2xGigE/FC-P2P, or 2x100BT-P2P circuit pack is not in its provisioned slot
- alarms with critical, service-affecting severity are raised when a Packet Edge circuit pack is missing but attached to a ring
- alarms with critical, service-affecting severity are raised when missing circuit packs are unprotected

  Note: The alarm status is always m, NSA for the ILAN, PSX, or network processor.

- alarms with major, non-service-affecting severity are raised when the PSC or shelf processor is missing. If the shelf processor is missing, communications and performance monitoring with the shelf are inactive, therefore, the only indication is the major audible alarm. The alarm status remains M, NSA.

—continued—

Procedure 4-29 (continued)
Circuit Pack Missing

The following table lists expected severities for each circuit pack if any cross-connects are provisioned.

Module	Inactive	Active	Unprotected Mode
DS1, DSM DS1x84 termination module	m, NSA	C, SA	C, SA
DS3x3, DS3x12, DS3x12e, DS3VTx12	m, NSA	C, SA	C, SA
EC-1x3, EC-1x12	m, NSA	C, SA	C, SA
ILAN	NA	m, NSA	NA
NPx	NA	m, NSA	NA
VTX-48, VTX-48e, STX-192 (see Note 3)	m, NSA	C, SA	C, SA
OC-3, OC-3x4 as host for DS1 service module	C, SA	C, SA	C, SA
linear (OC-3, OC-3x4, OC-12, OC-12x4 STS, OC-48 STS, OC-48, OC-192 STS)	m, NSA	C, SA	C, SA
BLSR (OC-48, OC-192) (see Note 2)	m, NSA	C, SA	C, SA
UPSR (OC-3, OC-3x4, OC-12, OC-12x4 STS, OC-48 STS, OC-48, OC-192) (Note 1)	C, SA	C, SA	C, SA
OPTera Packet Edge (see Note 4)	C, SA	C, SA	NA
2x100BT-P2P	m, NSA	C, SA	NA
2xGigE/FC-P2P	m, NSA	C, SA	NA
PSC	NA	M, NSA	NA
PSX	NA	m, NSA	NA
SPx (see Note 5)	NA	M, NSA	NA

Note 1: If the circuit pack is inactive the alarm severity is m, NSA, except in the case of an OC-3, OC-3x4, OC-12, OC-12x4 STS, OC-48, OC-48 STS, or OC-192 UPSR ring configuration.

Note 2: In a BLSR configuration, both circuit packs are active.

Note 3: If the VTX or STX modules are removed, the alarm severity is C, SA on both slots.

Note 4: If an alarmed OPTera Packet Edge circuit pack is attached to a ring, the alarm severity is C, SA. If the alarmed OPTera Packet Edge circuit pack is not attached to a ring, the alarm severity is m, NSA.

Note 5: A major audible alarm is the only indication if the shelf processor is missing.

—continued—

Procedure 4-29 (continued)
Circuit Pack Missing

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 3 or higher user privilege code (UPC) if the alarm is for the PSX
- obtain replacement circuit packs
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
3	**If** / **Then** go to the PSX is missing — step 4 both VTX or STX modules are missing — step 15 the PSC is missing — step 16 the DSM DS1x84 TM is missing — step 17 the OPTera Packet Edge circuit pack is missing — step 18 other circuit pack is missing — step 11
4	Verify if any cross-connects exist on DS1 ports 29 to 84 by clicking Cross-Connect in the Shelf view. **If** you / **Then** want to use ports 29 to 84 — insert a PSX. Go to step 11. do not want to use ports 29 to 84 — go to step 5
5	Delete any cross-connects. See 323-1059-320, Deleting a cross-connect on page 6-4.
6	Put all DS1 facilities in slots 6 to 10 out of service. See 323-1059-350, Changing a facility state to Out of Service (OOS) on page 2-25.
7	Delete all of the DS1 facilities in slots 6 to 10. See 323-1059-350, Deleting a facility on page 2-22.

—continued—

Procedure 4-29 (continued)
Circuit Pack Missing

Step	Action
8	Put all of the DS1 equipment in slots 6 to 10 out of service. 323-1059-350, Putting circuit pack equipment out of service (OOS) on page 2-15.
9	Delete all of the DS1 equipment in slots 6 to 10. See 323-1059-350, Deleting a circuit pack on page 2-17.
10	Delete the PSX equipment. See 323-1059-350, Deleting a circuit pack on page 2-17. You have completed this procedure.
11	If no circuit pack is in the slot, insert a circuit pack of the correct type. If a circuit pack is in the slot identified by the AID, remove the circuit pack and insert it again.
12	Wait 30 seconds to see if the alarm clears.
13	If the alarm does not clear, replace the circuit pack. See Procedures for equipment replacement on page 3-1.
14	Wait 30 seconds to see if the alarm clears. Go to step 19.
15	If both VTX or STX modules are missing or have been extracted: **a.** Insert the VTX or STX module in slot 13 first. **b.** Insert the VTX or STX module in slot 14. ***Note:*** Slot 13 and 14 must contain the same type of clock and cross-connect module (VTX or STX), with the same PEC. **c.** Wait 30 seconds to see if the alarm has cleared. **d.** If the alarm does not clear, replace the VTX or STX module. See Replacing a VTX module on page 3-48 or Replacing an STX-192 circuit pack on page 3-51. You have completed this procedure. Go to step 19.
16	If the PSX has been inserted before the PSC: **a.** Pull the PSX out of its slot. **b.** Insert the PSC in slot 2 and wait 5 minutes. **c.** Insert the PSX in slot 17. **d.** Wait 30 seconds to see if the alarm has cleared. Go to step 19.
17	If a DSM DS1x84 TM is missing, insert the required DSM DS1x84 TM and link by fiber. See Procedures for equipment replacement on page 3-1. Go to step 19.

—continued—

Procedure 4-29 (continued)
Circuit Pack Missing

Step	Action
18	If a Packet Edge circuit pack is missing, insert the circuit pack in to the appropriate slot and ensure it is attached to the ring. See 323-1059-320, Attaching an OPTera Packet Edge circuit pack to an RPR on page 5-22. ***Note:*** If the previous circuit pack was attached to the ring, the circuit pack you insert will automatically be attached to the ring.
19	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-30
Circuit Pack Missing - Pluggable

This alarm is raised when a provisioned Small Form Factor Pluggable (SFP) optical transceiver module is not physically installed in the 2xGigE/FC-P2P circuit pack.

Impact

Critical, service-affecting (C, SA) alarm for a 2xGigE/FC-P2P circuit pack with cross-connects
Minor, non-service-affecting (m, NSA) alarm for a 2xGigE/FC-P2P circuit pack without cross-connects

Requirements

Before you perform this procedure, ensure you

- have all the documentation referenced in this procedure
- obtain a supported SFP optical transceiver module
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify the 2xGigE/FC-P2P circuit pack and SFP port raising the alarm. The Unit field in the Active Alarms window specifies the circuit pack and port using the following format: GEFC-slot#-port#. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	Install an SFP optical transceiver module in the port you identified in step 1. See *Installation*, 323-1059-201. ***Note:*** Refer to the Hardware feature descriptions chapter of the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM for the list of PECs of supported SFP optical transceiver modules.
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-31
Circuit Pack Unknown

Probable cause

This alarm is raised in the following situations:

- when the on-board processor of a circuit pack cannot communicate with the shelf processor after you insert the circuit pack into the shelf
- when a DS1 mapper in a shelf has a missing or damaged PSC

  Note: The PSC is required to access a DS1 circuit pack.

- when an unknown circuit pack is inserted into an unprovisioned slot

  Note: An unknown circuit pack could be a circuit pack specific to an OPTera Metro 3300/3400 shelf that is inserted in to an OPTera Metro 3500 shelf.

- when a circuit pack is in the wrong slot

  Note: A circuit pack in the wrong slot is a situation that can only occur if the circuit pack keying is removed. Circuit packs are keyed to fit into specific slots. Do not remove the circuit pack keying for any reason.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.

—continued—

Procedure 4-31 (continued)
Circuit Pack Unknown

Step	Action
3	Compare the circuit pack raising the alarm with the supported circuit packs for each slot on the shelf. See the Hardware feature descriptions chapter in the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM. Ensure that the circuit pack is supported in the slot.
4	**If** the circuit pack you identified is — **Then** go to a DS1 circuit pack — step 5 not a DS1 circuit pack — step 12
5	Verify that the PSC is in slot 2 in the Shelf Level View.
6	If no PSC is in the shelf, install a PSC circuit pack in slot 2.
7	If a PSC is in the shelf, double click the PSC to open the PSC Status and Provisioning dialog.
8	Verify that the primary state of the PSC is in service.
9	If the PSC is out of service, select IS in the Primary field and click Set. **a.** Click OK in the confirmation dialog box. **b.** Click Close in the PSC Status dialog box. **c.** Wait 30 seconds. Retrieve all alarms. If the alarm clears, you have completed this procedure. If the alarm does not clear, go to the next step.
10	Remove the PSC and reinsert it in slot 2.
11	Wait 30 seconds. If the alarm does not clear, contact your next level of support or your Nortel Networks support group. You have completed this procedure.
12	Replace the circuit pack raising the alarm with a supported circuit pack. See Procedures for equipment replacement on page 3-1.
13	Wait 30 seconds. If the alarm clears, the identified circuit pack was damaged.
14	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-32
Circuit Pack Unknown - Pluggable

Probable cause

This alarm is raised when an unsupported Small Form Factor Pluggable (SFP) optical transceiver module is installed in a unprovisioned port of a 2xGigE/FC-P2P circuit pack.

Impact

Critical, service-affecting (C, SA) alarm for a 2xGigE/FC-P2P circuit pack with cross-connects
Minor, non-service-affecting (m, NSA) alarm for a 2xGigE/FC-P2P circuit pack without cross-connects

Requirements

Before you perform this procedure, ensure you

- have all the documentation referenced in this procedure
- obtain a supported SFP optical transceiver module
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify the 2xGigE/FC-P2P circuit pack and SFP port raising the alarm. The Unit field in the Active Alarms window specifies the slot and port using the following format: UNKNOWN-slot#-port#. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	Replace the SFP optical transceiver module you identified in step 1 with a supported SFP optical transceiver module. See Replacing a Small Form Factor Pluggable (SFP) optical transceiver module on page 3-21. ***Note:*** Refer to the Hardware feature descriptions chapter of the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM for the list of PECs of supported SFP optical transceiver modules.
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-33
Circuit Pack Upgrade Failed

Probable cause

This alarm is raised against a circuit pack when the upgrade process of the circuit pack fails or if a fiber is disconnected during the upgrade.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 3 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	**If** the alarm is raised against / **Then** go to

If the alarm is raised against	Then go to
an optical interface or tributary circuit pack	step 3
a Host OCn equipment	step 5
a protected DSM DS1x84 TM mapper	step 8
an unprotected DSM DS1x84 TM mapper	step 11

3	Reseat the circuit pack raising the alarm. See Reseating a circuit pack on page 3-4.
4	If the alarm does not clear, replace the circuit pack. See Procedures for equipment replacement on page 3-1. Go to step 13.
5	Clear any SDCC alarms that are raised, verify the status of the Host OCn equipment, and verify that SDCC is functioning. See 323-1059-350, Enabling or disabling the lower layer SDCC parameters on page 2-39.
6	If the alarm does not clear, perform a lamp test to verify the fiber is properly connected. See 323-1059-302, Performing a lamp test for a DSM on page 5-6.
7	If the alarm does not clear, perform a WARM restart of the circuit pack. See Restarting a circuit pack on page 2-45. Go to step step 13.

—continued—

Procedure 4-33 (continued)
Circuit Pack Upgrade Failed

Step	Action
8	Retrieve all active and disabled alarms on the system. See Retrieving active alarms for a network element on page 2-3. If the OAM Not Available alarm is raised against the DSM DS1x84 TM mapper, refer to OAM Not Available on page 5-50 to clear the alarm.
9	If the alarm does not clear, perform the following steps: — Verify the fiber connections of the DSM DS1x84 TM mapper and its mate. — Verify the status of the DSM DS1x84 TM mapper, and verify that SDCC is functioning on at least one DSM DS1x84 TM mapper. See 323-1059-350, Enabling or disabling the lower layer SDCC parameters on page 2-39. — If the alarm does not clear, restart the DSM DS1x84 TM mapper. See Restarting a circuit pack on page 2-45. — If the alarm does not clear, restart the DSM DS1x84 TM mate mapper. See Restarting a circuit pack on page 2-45. — If the alarm does not clear, restart both host OC-3 circuit pack connected to the DSM DS1x84 TM mappers. See Restarting a circuit pack on page 2-45.
10	If the alarm still does not clear, replace the circuit packs or mappers in the following order. ***Note:*** Before proceeding to replace the next circuit pack or mapper, verify if the alarm has cleared. — DSM DS1x84 TM mapper. See Replacing the DSM DS1x84 termination module mapper on page 3-26. — DSM DS1x84 TM mate mapper. See Replacing the DSM DS1x84 termination module mapper on page 3-26. — host OC-3 or OC-3x4 circuit pack connected to the DSM DS1x84 TM mapper. See Replacing an optical interface circuit pack in a linear system on page 3-34 or Replacing an optical interface circuit pack in a UPSR on page 3-38. — host OC-3 or OC-3x4 circuit pack connected to the DSM DS1x84 TM mate mapper. See Replacing an optical interface circuit pack in a linear system on page 3-34 or Replacing an optical interface circuit pack in a UPSR on page 3-38. — Go to step 13.

—continued—

Procedure 4-33 (continued)
Circuit Pack Upgrade Failed

Step	Action
11	If the alarm does not clear, perform the following steps: — Verify the fiber connections of the DSM DS1x84 TM mapper. — Verify the status of the DSM DS1x84 TM mapper, and verify that SDCC is functioning. See 323-1059-350, Enabling or disabling the lower layer SDCC parameters on page 2-39. — If the alarm does not clear, restart the DSM DS1x84 TM mapper. See Restarting a circuit pack on page 2-45. — If the alarm does not clear, restart the host OC-3 or OC-3x4 circuit pack connected to the DSM DS1x84 TM mapper. See Restarting a circuit pack on page 2-45.
12	If the alarm still does not clear, replace the circuit packs or mappers in the following order. ***Note:*** Before proceeding to replace the next circuit pack or mapper, verify if the alarm has cleared. — DSM DS1x84 TM mapper. See Replacing the DSM DS1x84 termination module mapper on page 3-26. — host OC-3 circuit pack connected to the DSM DS1x84 TM mapper. See Replacing an optical interface circuit pack in a linear system on page 3-34 or Replacing an optical interface circuit pack in a UPSR on page 3-38.
13	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-34
Client Service Mismatch

Probable cause

This alarm is raised against a Ethernet or Fibre Channel facility of a 2xGigE/FC-P2P circuit pack when the service provisioned on the remote 2xGigE/FC-P2P circuit pack does not match the service provisioned on the local 2xGigE/FC-P2P circuit pack. This alarm indicates that the local 2xGigE/FC-P2P circuit pack is expecting Gigabit Ethernet or Fibre Channel traffic and the far end is not provisioned with the same traffic.

When this alarm is active, traffic from the far end is lost.

Impact

Critical, service-affecting (C, SA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- have the network connection information (that is, how the optical modules on each network element connect to other network elements)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201
- use an account with level 3 or higher user privilege code (UPC)

—continued—

Procedure 4-34 (continued)
Client Service Mismatch

Step	Action
1	Trace the cross-connect information to determine the corresponding facility of the far end 2xGigE/FC-P2P circuit pack. ***Note:*** This alarm is also raised against the corresponding facilty of the 2xGigE/FC-P2P circuit pack at the far end.
2	Ensure that the nodal cross-connects are provisioned correctly. For more information on provisioning nodal cross-connects, see 323-1059-320, Procedures for nodal cross-connect management on page 6-1.
3	Determine the facility (ETH or FC) provisioned on the port of the 2xGigE/FC-P2P circuit pack raising the alarm at the near end: • Display the Equipment and Facility Provisioning window. See 323-1059-350, Retrieving equipment and facility details on page 2-2. • From the Equipment area in the Equipment & Facility Provisioning window, select the SFP optical transceiver module that corresponds to port of the 2xGigE/FC-P2P circuit pack raising the alarm. • From the Facility area, click the Facility Type drop-down list box to view which facility is provisioned (ETH or FC).
4	Repeat step 3 for the port of the 2xGigE/FC-P2P circuit pack at the far end.
5	**If** the facility at the near end and at the far end are provisioned with — **Then** go to different facility types — step 6 the same facility type — step 7
6	The facility at the near end or at the far end is incorrectly provisioned with the incorrect facility type (ETH or FC). You must: • Delete the WAN facility cross-connects of the incorrectly provisioned 2xGigE/FC-P2P circuit pack. See 323-1059-320, Deleting a cross-connect on page 6-4. • Delete the incorrectly provisioned facility. See 323-1059-350, Deleting a facility on page 2-22 • Add the required facility (ETH or FC). See 323-1059-350, Adding a facility on page 2-20.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-35
Concatenated Path Monitoring Unsupported

Probable cause

This alarm is raised against an OC-12 circuit pack that does not support STS-12c path monitoring if you try to provision it for STS-12c.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 1 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	If STS-12c path monitoring is not required, you have completed this procedure.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	Replace the circuit pack raising the alarm with an OC-12 circuit pack that supports STS-12c. See Replacing an optical interface circuit pack in a linear system on page 3-34 or Replacing an optical interface circuit pack in a UPSR on page 3-38.
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-36
Configuration Mismatch

Probable cause

This alarm is raised in the following circumstances:

- A supported circuit pack is in an unprovisioned slot but cannot be provisioned because of the provisioning state of the related or required slots. For example, a DS3x3 mapper is in slot 6 and raises this alarm, because a DS1 mapper is provisioned in slot 5.
- A 4x100BT, 4x100FX, 2xGigE/FC-P2P, or 2x100BT-P2P circuit pack is inserted into an unprovisioned empty slot and the mate slot has been provisioned for an incompatible service.

  Note: Refer to the Hardware feature descriptions chapter of the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM, for information on supported mate circuit packs for Packet Edge, 2xGigE/FC-P2P, and 2x100BT-P2P circuit packs.

- A DS3x3, DS3x12, DS3x12e, DS3VTx12, EC-1x3, or EC-1x12 circuit pack is provisioned in the protection slot of another transport circuit pack.

Impact

Minor, non-service-affecting (m, NSA) alarm

Note: Shelf function is not affected by this alarm.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Compare the circuit packs in the Shelf Level View window to the circuit packs in the shelf. Note any circuit packs that are in the shelf, but not in the Shelf Level View window.
3	Remove the circuit pack that is missing from the Shelf Level View window.

—continued—

Procedure 4-36 (continued)
Configuration Mismatch

Step	Action
4	Find another appropriate slot and provision the circuit pack there. If the system is not carrying traffic, use the required slot to delete the equipment and provisioning and insert the correct circuit pack. See Circuit pack slot assignments for OPTera Metro 3500 on page 4-38.

—end—

Procedure 4-37
Corrupt Network Backup

Probable cause

This alarm is raised when the network processor sees that a corrupt shelf processor backup is on the network processor.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- be able to connect to the network processor or shelf processor
- use an account with level 3 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Retrieve a list of save and restore directories to determine which backup is causing the alarm. See 323-1059-302, Retrieving a list of shelf processor provisioning data backups on page 6-45.
2	**If** you want to / **Then** go to delete the SP backup / step 3 replace the SP backup / step 4
3	Delete the corrupted shelf processor backup from the network processor. See 323-1059-302, Deleting shelf processor provisioning data backups from a network processor on page 6-46.
4	Replace the corrupted shelf processor backup. See 323-1059-302, Saving provisioning data from a shelf processor to a network processor on page 6-8.
5	Retrieve alarms from the network element. See Retrieving active alarms for a network element on page 2-3.
6	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-38
CP Loss of Host Timing Ref.

Probable cause

This alarm is raised when the frequency gap between the reference source from the OC-3 host and the DSM DS1x84 termination module (TM) internal source is too large. A timing reference is considered invalid if the absolute frequency offset from the internal DSM DS1x84 TM clock is greater than 32 +/- 5 ppm.

Note: This alarm does not result in circuit pack conviction and it clears when the conditions that caused the alarm change.

Impact

Critical, service-affecting (C, SA) alarm if active
Major, non-service-affecting (M, NSA) alarm if inactive

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Retrieve alarms from the network element. See Retrieving active alarms for a network element on page 2-3.
2	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52
3	Look for any other alarms in the active alarm list that are against the DSM DS1x84 TM. Use the appropriate alarm clearing procedure to clear the alarm.
4	Verify the timing reference is correct. See 323-1051-310, Synchronizing a network element to an internal timing source on page 1-4.
5	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
6	If the alarm does not clear, replace the DSM DS1x84 TM mapper. See Replacing the DSM DS1x84 termination module mapper on page 3-26.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-39
DataBase Corruption Detected

Probable cause

This alarm is raised when the shelf processor is replaced and there is a missing or failed circuit pack on the shelf. The alarm is the result of a data consistency audit depending on whether any equipment had to be autoprovisioned.

> ***Note:*** The DSM site address is lost if the host OC-3 or OC-3x4 circuit pack to the DSM DS1x84 termination module is missing or in a failed state when you replace the shelf processor.

The data consistency audit helps correct problems when a shelf processor is replaced and a transport circuit pack is not able to send its data to the shelf processor. The audit runs on every restart to ensure the integrity of data such as connections, protection, and synchronization.

For each slot, the audit compares provisioned equipment known to the shelf processor to that equipment known by the VTX or STX module. If there is a mismatch in the comparison:

- the mismatched circuit pack is autoprovisioned
- all known synchronization sources are informed that they are a reference
- all sources of all connections are informed of their connection information
- all protection data is recreated

  Note: The data consistency audit requires at least one VTX or STX module, and will not run if it detects that it was run and previously found problems.

Impact

Major, non-service-affecting (M, NSA) alarm

> ***Note:*** The data transfer to the transport circuit pack is blocked until the data consistency audit is successfully completed.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

—continued—

Procedure 4-39 (continued)
DataBase Corruption Detected

Step	Action
1	Retrieve the current alarms. See Retrieving active alarms for a network element on page 2-3.
2	If there is an Upgrade in Progress alarm, continue with the upgrade until it is committed before continuing this procedure. ***Note:*** Do not perform any FPGA upgrades until the DataBase Curruption Detected alarm has been cleared and a cold restart has been performed on the SPx.
3	Retrieve the current events. See Retrieving events for a network element on page 2-11. ***Note 1:*** If there is an Upgrade In Progress, complete the upgrade before continuing this procedure. ***Note 2:*** If there is a Loads Mismatch alarm, clear the alarm before continuing. See Loads Mismatch on page 5-33.
4	From the list of events find the DataBase Rebuilt For Slot event. The DataBase Rebuilt For Slot event is raised against the newly created Equipment AID.
5	Accept the data created by the audit. **If** you are performing — **Then** go to a database restore — step 6 a thorough analysis — step 7
6	Complete a database restore. See 323-1059-302, Procedures for provisioning data and software management on page 6-1. Go to step 9.

—continued—

Procedure 4-39 (continued)
DataBase Corruption Detected

Step	Action
7	If you want to perform a thorough analysis, analyze the data for the slots indicated by the DataBase Rebuilt For Slot event. Ensure that the facility provisioning data is consistent with the system provisioning. Edit the provisioning data as required. See 323-1059-350, Retrieving equipment and facility details on page 2-2, Editing DS1, DS3, EC-1, 2x100BT-P2P or GE/FC SFP facility signal attributes on page 2-28, or Editing the line SDTH of an optical facility on page 2-38. See 323-1059-520, Procedures for section and path trace on page 2-1. • For T1 facilities on DS1 — Far end NE — Fault Locate Mode — Format — Output stream coding — Mapping — Line code — Equalization — Timing Reference • For T3 facilities on, DS3x3, DS3x12, DS3x12e, and DS3VTx12 — Line build out — Format • For EC-1x3, EC-1x12, and OCn — Signal degrade threshold — Section trace format — Section trace message — Expected section trace message — Section trace fail mode — SS Bit Operation Mode — Timing reference — Section Data Communications Channel (SDCC) • Other data to consider for facility type — Path trace Data — PM Threshold Settings — Test Access Port (TAP) **—continued—**

Procedure 4-39 (continued)
DataBase Corruption Detected

Step	Action
8	If the shelf processor has been rebooted recently, wait for at least 10 minutes before proceeding (see Note). Then, perform a cold restart of the shelf processor. See Restarting the shelf processor on page 2-47. ***Note:*** If the shelf processor has been rebooted recently, wait for at least 10 minutes before you issue a cold restart to accept the data.
9	If the alarm does not clear, contact your next level of support or your Nortel Networks support group. **—end—**

Procedure 4-40
Database Not Ready

Probable cause

This alarm is raised before the NPx attempts to set up its provisioning data.

Impact

Minor, non-service-affecting (m, NSA) alarm

Step	Action
1	The alarm clears when the NPx provisioning data is released and available to the Site Manager applications.
2	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-41
Database Restore in Progress

Probable cause

This alarm is raised when the network processor or shelf processor detects that the circuit pack is restoring its provisioning files from a remote source.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- be able to connect to the network processor or shelf processor
- use an account with level 3 or higher user privilege code (UPC)

Step	Action
1	Wait until the database successfully restores the provisioning data. See 323-1059-302, Procedures for provisioning data and software management on page 6-1. If you want to abort the database restore, click Cancel in the Database Backup and Restore dialog box. ***Note:*** Canceling stops the action and cleans up any backup files left in invalid states.
2	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-42
Database Save and Restore Failed

Probable cause

This alarm is raised when the network processor or shelf processor detect that a save, restore, or commit command sent to the network processor or shelf processor fails.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- be able to connect to the network processor or shelf processor
- use an account with level 3 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Click Cancel in the Database Save and Restore dialog box. See 323-1059-302, Procedures for provisioning data and software management on page 6-1. ***Note:*** Canceling stops the action and cleans up any backup files left in invalid states.
2	This alarm can also clear if you try to save and restore the provisioning data again. The alarm clears if the save or restore action is successful. See 323-1059-302, Procedures for provisioning data and software management on page 6-1.
3	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-43
Default K-bytes

Probable cause

This alarm is raised when an OC-48 or OC-192 optical interface circuit pack receives a default K-bytes pattern.

This problem arises when a co-located network element is:

- not setup for bidirectional line-switched ring (BLSR)
- setup for BLSR but does not have a BLSR configuration

The default K-bytes pattern is detected when the automatic protection switching (APS) bytes are transmitted with the source node ID equal to the destination node ID.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

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

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52. The circuit pack raising the alarm is the receiving network element.
3	**If** the transmitting network element is … **Then** go to set up for BLSR — step 4 not set up for BLSR — step 5
4	Perform a manual ring audit. See 323-1059-320, Performing a BLSR audit and retrieving diagnostics on page 6-45. Go to step 7.
5	Verify the network topology for BLSR. See 323-1059-320, Provisioning a BLSR (bidirectional) on page 4-2.
6	If the alarm does not clear, verify the fiber connections of the OC-48 or OC-192 optical interface circuit pack.

—continued—

Procedure 4-43 (continued)
Default K-bytes

Step	Action
7	If the alarm does not clear, replace the OC-48 or OC-192 optical interface circuit pack. See Replacing an OC-48 or OC-192 optical interface circuit pack in a BLSR on page 3-41.
8	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-44
Degraded Performance

Probable cause

This alarm is raised when the network processor receives and detects errors in more than 10% of the frames from network processor facilities ILANNP or COLAN over a period of 60 seconds.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- have an Ethernet LAN analyzer
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Log in to the network processor. See 323-1059-302, Procedures for logging in to a network processor on page 2-1. ***Note 1:*** If an network processor restart occurred, you cannot access the network processor until the network processor database is released. ***Note 2:*** If you log in to a network processor using an account with level 5 user privilege code (UPC), you automatically log into all the network elements in the network processor span of control.
2	Identify the facility raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
3	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

—continued—

Procedure 4-44 (continued)
Degraded Performance

Step	Action
4	If the alarm is raised against the COLAN facility, perform the following Degraded performance (COLAN) procedures. **a.** Replace the COLAN cable connected to the COLAN connector on the LOAM. **b.** Use the LAN analyzer to verify errors on COLAN. **c.** If the alarm does not clear, replace the network processor. See Replacing the network processor on page 3-10.
5	If the alarm is raised against the ILANNP facility, perform the following Degraded performance (ILANNP) procedures. **a.** Replace the ILAN cable connected to the ILAN1 and ILAN2 connectors on the LOAM. **b.** Use the LAN analyzer to verify errors on ILANNP. **c.** If the alarm does not clear, replace the network processor. See Replacing the network processor on page 3-10. **d.** If the alarm does not clear, replace the shelf processor. See Replacing the shelf processor on page 3-7.

—end—

Procedure 4-45
Disk Full

Probable cause

This alarm is raised when the disk is full on either the shelf processor or the network processor. The disk is full on the shelf processor or network processor when the remaining capacity is less than 100 kbyte.

Impact

Major, non-service-affecting (M, NSA) alarm

Note 1: This condition prevents data collection and blocks the TBOS port. The TBOS connection to the shelf, by RS-422, times out during this alarm.

Note 2: Any time a Disk Full condition is reached, some applications or operations are blocked. For example, the system blocks upgrades, circuit pack provisioning, and initializations.

Requirements

Before you perform this procedure, you must

- use an account with level 4 user privilege code (UPC)

Step	Action	
1	**If** the disk is full for the	**Then**
	shelf processor	contact your next level of support or your Nortel Networks support group
	network processor	Delete the load that you do not need on the disk. Go to step 2
2	Select Release Management from the Configuration menu to open the Release Management window.	
3	Select a software release in the Release loads box.	
4	Click Delete.	
5	Click Yes in the confirmation dialog box.	
6	If the alarm does not clear, repeat step 1.	
7	Click Close. The alarm clears when the shelf processor or network processor disk capacity is at 95%.	

—end—

Procedure 4-46
DS1 Loopback Active or DS3 Loopback Active

Probable cause

This alarm is raised when you execute an operate loopback command.

> ***Note:*** Only execute loopback during facility testing. Never execute a loopback at any other time.

The loopback active alarm is an important advisory message. For example, if more than one user logs into a network element and one of the users activates loopback mode, the other users get this alarm message. The unavailability of a circuit can affect other maintenance being performed at the same time.

Impact

Minor, non-service-affecting (m, NSA) alarm

> ***Note:*** The facility must be OOS (out of service) to engage the loopback command, so it does not affect shelf function.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)

Step	Action
1	Identify the DS1 or DS3 in loopback mode. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Release the loopback. See 323-1059-222, Releasing a software loopback on page 2-58.

—end—

Procedure 4-47
DS1 Rx AIS

Probable cause

This alarm is raised when there is a far-end failure that causes traffic loss or the far-end equipment is out of service. The DS1 alarm indication signal (AIS) is received from the VT1.5 envelope. The DS1 Rx AIS alarm is raised when the network element detects an AIS on the DS1 traffic stream at the input. This alarm can also be generated if a test access session is in progress, no action is required if this is the cause.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- have an account with a level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Identify the DS1, DSM DS1x84 TM, or DS3VTx12 mapper raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
3	Use a DS1 test set to test the signal source. See 323-1059-222, Testing a basic network configuration on page 2-21.
4	If there is AIS, the problem is in the DS1 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures.
5	If the alarm does not clear, operate a manual switch on the mapper you identified in step 2. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16. ***Note:*** DS1 protection switching is 1:N revertive for DS1 circuit packs on the shelf but 1+1 protection switching is used on DSM DS1x84 TM and DS3VTx12 mappers.

—continued—

Procedure 4-47 (continued)
DS1 Rx AIS

Step	Action
6	Wait 30 seconds. If the alarm clears, the working mapper is faulty. Replace the mapper that is detecting AIS. See Replacing a DS1 mapper on page 3-24, Replacing the DSM DS1x84 termination module mapper on page 3-26, or Replacing the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper on page 3-30.
7	Release the manual switch on the circuit pack. See 323-1059-311, Releasing a protection switch on a tributary circuit pack on page 1-21.
8	Verify the cross-connects on every network element between the near-end and the far-end inclusively. See 323-1059-320, Retrieving cross-connects on page 6-3.
9	Retrieve all active and disabled alarms at the far-end. Clear any alarms on the connection by following the appropriate procedure.
10	Ensure the far-end network element is in-service.
11	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-48
DS1 Rx Bipolar Violations

Probable cause

This alarm is raised when a DS1 or DSM DS1x84 termination module (TM) mapper is faulty or the received signal from the outside DS1 source is degraded. A bipolar violation (BPV) means that two +V or two -V binary ones are transmitted consecutively without an opposite voltage binary one in between.

DS1 protocol uses ground as a binary zero and both +1V and -1V as binary ones. The polarity of ones is always toggled, which gives the signal desirable electrical characteristics and can be used to detect signal errors. This system is called a bipolar system.

Impact

Major, service-affecting (M, SA) alarm

Note: The DS1 signal is severely degraded.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify the mapper raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	Use a DS1 test set to test the signal source. • If there are bipolar violations (BPVs), the problem is in the DS1 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. • If there are no BPVs, go to the next step.

—continued—

Procedure 4-48 (continued)
DS1 Rx Bipolar Violations

Step	Action
4	Manually switch the circuit pack into protection mode. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16. ***Note:*** Ensure that the protection mapper is not carrying traffic for another working mapper before you switch traffic from a working mapper to the protection mapper.
5	Wait 30 seconds. If the alarm clears, the working mapper is faulty. Replace the mapper that is detecting BPVs. See Replacing a DS1 mapper on page 3-24 or Replacing the DSM DS1x84 termination module mapper on page 3-26.
6	Release the protection switch. See 323-1059-311, Releasing a protection switch on a tributary circuit pack on page 1-21.
7	If the alarm does not clear, inspect the cabling and the connection. The cabling may be loose or damaged. Repair any damage.
8	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-49
DS1 Rx Frequency Out of Range

Probable cause

This alarm is raised when the network element detects a signal on a DS1 input that it cannot lock onto because of a frequency difference.

Impact

Major, service-affecting (M, SA) alarm

Note: The shelf cannot carry traffic.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify the DS1 or DSM DS1x84 termination module (TM) mapper raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	Use a DS1 test set to test the signal source. • If there is an out of range frequency for DS1 the problem is in the DS1 source. The shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. • If there are no such conditions, go to the next step.
4	Manually switch the circuit pack into protection mode. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16. ***Note:*** Ensure the protection is not carrying traffic for another working mapper before you switch traffic from a working mapper to the protection mapper.
5	Wait 30 seconds. If the alarm clears, the working mapper is faulty. Replace the mapper that is detecting frequency out of range. See Replacing a DS1 mapper on page 3-24 or Replacing the DSM DS1x84 termination module mapper on page 3-26.
6	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-50
DS1 Rx Loss of Frame

Probable cause

This alarm is raised when the DS1, DSM DS1x84 termination module (TM), or DS3VTx12 mapper is unable to detect the provisioned framing pattern in the input signal.

Impact

Major, service-affecting (M, SA) alarm

Note 1: The shelf cannot carry traffic.

Note 2: This procedure assumes that the provisioned framing is correct and was not changed to create the alarm.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify the mapper raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	Use a DS1 test set to test the signal source. • If there is an LOF or incorrect framing, the problem is in the DS1 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. • If there are no such conditions, go to the next step.
4	Manually switch the circuit pack into protection mode. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16. ***Note:*** Ensure the protection circuit pack is not carrying traffic for another working mapper before you switch traffic from a working mapper to the protection mapper.

—continued—

Procedure 4-50 (continued)
DS1 Rx Loss of Frame

Step	Action
5	Wait 30 seconds. If the alarm clears, the working mapper is faulty. Replace the mapper that is detecting LOF. See Replacing a DS1 mapper on page 3-24, Replacing the DSM DS1x84 termination module mapper on page 3-26, or Replacing the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper on page 3-30.
6	Release the protection switch. See 323-1059-311, Releasing a protection switch on a tributary circuit pack on page 1-21.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-51
DS1 Rx Loss of Signal

Probable cause

This alarm is raised when one of the following conditions exists:

- the DS1 or DSM DS1x84 termination module (TM) mapper is faulty
- the DS1 signal stops transmitting from the adjacent network element
- the corresponding DS1 I/O module was removed
- the corresponding DS1 I/O module is not fully inserted and locked into position

Impact

Major, service-affecting (M, SA) alarm

Note: The shelf cannot carry traffic.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify the DS1 or DSM DS1x84 TM mapper raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	Ensure the corresponding I/O module is fully inserted and locked into position.
4	Use a DS1 test set to test the signal source. • If there is a LOS, the problem is in the DS1 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. • If there are no such conditions, go to the next step.

—continued—

Procedure 4-51 (continued)
DS1 Rx Loss of Signal

Step	Action
5	Manually switch the circuit pack into protection mode. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16. ***Note:*** Ensure the protection is not carrying traffic for another working mapper before you switch traffic from a working mapper to the protection mapper.
6	Wait 30 seconds. If the alarm clears, the working mapper is faulty. Replace the DS1 circuit pack that is detecting LOS. See Replacing a DS1 mapper on page 3-24 or Replacing the DSM DS1x84 termination module mapper on page 3-26.
7	If the alarm does not clear, inspect the cabling and the connection. The cabling may be loose or damaged. Repair any damage.
8	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.
9	Release the protection switch. See 323-1059-311, Releasing a protection switch on a tributary circuit pack on page 1-21.

—end—

Procedure 4-52
DS1 Rx Yellow

Probable cause

This alarm is raised when the following occurs:

- the DS1, DSM DS1x84 termination module (TM), or DS3VTx12 receiver detects a bad DS1 signal on the copper side and sends yellow back to the network element
- partial failure of a single port of the DS1, DSM DS1x84 TM, or DS3VTx12 mapper

Impact

Minor, non-service-affecting (m, NSA) alarm

Note: Traffic is being reported down by the remote system.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Inspect the remote system at the other end of the DS1 and clear any alarms you find.
3	If the alarm does not clear, identify the mapper raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
4	Use a DS1 test set to test the signal source. • If there is a valid signal on the Tx side and there is Yellow on the Rx side, the problem is in the source system. Perform troubleshooting on the source system according to your company procedures. • If there are no such conditions, go to the next step.

—continued—

Procedure 4-52 (continued)
DS1 Rx Yellow

Step	Action
5	Manually switch the circuit pack into protection mode. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16. ***Note:*** Ensure the protection circuit pack is not carrying traffic for another working mapper before you switch traffic from a working mapper to the protection mapper.
6	Wait 30 seconds. If the alarm clears, the working mapper is faulty. Replace the DS1 or DSM DS1x84 TM mapper that is detecting Rx Yellow. See Replacing a DS1 mapper on page 3-24, Replacing the DSM DS1x84 termination module mapper on page 3-26, or Replacing the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper on page 3-30.
7	Release the protection switch. See 323-1059-311, Releasing a protection switch on a tributary circuit pack on page 1-21.
8	If the alarm does not clear, inspect the cabling and the connection. The cabling may be loose or damaged. Repair any damage.
9	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-53
DS1 Test Signal Active

Probable cause

This alarm is raised when a connect test signal command is executed for facility testing.

Impact

Minor, non-service-affecting (m, NSA) alarm

Note: The DS1 must be OOS to operate the command to turn on the test signal, so there is no effect on current shelf functions.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify the DS1 mapper in test mode. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	If testing indicates a damaged port, replace the faulty circuit pack. See Attaching or detaching a circuit pack from the back plane on page 3-94.
4	Release the DS1 test signal you identified. **a.** Select Equipment and Facility Provisioning from the Configuration menu. **b.** Select the DS1 circuit pack with the DS1 in test mode from the Equipment list. **c.** Select the DS1 port with the DS1 in test mode from the Facility list. **d.** Click Test to open the Test Functions window. **e.** Select Test signal from the Test type drop-down list. **f.** Click Release in the Test Functions window. **g.** Click Close.

—end—

Procedure 4-54
DS1 Tx AIS

Probable cause

This alarm is raised when the network element detects a failed DS1 signal upstream on the other side of the connection. The network element is transmitting an alarm indication signal (AIS) to the remote end of the input.

This alarm indicates a warning to the downstream network element that the signal is not usable.

This alarm occurs because of:

- a DS1 receive fault (for example, Rx loss of signal, Rx loss of frame, Rx AIS) where the signal enters the network. If the DS1 mapping is byte synchronous, additional SONET alarms are active.
- a SONET fault condition (OC-3/OC-12/OC-48/OC-192/STS-1/STS-3c/STS-12c/STS-24c/STS-48c/VT alarms)
- no cross-connect assigned for the DS1

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- clear all SONET (OC-3, OC-12, OC-48, OC-192, STS-1, STS-3c, STS-12c, STS-24c, STS-48c, VT) and DS1 Rx alarms related to the circuit path in the network.

Step	Action
1	Another failure in the system normally causes this alarm. If other EC-1/OC-3/OC-12/OC-48/OC-192/STS-1/STS-3c/STS-12c/STS-24c/STS-48c/VT1.5 or DS1 Rx alarms exist on the system related to the circuit path, clear them first. Perform this procedure if the Tx AIS alarms are the only active alarms.
2	Identify the DS1 or DSM DS1x84 termination module (TM) facility raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
3	Retrieve the cross-connects. See 323-1059-320, Retrieving end-to-end connections on page 1-2.

—continued—

Procedure 4-54 (continued)
DS1 Tx AIS

Step	Action
4	Look for cross-connects provisioned for the DS1 raising the alarm. If there are no cross-connects for the DS1, the DS1 is in service (IS) without connections. Put the DS1 facility out of service (OOS). See 323-1059-350, Retrieving equipment and facility details on page 2-2.
5	Determine where the DS1 signal enters the network. See 323-1059-320, Retrieving end-to-end connections on page 1-2. If it is a EC-1/OC-3/OC-12/OC-48/OC-192 signal, check connecting equipment and ensure that is is correctly transmitting a DS1 signal.
6	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-55
DS1 Tx Frequency Out of Range

Probable cause

This alarm is raised when the network element detects that a DS1 signal transmitting into the input is out of the normal frequency range.

The DS1 that is out of frequency range on input to the system normally causes this alarm.

Impact

Major, service-affecting (M, SA) alarm

Note: The equipment may be unable to lock onto the DS1 and traffic may be lost.

Step	Action
1	Clear all SONET (OC-3, OC-12, OC-48, OC-192, STS-1, STS-3c, STS-12c, STS-24c, STS-48c, VT1.5) and DS1 Rx alarms from the network.
2	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-56
DS1 Tx Loss of Frame

Probable cause

This alarm is raised when the local network element detects that the DS1 payload from the VT1.5 transmitted from the shelf is not framed in the same format as the commissioned port.

Note 1: According to Telcordia GR-253-CORE, Loss of frame (LOF) on an async mapped DS1 does not result in AIS insertion. An alarm is raised, and the LOF signal passes downstream.

Note 2: This procedure assumes that the system was operating alarm free before the Tx loss of frame alarm. If this alarm is raised during DS1 provisioning, verify the provisioned framing with the test traffic you are running.

Impact

Major, service-affecting (M, SA) alarm

Note: The payload continues to transmit to the input. However, the change of framing can cause the equipment to reject the DS1 signal.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- clear all SONET (OC-3, OC-12, OC-48, OC-192, STS-1, STS-3c, STS-12c, STS-24c, STS-48c, VT) and DS1 Rx alarms from the network
- use an account with level 3 or higher user privilege code (UPC)

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Another failure in the system normally causes this alarm. Clear any other OC-3/OC-12/OC-48/OC-192/STS-1/VT1.5 or DS1 Rx alarms on the system first. Perform this procedure if the Tx LOF alarms are the only active alarms on the system.
3	Identify the DS1 or DSM DS1x84 termination module (TM) mapper raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
4	Record the AID in the form DS1-slot#-port#.

—continued—

Procedure 4-56 (continued)
DS1 Tx Loss of Frame

Step	Action
5	Retrieve the attributes of the DS1 or DSM DS1x84 (TM) you identified in step 4 from the Equipment and Facility Provisioning window. By default, the Table tab is enabled. Select the Detail tab for information specific to that circuit pack. Select the circuit pack under Equipment to display the Facility information. ***Note:*** When the Equipment and Facility Provisioning dialog box opens, it is a snapshot of the equipment and facility attribute values. Equipment and facility attributes do not automatically update as they change. Click Refresh to retrieve the current attribute values.
6	Compare the frame (FMT) attributes of the DS1 or DSM DS1x84 TM mappers. See 323-1059-350, Retrieving equipment and facility details on page 2-2. • If the two FMT attributes are different, determine which one is correct from company records and edit the incorrect facility. See 323-1059-350, Editing DS1, DS3, EC-1, 2x100BT-P2P or GE/FC SFP facility signal attributes on page 2-28. • If the condition does not clear, go to the next step.
7	Determine from the company records the location on the OPTera Metro 3500 shelves where the DS1 originates and retrieve the attributes as in step 5. **If** the source — **Then** go to is a DS1 mapper — step 8 is not a DS1 mapper — step 14
8	Manually switch the DS1 mapper you identified as the source into protection mode. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16. ***Note:*** Ensure the protection is not carrying traffic for another working mapper before you switch traffic from a working mapper to the protection mapper.
9	Wait 30 seconds. If the alarm clears, the working mapper is faulty. Replace the mapper you identified as the source. See Replacing a DS1 mapper on page 3-24.
10	Manually switch the DS1 mapper reporting the alarm into protection mode. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16. ***Note:*** For DS1 mappers, ensure the protection is not carrying traffic for another working mapper before you switch traffic from a working mapper to the protection mapper.

—continued—

Procedure 4-56 (continued)
DS1 Tx Loss of Frame

Step	Action
11	Wait 30 seconds. If the alarm clears, the working mapper is faulty. Replace the circuit pack reporting the Tx Loss of Frame alarm. See Replacing a DS1 mapper on page 3-24.
12	Release the manual switch you performed in step 10.
13	If the alarm does not clear, contact your next level of support or your Nortel Networks support group. You have completed this procedure.
14	If the source is a DSM DS1x84 termination module (TM) mapper, determine the original source of the DS1, the framing it is provisioned for, and ensure that it is generating the correct framing by using your company procedures.
15	Manually switch the DSM DS1x84 TM mapper reporting the alarm into protection mode. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16.
16	Wait 30 seconds. If the alarm clears, the working DSM DS1x84 TM mapper is faulty. Replace the DSM DS1x84 TM mapper reporting the Tx Loss of Frame alarm. See Replacing the DSM DS1x84 termination module mapper on page 3-26.
17	Release the protection switch you performed at step 15. See 323-1059-311, Releasing a protection switch on a tributary circuit pack on page 1-21.
18	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-57
DS3 Rx AIS

Probable cause

This alarm is raised when the network element detects an alarm indication signal (AIS) on the DS3 traffic stream at the input.

Note: This alarm can also be generated if a test access session is in progress, no action is required if this is the cause.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Identify the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
3	Use a DS3 test set to determine if a valid DS3 signal is on the DS3x3, DS3x12, DS3x12e, or DS3VTx12 cross-connect for that facility.
4	If there is AIS, the problem is in the DS3x3, DS3x12, DS3x12e, or DS3VTx12 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures.
5	If there is no AIS, operate a manual switch on the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper you identified. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16. ***Note:*** When a failed DS3x3, DS3x12, DS3x12e, or DS3VTx12 circuit pack is replaced with a functional circuit pack, traffic does not automatically switch back to the original circuit pack. You can manually switch traffic back to the circuit pack.

—continued—

Procedure 4-57 (continued)
DS3 Rx AIS

Step	Action
6	Wait 30 seconds. If the alarm clears, the working DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper is faulty. Replace the mapper that is detecting AIS. See Replacing the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper on page 3-30. ***Note:*** When a failed DS3x3, DS3x12, DS3x12e, or DS3VTx12 circuit pack is replaced with a functional circuit pack, traffic does not automatically switch back to the original circuit pack. You can manually switch traffic back to the circuit pack.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-58
DS3 Rx Bipolar Violations

Probable cause

This alarm is raised when the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper becomes faulty, or the signal from outside DS3x3, DS3x12, DS3x12e, or DS3VTx12 sources is degraded. A bipolar violation alarm means that two +1V or two -1V binary ones transmitted consecutively without an opposite voltage binary one in between and the errors occurred at a rate greater than 10^{-3} a second.

DS3 protocol uses ground as a binary zero and both +1V and -1V as binary ones. The polarity of ones is always toggled, which gives the signal desirable electrical characteristics and can be used to detect signal errors. This system is called a bipolar system.

Impact

Major, service-affecting (M, SA) alarm

Note: The DS3 signal is severely degraded.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	Use a DS3 test set to determine if a valid DS3 signal is on the cross-connect for that facility. • If there are BPVs, the problem is in the DS3x3, DS3x12, DS3x12e, or DS3VTx12 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. • If there are no BPVs, go to the next step.

—continued—

Procedure 4-58 (continued)
DS3 Rx Bipolar Violations

Step	Action
4	Manually switch the mapper into protection mode. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16.
5	Wait 30 seconds. If the alarm clears, the working DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper is faulty. Replace the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper that is detecting BPVs. See Replacing the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper on page 3-30. ***Note:*** When a failed DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper is replaced with a functional circuit pack, traffic does not automatically switch back to the original circuit pack. The user can manually switch traffic back to the circuit pack.
6	If the alarm does not clear, inspect the DS3x3, DS3x12, DS3x12e, or DS3VTx12 cabling and connections on the BNC 12-port I/O module. The cabling may be loose or damaged. Repair any damage.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-59
DS3 Rx Frame Format Mismatch

Probable cause

This alarm is raised when the frame format provisioned for a DS3 facility on a DS3VTx12 circuit pack does not match the frame format of the received signal, that is, one format uses M23 framing and the other format uses C-bit framing.

> ***Note:*** If a DS3 facility on a DS3VTx12 circuit pack is provisioned for C-bit framing but the received signal uses M23 framing, then the channelized DS3 signal cannot be demultiplexed into 28 DS1 signals. In this case, 28 DS1 AIS are transmitted toward the optics.
> If a DS3 facility on a DS3VTx12 circuit pack is not provisioned for C-bit framing but the received signal uses C-bit framing, then only the third DS2 (DS1s 9, 10, 11, and 12) cannot be demultiplexed. In this case, 4 DS1 AIS are transmitted toward the optics for the paths that correspond to DS1s 9, 10, 11, and 12.

Impact

Major, service-affecting (M, SA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify the DS3VTx12 mapper raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Modify the frame format of the DS3 facility so that it matches the frame format of the received signal. See 323-1059-350, Editing DS1, DS3, EC-1, 2x100BT-P2P or GE/FC SFP facility signal attributes on page 2-28.
3	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-60
DS3 Rx Frequency Out of Range

Probable cause

This alarm is raised when the network element detects a signal on a DS3 input that is out of the normal frequency range of a DS3x3, DS3x12, or DS3x12e mapper.

Impact

Major, service-affecting (M, SA) alarm

Note: The shelf may be unable to carry traffic.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify the DS3x3, DS3x12, or DS3x12e mapper raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	Use a DS3 test set to determine if a valid DS3 signal is on the cross-connect for that facility. • If there is a frequency that is out of range for DS3x3, DS3x12, or DS3x12e, the problem is in the DS3 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. • If there are no such conditions, go to the next step.
4	Manually switch the circuit into protection mode. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16.

—continued—

Procedure 4-60 (continued)
DS3 Rx Frequency Out of Range

Step	Action
5	Wait 30 seconds. If the alarm clears, the working DS3x3, DS3x12, or DS3x12e mapper is faulty. Replace the mapper that is detecting frequency out of range. See Replacing the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper on page 3-30. ***Note:*** When a failed DS3x3, DS3x12, or DS3x12e mapper is replaced with a functional circuit pack, traffic does not automatically switch back to the original circuit pack. The user can manually switch traffic back to the circuit pack.
6	If the alarm does not clear, contact your next level of support or your Nortel Networks support group. **—end—**

Procedure 4-61
DS3 Rx Loss of Frame

Probable cause

The DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper is faulty, or the framing format from the received DS3 is not compatible, or the incoming quality of the signal is degraded.

Note 1: This procedure assumes that the provisioned framing is correct and was not changed to create the alarm.

Note 2: This procedure assumes that the upstream and downstream network elements have been operating with the same frame format configuration. It also assumes that the alarm is not caused by provisioning activity.

Impact

Major, service-affecting (M, SA) alarm

Note: The shelf cannot carry traffic.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	Use a DS3 test set to determine if a valid DS3 signal is on the DS3x3, DS3x12, DS3x12e, or DS3VTx12 cross-connect for that facility. • If there is an LOF or incorrect framing, the problem is in the DS3 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. • If there are no such conditions, go to the next step.

—continued—

Procedure 4-61 (continued)
DS3 Rx Loss of Frame

Step	Action
4	Manually switch the circuit into protection mode. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16.
5	Wait 30 seconds. If the alarm clears, the working DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper is faulty. Replace the mapper that is detecting LOF. See Replacing the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper on page 3-30. ***Note:*** When a failed DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper is replaced with a functional circuit pack, traffic does not automatically switch back to the original circuit pack. The user can manually switch traffic back to the circuit pack.
6	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-62
DS3 Rx Loss of Signal

Probable cause

This alarm is raised when one of the following conditions exists:

- theDS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper is faulty
- the DS3 signal stopped transmitting from the adjacent network element
- the BNC 12-port I/O module was removed
- the BNC 12-port I/O module is not fully inserted and locked into position

Impact

Major, service-affecting (M, SA) alarm

Note: The shelf cannot carry traffic.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify theDS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	Ensure the corresponding I/O module is fully inserted and locked into position.
4	Use a DS3 test set to determine if a valid DS3 signal is on the cross-connect for that facility. • If there is a LOS, the problem is in the DS3 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. • If there is no LOS, go to the next step.
5	Manually switch the circuit into protection mode. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16.

—continued—

Procedure 4-62 (continued)
DS3 Rx Loss of Signal

Step	Action
6	Wait 30 seconds. If the alarm clears, the working mapper is faulty. Replace the mapper that is detecting LOS. See Replacing the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper on page 3-30. ***Note:*** When a failed DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper is replaced with a functional circuit pack, traffic does not automatically switch back to the original circuit pack. The user can manually switch traffic back to the circuit pack.
7	If the alarm does not clear, inspect the DS3 cabling and the DS3 connection. The cabling and connection are on the BNC 12-port I/O module. The cabling may be loose or damaged. Repair any damage.
8	If the alarm does not clear, contact your next level of support or your Nortel Networks support group. **—end—**

Procedure 4-63
DS3 Rx Parity Er Rate Exceeds 10E-6

Probable cause

This alarm is raised when a DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper detected parity errors coming from the DS3 input signal. One of the following conditions exists:

- faulty DS3 input cable or connector
- problem with the DS3 signal source
- faulty DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper

Impact

Minor, non-service-affecting (m, NSA) alarm

Note: Traffic is being reported down by the remote system.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201.

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Unplug the DS3 cable and connect it to a DS3 receiver test set. Verify that a DS3 signal is on the cable and the test set does not detect any errors.

CAUTION
Risk of service loss
Ensure that the correct DS3 cable is unplugged. Removing the wrong cable will cause another DS3 signal to be lost.

3	If there is no signal, repair and reconnect the DS3 cable. If there are errors, repair the source generating the DS3 signal.
4	If the alarm does not clear, replace the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper carrying this facility. See Replacing the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper on page 3-30.
5	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-64
DS3 Rx Yellow

Probable cause

This alarm is raised when the remote network element detects a defective DS3 signal from the OPTera Metro 3500 network element and returns a Yellow signal in the DS3 overhead.

Impact

Minor, non-service-affecting (m, NSA) alarm

Note: Traffic is being reported down by the remote system.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201
- use an account with level 2 or higher UPC

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Identify the DS3x3, DS3x12, or DS3x12e circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
3	Use a DS3 test set to determine if a valid DS3 signal is on the cross-connect for that facility. • If there is a valid signal on the transmit side and there is Yellow on the receive side, the problem is in the DS3 source system. The shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. • If there are no such conditions, go to the next step.

—continued—

Procedure 4-64 (continued)
DS3 Rx Yellow

Step	Action
4	Manually switch the circuit into protection mode. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16. ***Note:*** Ensure the protection circuit pack is not carrying traffic for another working mapper before you switch traffic from a working mapper to the protection mapper.
5	Wait 30 seconds. If the alarm clears, the working DS3x3, DS3x12, or DS3x12e mapper is faulty. Replace the DS3x3, DS3x12, or DS3x12e mapper that is detecting Rx Yellow. See Replacing the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper on page 3-30. ***Note:*** When a failed DS3x3, DS3x12, or DS3x12e mapper is replaced with a functional mapper, traffic does not automatically switch back to the original circuit pack. The user manually switches traffic back to the circuit pack.
6	If the alarm does not clear, inspect the DS3 cabling and the DS3 connection. The cabling and connection are on one of the OPTera Metro 3500 BNC 12-port I/O modules. The cabling may be loose or damaged. Repair any damage.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-65
DS3 test signal active

Probable cause

This alarm is raised when the loopback active message appears after a connect test signal command is executed for facility testing.

Note: The facility must be out of service for memory administration (OOS-MA) to be put in test signal mode.

Impact

Minor, non-service-affecting (m, NSA) alarm

Note: The facility must be OOS (out of service) to operate the command to turn on the test signal, so there is no effect on current shelf functions.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201
- use an account with level 2 or higher UPC

Step	Action
1	From the navigation tree, select the network element with the DS3 in test mode.
2	Identify the DS3x3, DS3x12, or DS3x12e mapper in test mode. See Retrieving active alarms for a network element on page 2-3.
3	If testing indicates a damaged port, replace the faulty circuit pack. See Replacing the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper on page 3-30.
4	Identify the DS3 in test mode. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
5	Release the DS3 signal you identified. **a.** Select Equipment and Facility Provisioning from the Configuration menu. **b.** Select the circuit pack with the DS3 in test mode from the Equipment list. **c.** Select the DS3 port with the DS3 in test mode from the Facility list. **d.** Click Test to open the Test Functions window. **e.** Click Release in the Test Functions window. **f.** Close the Test Functions window.

—end—

Procedure 4-66
DS3 Tx AIS

Probable cause

This alarm is raised when the network element detects a failed signal coming from a DS3x3, DS3x12, or DS3x12e mapper upstream on the optical fiber side. The network element is transmitting an alarm indication signal (AIS) to the remote end of the input.

The alarm indicates a warning to the downstream network element that the signal is bad.

The following causes this alarm:

- a DS3 receive fault (for example, Rx LOS, LOF, AIS) on the upstream mapper
- a SONET fault condition (OC-3, OC-12, OC-48, STS-1 alarms)
- no cross-connect for the DS3

Impact

Minor, non-service-affecting (m, NSA) alarm

Note: The shelf cannot carry traffic on this DS3x3, DS3x12, or DS3x12e mapper.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- clear all SONET (OC-3, OC-12, OC-48, STS-1) and DS3 Rx alarms from the network.

Step	Action
1	Another failure in the system usually causes this alarm. Clear any other OC-3, OC-12, OC-48, STS1 or DS3 Rx alarms on the system first. Perform this procedure if the Tx AIS alarms are the only active alarms on the system.
2	Identify the DS3x3, DS3x12, or DS3x12e mapper raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
3	Record the AID in the form DS3-slot#-port#.
4	If there are any connections to the DS3x3, DS3x12, or DS3x12e, contact your next level of support or your Nortel Networks support group.

—continued—

Procedure 4-66 (continued)
DS3 Tx AIS

Step	Action
5	If there are no connections, the DS3x3, DS3x12, or DS3x12e is in-service without connections. Put the DS3x3, DS3x12, or DS3x12e facility out of service. See 323-1059-350, Changing a facility state to Out of Service (OOS) on page 2-25.

—end—

Procedure 4-67
DS3 Tx Frequency Out of Range

Probable cause

This alarm is raised when the network element detects a DS3 signal that is transmitting to the input out of normal frequency range. The DS3 out of frequency range on the input to the system usually causes this alarm. A DS3 Rx frequency out of range alarm should also be active.

Impact

Major, service-affecting (M, SA) alarm

Requirements

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

Step	Action
1	Clear all SONET (OC-3, OC-12, OC-48, STS-1) and DS3 Rx alarms from the network.
2	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-68
DS3 Tx Loss of Frame

Probable cause

This alarm is raised when the local network element detects that the DS3 payload from the STS-1 transmitted from the shelf is not framed in the same format as the commissioned port.

Note 1: According to Telcordia GR-253-CORE, loss of frame on an async mapped DS3 does not result in AIS insertion. An alarm is raised, and the LOF signal passes downstream.

Note 2: This procedure assumes the system was operating alarm free before the Tx loss of Frame alarm. If this alarm is raised during DS3 provisioning, verify the provisioned framing with the running test traffic.

Impact

Major, service-affecting (M, SA) alarm

Note: The payload continues to transmit to the input, but the change of framing can cause the equipment to reject the DS3x3, DS3x12, or DS3x12e mapper.

Requirements

Before you perform this procedure, you must

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

Step	Action
1	Another failure in the system usually causes this alarm. Clear any other OC-3/OC-12/OC-48/STS-1/VT1.5, or DS3 Rx alarms on the system first. Perform this procedure if the Tx LOF alarms are the only active alarms.
2	Identify the DS3x3, DS3x12, or DS3x12e mapper raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
3	Record the AID in the form DS3-slot#-port#.

—continued—

Procedure 4-68 (continued)
DS3 Tx Loss of Frame

Step	Action
4	Retrieve the attributes of the DS3 facility you recorded. See 323-1059-350, Retrieving equipment and facility details on page 2-2. ***Note:*** The Equipment & Facility Provisioning dialog box is a snapshot of the equipment and facility attribute values. Equipment and facility attributes do not update as they change. Click Refresh to retrieve the current attribute values.
5	Determine from the company records the location on the OPTera Metro 3500 shelves where the signal originates. If the source is a DS3x3, DS3x12, or DS3x12e mapper in the system, go to step 6. If the source is not a DS3x3, DS3x12, or DS3x12e mapper, go to step 17.
6	Retrieve the attributes of the DS3x3, DS3x12, or DS3x12e mappers you identified. See 323-1059-350, Retrieving equipment and facility details on page 2-2. ***Note:*** When the Equipment & Facility Provisioning dialog box opens, it is a snapshot of the equipment and facility attribute values. Equipment and facility attributes do not automatically update as they change. Click Refresh to retrieve the current attribute values.
7	Compare the frame (FMT) attributes of the two DS3x3, DS3x12, or DS3x12e mappers. • If the two framing attributes are different, determine which one is correct from company records and edit the incorrect framing parameter: — Select Equipment and Facility Provisioning from the Configuration drop-down list. — Select the Table tab. — Select the Active DS3x3, DS3x12, or DS3x12e mapper under the Equipment drop-down list. — Select the required port under the Port list. — Click Edit to open the Edit Facility DS3 dialog box. — Change the Primary state to OOS. — Click Apply. — Click Yes in the confirmation dialog box. — Edit the attributes as required. — Click Apply. — Change the Primary state to IS. — Click OK. • If the condition does not clear go to the next step.

—continued—

Procedure 4-68 (continued)
DS3 Tx Loss of Frame

Step	Action
8	Manually switch the DS3x3, DS3x12, or DS3x12e mapper you identified as the source into protection mode. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16.
9	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
10	Wait 30 seconds. If the alarm clears, the working DS3x3, DS3x12, or DS3x12e mapper is faulty. Replace the DS3x3, DS3x12, or DS3x12e mapper you identified as the source. See Replacing the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper on page 3-30. ***Note:*** When a failed DS3x3, DS3x12, or DS3x12e mapper is replaced with a functional circuit pack, traffic does not automatically switch back to the original circuit pack. The user can manually switch traffic back to the circuit pack.
11	If the alarm clears, you have completed this procedure.
12	Manually switch the DS3x3, DS3x12, or DS3x12e mapper reporting the alarm into protection mode. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16.
13	Wait 30 seconds. If the alarm clears, the working DS3x3, DS3x12, or DS3x12e mapper is faulty. Replace the DS3x3, DS3x12, or DS3x12e mapper reporting the Tx loss of frame alarm. See Replacing the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper on page 3-30. ***Note:*** When a failed DS3x3, DS3x12, or DS3x12e mapper is replaced with a functional circuit pack, traffic does not automatically switch back to the original circuit pack. The user can manually switch traffic back to the circuit pack.
14	If the alarm clears, you have completed this procedure.
15	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.
16	If the source is not a DS3x3, DS3x12, or DS3x12e mapper, determine the original source of the DS3 signal, the framing provisioned, and ensure that it is generating the correct framing by using your company procedures.

—continued—

Procedure 4-68 (continued)
DS3 Tx Loss of Frame

Step	Action
17	Manually switch the DS3x3, DS3x12, or DS3x12e mapper reporting the alarm into protection mode. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16. ***Note:*** Because DS3x3, DS3x12, or DS3x12e protection switching is 1+1 nonrevertive, traffic that has been switched (forced) to one circuit pack does not automatically switch back to the other circuit pack of the protected pair. Manual switches cannot be released. You can move traffic between the circuit packs of the protected pair by performing another manual switch.
18	Wait 30 seconds. If the alarm clears, the working DS3x3, DS3x12, or DS3x12e mapper is faulty. Replace the DS3x3, DS3x12, or DS3x12e circuit pack reporting the Tx loss of frame alarm. See Replacing the DS3x3, DS3x12, DS3x12e, or DS3VTx12 mapper on page 3-30. ***Note:*** When a failed DS3x3, DS3x12, or DS3x12e mapper is replaced with a functional circuit pack, traffic does not automatically switch back to the original circuit pack. The user can manually switch traffic back to the circuit pack.
19	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-69
DSM Fan Failure

Probable cause

This alarm is raised when a cooling unit in the fan module of the DS1 service module (DSM) is equipped but fails.

Impact

Critical, service-affecting (C, SA) alarm if all three cooling units fail
Minor, non-service-affecting (m, NSA) alarm if less than three cooling units fail in the module

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Replace the fan module of the DSM. See Replacing a fan module on the DS1 service module on page 3-54.
3	Retrieve all alarms to determine if the alarm has cleared and ensure the red LED is off.
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-70
DSM Fan Missing

Probable cause

This alarm is raised on a DS1 service module (DSM) when the cooling unit fan module is missing.

Impact

Critical, service-affecting (C, SA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Replace the fan module of the DSM. See Replacing a fan module on the DS1 service module on page 3-54.
3	Retrieve all alarms to determine if the alarm has cleared.
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-71
DSM-HOST Misconnection

Probable cause

This alarm is raised against a Host optical interface (OCn) facility if the Host OCn facility is a prov-link of one DSM DS1x84 termination module (TM) mapper but

- is linked by fiber to an OCn port in another optical interface circuit pack
- is linked by fiber to an OCn port in another optical interface circuit pack in another network element
- is linked by fiber to the incorrect DSM DS1x84 TM mapper of the same DS1 service module (DSM)
- is linked by fiber to a DSM DS1x84 TM mapper in another DSM (if this is a protected scenario only)
- has a misconnected DSM DS1x84 TM mapper in the same DSM DS1x84 TM

Impact

Critical, service-affecting (C, SA) alarm if the OC-3 facility is active
Major, non-service-affecting (M, NSA) alarm if not active

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Select Inventory from the Configuration menu to see if the DSM DS1x84 TM is displayed in the inventory list. If the DSM DS1x84 TM inventory is displayed then an OAM link exists. Go to step 2. If the DSM DS1x84 TM is not displayed in the inventory list, there is no OAM link, verify the fiber-links.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	If you want an unprotected connection, verify that the Host OC-3 is fiber-linked to the slot 1 DSM DS1x84 TM mapper of the correct DSM and that provisioning is for that slot 1 DSM DS1x84 TM.

—continued—

Procedure 4-71 (continued)
DSM-HOST Misconnection

Step	Action
4	**CAUTION** **Risk of misconnection** Ensure the fibers from the OC-3 hosts are connected to the intended DSM. If you have two DSMs that will use two different OC-3 facilities, perform a lamp test to verify that you have connected the fiber to the intended DSM. If the fiber is not connected to the intended DSM, link the fiber to the appropriate OC-3 line facility of the DSM DS1x84 TM mapper in the correct DSM.
5	If you want a protected connection, verify that the DSM DS1x84 TM mapper in slot 2 of the DSM is not connected: • to another network element • to another DSM DS1x84 TM mapper in another DSM • to the wrong OCn on the same network element ***Note:*** If two DSMs are misconnected, the condition may only show up as one misconnection alarm.
6	If any situation from step 5 is true, link the fiber to the appropriate OC-3 line facility for the DSM DS1x84 TM mapper on the correct DSM.
7	If the alarm does not clear, look for an Intercard suspected alarm on both the DSM DS1x84 TM mappers and clear them first. See Intercard Suspected on page 4-200.
8	Select Active Alarms from the Faults drop-down menu to retrieve alarms and determine if the misconnection alarm cleared.
9	If the alarm does not clear, verify the parity of the connection • Host OC-3 odd slot-port to DSM DS1x84 termination module-1 • Host OC-3 even slot-port to DSM DS1x84 termination module-2
10	If the alarm does not clear, verify that the even slot Host OC-3 is connected to the same DSM as the odd slot Host OC-3. ***Note:*** Match the serial numbers of the working and mate circuit packs from the inventory list to verify the connection is to the same DSM. If the connection is to a different DSM, go to step 9.
11	Link the fiber from the OC-3 line facility to the DSM DS1x84 TM mapper in the appropriate DSM.

—end—

Procedure 4-72
DSM Low Voltage

Probable cause

This alarm is raised when an active DS1 service module (DSM) detects the power input is above -38V. The DSM enters or exits this brownout state regardless of the power status on the host shelf or on other DSMs attached to the shelf. When the DSM is in a brownout state it will not report any other alarms on the DSM to the shelf.

Impact

Critical, service-affecting (C, SA) alarm

CAUTION
Risk of traffic loss
Do not reseat any circuit pack while this alarm is active. Unexpected problem conditions result when a circuit pack is reseated.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201.

Step	Action
1	Verify the power supply to the DSM box raising the alarm. Use your company procedure to clear the power supply problem. This alarm is cleared when the DSM monitor input power is below -42V. ***Note:*** When the DSM detects that the input power has recovered to below -42V the DSM will automatically perform a cold restart on the slot 2 DSM DS1x84 termination module (TM) mapper and then the slot 1 DSM DS1x84 TM mapper.
2	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-73
DSM Power Failure - A or DSM Power Failure - B

Probable cause

This alarm is raised when the DS1 service module (DSM) detects that no voltage exists on the A or B backplane power bus for the DSM.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Use a voltmeter to measure the voltage available at the power input connectors. The power input connectors are on the power module accessible from the left side of the DSM.
3	If 48V dc is not on both of the power inputs, and if the 5A breaker is good, then the bay power supply is faulty. Use your company procedures to clear the problem.
4	If the breaker tripped, press the breaker button back in to reset it.
5	If the alarm does not clear, replace the OAM module. See Replacing the DSM-OAM adapter module on page 3-82.
6	If the alarm does not clear, and the breaker does not remain set, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-74
DSM SITE Provisioning Required

Probable cause

This alarm is raised against the DS1 service module (DSM) when the address is not defined. The site address defines a shelf-wide unique identifier for each DSM on an OPTera Metro 3000 series shelf. The address must be manually provisioned and until it is provisioned the DSM DS1x84 termination module (TM) mappers in the DSM remain out of service.

Note 1: It is possible to edit the site address but you cannot delete it.

Note 2: Taking the DSM DS1x84 TM mappers out of service (OOS-MA or OOS-AUMA) masks the alarm.

Impact

Critical, service-affecting (C, SA) alarm if the DSM is provisioned with cross connections
Minor, non-service-affecting (m, NSA) alarm if the DSM is provisioned and has no cross connections

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201
- use an account with a level 3 user privilege code (UPC)

Step	Action
1	Edit the DSM site address. See 323-1059-350, Defining or editing a site address for a DSM on page 2-11.
2	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-75
Duplicate SID Detected

Probable cause

This alarm is raised 20 minutes after a shelf processor or network processor restart.

The local network element or network processor detects another network element or network processor with the same source identifier (SID).

The alarm occurs at the same time at all network elements or network processors that share the same SID. Each shelf processor detects the condition.

> ***Note:*** This procedure only works when executed from one duplicate SID network element or network processor.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with a level 4 user privilege code (UPC)
- be able to log in to the nodes that do not have a unique SID

Step	Action
1	Identify the network element or network processor raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Select one of the alarmed network elements or network processors from the navigation tree.
3	Build the NSAP. See 323-1059-520, Building or editing an NSAP value on page 6-10.
4	Perform step 2 and step 3 for each network element or network processor raising this alarm.
5	Determine from network plans or other documents which network element or network processor has the correct System ID.

—continued—

Procedure 4-75 (continued)
Duplicate SID Detected

Step	Action
6	If a network element has the incorrect System ID, go to that network element site and directly log in to the incorrectly named network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1. If a network processor has the incorrect name, log in to the NP and open the Map view. See 323-1059-302, Procedures for logging in to a network element on page 2-1. ***Note 1:*** If an network processor restart occurs, you cannot access the network processor until the network processor database is released. ***Note 2:*** If you log in to a network processor using an account with a level 5 user privilege code (UPC), you automatically log into all the network elements in the network processor span of control. ***Note 3:*** If you get a "Status, Data Not Consistent" error message after any configuration retrieval, try the command again after approximately 3 minutes. If the same error message appears, verify each network element in the network processor span of control to ensure that no SDCC failure alarms exist. Clear any SDCC failure alarms. Correct any SDCC links that are out of service (OOS) by placing the support facilities and equipment in service (IS).
7	**CAUTION** **Risk of loss of functionality** Ensure every network element and network processor has a unique system identifier (SID). If you are changing the name of a network element or network processor, ensure that the new name is unique. Rename the network element if it has an incorrect name. See 323-1059-302, Changing the name of a network element or network processor on page 3-37. ***Note:*** After a shelf processor or network processor restart, the Duplicate SID alarm is masked for 20 minutes.

—continued—

Procedure 4-75 (continued)
Duplicate SID Detected

Step	Action
8	**CAUTION** **Risk of loss of functionality** Ensure every network element and network processor has a unique system identifier (SID). If you are changing the name of a network element or network processor, ensure that the new name is unique. Rename the network processor if it has an incorrect name. See 323-1059-302, Changing the name of a network element or network processor on page 3-37. ***Note 1:*** After a shelf processor or network processor restart, the Duplicate SID alarm is masked for 20 minutes. ***Note 2:*** If the default network processor name is changed, an error message appears.
9	Repeat step 1 to ensure no other duplicate SIDs exist. If there are other duplicate SIDs, repeat this procedure for the new duplicate.
10	If the alarm does not clear after renaming all duplicate SIDs, contact your next level of support or your Nortel Networks support group. **—end—**

Procedure 4-76
EC1 Loopback Active

Probable cause

This alarm is raised when one user executes a loopback command. The loopback active alarm is an advisory message to other users that a loopback is active.

Note 1: The unavailability of a circuit can affect other maintenance being performed at the same time.

Note 2: The facility is in out-of-service-for-memory-administration (OOS-MA) mode while in loopback mode.

Impact

Minor, non-service-affecting (m, NSA) alarm

Note: The facility must be OOS (out of service) to engage the loopback, so this command cannot affect shelf function.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC).

Step	Action
1	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52. ***Note:*** This procedure assumes that testing is complete and the circuit is ready to be released from loopback mode.
2	Release the EC-1 loopback. See 323-1059-222, Releasing a software loopback on page 2-58.

—end—

Procedure 4-77
EC1 Rx AIS

Probable cause

This alarm is raised when the network element detects an alarm indication signal (AIS) on the EC-1 traffic stream at the input.

> ***Note:*** This alarm can also be generated if a test access session is in progress, no action is required if this is the cause.

Impact

Major, service-affecting (M, SA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	Use an EC-1 test set to determine if a valid EC-1 signal is on the EC-1 cross-connect for that facility. • If there is AIS, the problem is in the EC-1 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. You have completed this procedure. • If there is no AIS, go to the next step.

—continued—

Procedure 4-77 (continued)
EC1 Rx AIS

Step	Action
4	Operate a manual switch on the EC-1x3 or EC-1x12 circuit pack raising the alarm. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16.
5	Wait 30 seconds. If the alarm clears, the working EC-1x3 or EC-1x12 circuit pack is faulty. Replace the circuit pack that is detecting AIS. See Replacing the EC-1x3 or EC-1x12 circuit pack on page 3-32.
6	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-78
EC1 Rx Loss of Frame

Probable cause

The EC-1x3 or EC-1x12 circuit pack is faulty or a signal is being transmitted from the adjacent network element without properly formatted frames.

Impact

Major, service-affecting (M, SA) alarm

Note: The shelf cannot carry traffic.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	Use an EC-1 test set to determine if a valid EC-1 signal is on the cross-connect for that facility. • If there is an LOF, the problem is in the EC-1 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. You have completed this procedure. • If there are no such conditions, go to the next step.
4	Operate a manual switch on the EC-1x3 or EC-1x12 circuit pack raising the alarm. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16.
5	Wait 30 seconds. If the alarm clears, the working circuit pack is faulty. Replace the EC-1x3 or EC-1x12 circuit pack that is detecting LOF. See Replacing the EC-1x3 or EC-1x12 circuit pack on page 3-32.
6	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-79
EC1 Rx Loss of Signal

Probable cause

This alarm is raised when:

- the EC-1x3 or EC-1x12 circuit pack is faulty
- the EC-1 signal stops transmitting from the adjacent network element
- the EC-1 input cable is disconnected or misconnected from the BNC 12-Port I/O module
- the BNC 12-Port I/O module was removed
- the BNC 12-Port I/O module is not fully inserted and locked into position

Impact

Major, service-affecting (M, SA) alarm

Note: The shelf cannot carry traffic.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
3	Ensure the corresponding I/O module is fully inserted and locked into position.
4	Use an EC-1 test set to determine if a valid EC-1 signal is on the cross-connect for that facility. • If there is a LOS, the problem is in the EC-1 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. You have completed this procedure. • If there are no such conditions, go to the next step.

—continued—

Procedure 4-79 (continued)
EC1 Rx Loss of Signal

Step	Action
5	If the alarm does not clear, inspect the EC-1x3 or EC-1x12 cabling and physical connections. The connection may be loose or damaged. Repair any damage.
6	Operate a manual switch on the EC-1x3 or EC-1x12 circuit pack raising the alarm. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16.
7	Wait 30 seconds. If the alarm clears, the EC-1x3 or EC-1x12 circuit pack that raised the alarm is faulty. Replace the EC-1x3 or EC-1x12 circuit pack that is detecting LOS. See Replacing the EC-1x3 or EC-1x12 circuit pack on page 3-32.
8	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-80
EC1 Rx RFI

Probable cause

This alarm is raised when the remote network element detects a faulty EC-1 signal from the network element and returns a remote fault indicator (RFI) signal in the SONET overhead.

Impact

Minor, non-service-affecting (m, NSA) alarm

Note: Traffic is being reported down by the remote system.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Verify the remote system at the other end of the EC-1 and clear any alarms you find.

If the alarm	**Then**
clears	you have completed this procedure
does not clear	go to step 2

Step	Action
2	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
3	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
4	Use an EC-1 test set to determine if a valid EC-1 signal is on the transmit and receive sides of the cross-connect for that facility.

If a valid signal	**Then**
is on the transmit side and RFI is on the receive side	the problem is in the source system. Perform troubleshooting on the source system according to your company procedures. You have completed this procedure.
is not on the transmit side and RFI is not on the receive side	go to step 6

—continued—

Procedure 4-80 (continued)
EC1 Rx RFI

Step	Action
5	If the alarm does not clear, inspect the EC-1x3 or EC-1x12 cabling and physical connections. The connection may be loose or damaged. Repair any damage.
6	Operate a manual switch on the EC-1x3 or EC-1x12 circuit pack raising the alarm. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16.
7	Wait 30 seconds. If the alarm clears, the working circuit pack is faulty. Replace the EC-1x3 or EC-1x12 circuit pack that is detecting Rx RFI. See Replacing the EC-1x3 or EC-1x12 circuit pack on page 3-32.
8	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-81
EC1 Rx Signal Degrade

This alarm is raised when the EC-1x3 or EC-1x12 circuit pack is faulty or the EC-1 signal is degraded. Signal quality is measured using the bit interleaved parity (BIP) information from the B2 byte of the line overhead. This alarm is raised when the BIP error rate is above the 10^{-6} threshold.

Impact

Minor, service-affecting (m, SA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201
- use an account with level 2 or higher user privilege code (UPC)

Step	Action
1	Identify the circuit pack that raised the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	Use an EC-1 test set to determine if a valid EC-1 signal is on the cross-connect for that facility. • If the signal degraded (contains B2 errors), the problem is in the EC-1 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. You have completed this procedure. • If the signal is not degraded, go to the next step.
4	Operate a manual switch on the EC-1x3 or EC-1x12 circuit pack raising the alarm. See 323-1059-311, Operating a manual switch on a tributary circuit pack on page 1-16.
5	Wait 30 seconds. If the alarm clears, the working EC-1x3 or EC-1x12 circuit pack is faulty. Replace the circuit pack that is detecting the signal degrade. See Replacing the EC-1x3 or EC-1x12 circuit pack on page 3-32.
6	If the alarm does not clear, inspect the cabling around the input connector of the affected port. Look for misconnected, damaged or loose cables. Repair any damage.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-82
Equipment below baseline

Probable cause

This alarm is raised when the installed power modules and cooling unit assembly are below the required baseline. When STX-192 circuit packs are provisioned in the OPTera Metro 3500 shelf, 20 A power modules (NTN451HA) and the cooling unit assembly (NTN458QA) are required.

Impact

Major, non-service-affecting (M, NSA) alarm

Requirements

Before you perform this procedure, ensure you have the documentation referenced in this procedure.

Step	Action
1	Install the power module and cooling unit upgrade kit (NTN458MW). See Installing the power module and cooling unit upgrade kit on page 3-55.

—end—

Procedure 4-83
Equipment upgrade failed

Probable cause

This alarm is raised if a failure occurs during a line rate upgrade of optical interface circuit packs.

Impact

Minor, non-service-affecting (m, NSA) alarm

Step	Action
1	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Use the appropriate save and restore procedure to restore the network element to its previous state. Refer to 323-1059-302, Procedures for provisioning data and software management on page 6-1.
3	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-84
Equipment upgrade in progress

Probable cause

This alarm is raised when an optical line rate upgrade is in progress. The alarm clears after the upgrade is complete.

Note: This alarm is for information only. Do not perform any actions other than the upgrade activity while it is active. The alarm clears after the upgrade is complete.

Impact

Major, non-service-affecting (M, NSA) alarm

Step	Action
1	If the alarm does not clear for an unreasonable length of time (more than 5 minutes), contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-85
Equipment upgrade required

Probable cause

This alarm is raised to indicate that the mate OC-3 or OC-12 circuit pack needs to be upgraded after a reconfiguration is performed on a pair of OC-3 or OC-12 circuit packs in linear 1+1 mode.

Note: This alarm is not raised in UPSR mode.

Impact

Minor, non-service-affecting (m, NSA) alarm

Step	Action
1	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Use the appropriate save and restore procedure to restore the network element to its previous state. Refer to 323-1059-302, Procedures for provisioning data and software management on page 6-1.
3	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-86
Ethernet loopback active

Probable cause

This alarm is raised when a user executes a loopback command on an Ethernet facility of a 2x100BT-P2P or 2xGigE/FC-P2P circuit pack. The alarm notifies other users that a loopback is active.

Note: This procedure assumes that testing is complete and the circuit pack can be released from loopback mode.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)

Step	Action
1	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Release the loopback. See 323-1059-222, Releasing a software loopback on page 2-58.

—end—

Procedure 4-87
Facility Failure

Probable cause

This alarm is raised on the network processor if any of the following conditions exists:

- hardware diagnostics fail when provisioning the X.25 facility
- stack provisioning fails or a file-access failure occurs when provisioning the X.25 facility or executing an X.25 TL1 command
- no Rx link activity is detected within 10 seconds for ILAN facilities or within 2 seconds for the COLAN facility
- the network processor and the co-located shelf processor do not share the same manual area address (MANAREA)

  Note: Alarm clearing time is 30 seconds for ILAN facilities and 10 seconds for COLAN.

Impact

Minor, non service-affecting (M, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure

Step	Action
1	Look for the Remote Fail alarm on the network processor and follow that procedure to clear this alarm. See Remote Fail on page 5-147. This alarm clears on its own when the condition clears or when the affected facility is deprovisioned.

—end—

Procedure 4-88
Facility Provisioned Mismatch

Probable cause

This alarm is raised when there are more facilities provisioned on a slot than the equipment can support. For example, this alarm will be raised if a DS3x3 mapper is inserted in a slot that has been provisioned with 12 facilities. This alarm is raised against DS3x3, EC-1x3, OC-3, and OC-12 circuit packs.

Impact

Critical, service-affecting (C, SA) alarm (when cross-connects are provisioned) on the unsupported facilities
Minor, non-service-affecting (m, NSA) alarm, when cross-connects are not provisioned) on the supported facilities

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Select the network element in the navigation tree and select Shelf Level View from the Configuration menu.
2	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
3	Identify the circuit pack in the mate slot. Ensure the mate circuit pack has the same number of ports available as does the odd slot circuit pack. If the same number of ports are not available, the pair is mismatched.
4	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
5	Replace the mate circuit pack which raised the alarm with the appropriate circuit pack. See Procedures for equipment replacement on page 3-1. Wait 30 seconds for the circuit pack to provision.
6	If you have inserted a DS3x3 mapper into an odd slot that was provisioned for a DS3x12 or DS3x12e mapper and you want to work with a DS3x3 mapper, delete ports 4 through 12. See 323-1059-350, Deleting a facility on page 2-22.

—continued—

Procedure 4-88 (continued)
Facility Provisioned Mismatch

Step	Action
7	If you have inserted an EC-1x3 circuit pack into an odd slot that was provisioned for an EC-1x12 circuit pack and you want to work with an EC-1x3 circuit pack, delete ports 4 through 12. See 323-1059-350, Deleting a facility on page 2-22.
8	If you have inserted an OC-3 circuit pack into an odd slot that was provisioned for an OC-3x4 circuit pack and you want to work with the OC-3 circuit pack, delete ports 2 through 4. See 323-1059-350, Deleting a facility on page 2-22.
9	If you have inserted an OC-12 circuit pack into an odd slot that was provisioned for an OC12x4 circuit pack and you want to work with the OC-12 circuit pack, delete ports 2 through 4. See 323-1059-350, Deleting a facility on page 2-22.
10	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-89
Fan Failure

Probable cause

This alarm is raised when a cooling unit fan module on the OPTera Metro 3500 shelf is equipped but fails.

Impact

Minor, non-service-affecting (m, NSA) alarm
Critical, service-affecting(C, SA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Verify and record the position of the cooling unit fan module raising the alarm. Fan failure and position are indicated by the LEDs on each cooling unit fan module. Each cooling unit fan module has a green LED when the module is working properly. A red LED is lit when the fan fails.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
Opening the front cover	
3	Rotate outward the two screws on the top, right and left of the front cover.
4	Open the cover completely.
Removing the grill/air deflector	
5	Rotate the fiber storage tray toward the front of the shelf.
6	On the left side of the shelf, push in the spring-loaded pins of the grill/air deflector; at the same time pull the left end of the grill/air deflector just enough to disengage the pin from the shelf hole. See Installing and removing the grill/air deflector on page 3-65.
7	On the right side of the shelf, push in the spring-loaded pins of the grill/air deflector; at the same time pull the right end of the grill/air deflector just enough to disengage the pin from the shelf hole.
8	Pull out the grill/air deflector and store it in a safe place.
9	Rotate the fiber-optic cable tray forward.

—continued—

Procedure 4-89 (continued)
Fan Failure

Step	Action
	Verifying the cooling unit fan module
10	Verify that the cooling unit fan module is seated properly.
11	Make any necessary adjustments.
12	Retrieve all alarms to determine if the alarm has cleared.
	Replacing the cooling unit
13	If the alarm does not clear, replace the failed cooling unit. See Replacing a cooling unit fan module on page 3-67 or Replacing a Universal cooling unit fan module on page 3-75.
14	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-90
Fan Missing

Probable cause

This alarm is raised when an OPTera Metro 3500 shelf equipped with a cooling unit assembly is missing one or more of the cooling unit fan modules.

Impact

Minor, non-service-affecting (m, NSA) alarm for the first fan that is missing
Critical, service-affecting (C, SA) alarm for the second and third fan that are missing.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Display the Shelf Level View. See 323-1059-302, Displaying shelf graphics on page 5-2.
2	Install the necessary cooling unit fan modules. See Replacing a cooling unit fan module on page 3-67 or Replacing a Universal cooling unit fan module on page 3-75.
3	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-91
Far End Client Rx Signal Failure

Probable cause

This alarm is raised against a 2xGigE/FC-P2P circuit pack when service is terminated at the near end because of a problem at the far-end 2xGigE/FC-P2P circuit pack.

Impact

Critical, service-affecting (C, SA) alarm

Requirements

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

Step	Action
1	Retrieve alarms from the far-end 2xGigE/FC-P2P circuit pack that connects to the circuit pack reporting the alarm. See Retrieving active alarms for a network element on page 2-3.
2	If one or more of the following alarms are raised against an Ethernet or Fibre Channel facility of the 2xGigE/FC-P2P circuit pack at the far end, follow the appropriate procedure to clear the alarm(s): • Rx Loss of Signal • Rx Loss of Data Synch • Link Down
3	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-92
Fiber Channel Loopback Active

Probable cause

This alarm is raised when a user executes a loopback command on a Fibre Channel facility of a 2xGigE/FC-P2P circuit pack. The alarm notifies other users that a loopback is active.

Note: This procedure assumes that testing is complete and the circuit pack can be released from loopback mode.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)

Step	Action
1	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Release the loopback. See See 323-1059-222, Releasing a software loopback on page 2-58.

—end—

Procedure 4-93
Fiber cross-connect

Probable cause

The network element detects that the protection and working fibers on a 1+1 protected OC-3, OC-12, OC-48, or OC-192 link are reversed. This means that working optics on NE1 are connected to protection optics on NE2.

Impact

Major, service-affecting (M, SA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Verify the following on every pair of optics on every shelf in the span of control: • the odd slot transmit connects to the odd slot receive on the far end shelf • the even slot transmit connects to even slot receive on the far end
2	Reconnect any faulty connections.

—end—

Procedure 4-94
File System Corruption Suspected

Probable cause

This alarm is raised when there is a possibility that provisioning data on the shelf processor is in a corrupted state.

Impact

Major, non-service-affecting (M, NSA) alarm

Step	Action
1	Contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-95
FLASH Bank Mismatch

Probable cause

This alarm is raised when an upgrade or load installation is interrupted.

Note: If an upgrade or installation is interrupted, there will be different software loads present on the shelf processor.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201
- use an account with a level 3 user privilege code (UPC)

Step	Action
1	Retrieve all active and disabled alarms on the system. Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Log in to the shelf processor. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
3	Check the load release on the shelf processor.
4	Perform an upgrade to the release that is running on the shelf processor.
5	Perform a load installation. Refer to the following: • 323-1059-302, Installing a software load on a shelf processor from a local computer on page 6-49, • 323-1059-302, Installing a software load on a shelf processor using an Ethernet connection on page 6-52 • 323-1059-302, Upgrading the software load on a network element from a local computer on page 6-58 • 323-1059-302, Upgrading the software load on a network element using an Ethernet connection on page 6-61 ***Note:*** Load installation can take 3 hours. Contact your next level of support or your Nortel Networks support group for assistance if necessary.
6	Ensure that the system is restored to its original state by retrieving all conditions and alarms.

—continued—

Procedure 4-95 (continued)
FLASH Bank Mismatch

Step	Action
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-96
Force STS1 Path Switch Complete, Force STS3C Path Switch Complete, or Force STS12C Path Switch Complete, Force STS24C Path Switch, or Force STS48C Path Switch Complete

Probable cause

This alarm is an advisory that a path level forced switch is complete.

> ***Note:*** The forced switch has higher priority than the manual switch and forces protection switching whether the protection circuit failed or is engaged. The forced switch does not override an equal or higher priority protection switch condition.

Impact

Minor, non-service-affecting (m, NSA) alarm

> ***Note:*** The alarm status is minor indicating a non-service-affecting condition. It is an advisory only.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)

Step	Action
1	Confirm that maintenance is complete.
2	Release the forced protection switch. See 323-1059-311, Releasing a path switch in a UPSR on page 1-25.

—end—

Procedure 4-97
Force Switch Complete

Probable cause

This alarm is raised when a forced switch has occurred and is complete. The forced switch overrides manual and automatic switch commands, so the protection equipment is not available.

Use the protection switch for the following:

- to force working DS1, DS3x3, DS3x12, DS3x12e, DS3VTx12, EC-1x3, EC-1x12, OC-3, OC-3x4, OC-12, OC-12x4 STS STS, OC-48 STS, OC-48, or OC-192 circuit packs into protection mode for the purpose of maintenance, for example when replacing a circuit pack
- to lock out working DS1 and optical interface circuit packs from switching to the protection circuit pack, or lock out the protection circuit pack to prevent working circuit packs from switching to protection

The forced switch has higher priority than the manual switch and forces protection switching whether the protection circuit failed or is engaged. The forced switch does not override an equal or higher priority protection switch.

The forced switch is usually used when two or more circuit packs fail and a decision is made to choose to protect one circuit instead of another.

Note: This alarm is a reminder to switch the equipment back to normal mode by releasing the switch to allow automatic protection switching to occur.

Impact

Critical, service-affecting (C, SA) alarm (unprotected)
Minor, non-service-affecting (m, NSA) alarm (linear, protected)

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)

Step	Action
1	Confirm that maintenance is complete and release the forced protection switch. See 323-1059-311, Releasing a protection switch on a tributary circuit pack on page 1-21, Releasing a path switch in a UPSR on page 1-25, or Releasing an optical line switch on page 1-30.

—end—

Procedure 4-98
Force Switch Complete-Remote

Probable cause

This alarm is raised when a protection switch occurs on a linear or BLSR protected pair, because a switch request came from the remote end of the link.

Impact

Minor, non-service-affecting (m, NSA) condition

Requirements

Before you perform this procedure, you must

- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	This is a secondary alarm that is caused by a forced switch request from the remote end. Clear the remote alarms first.
2	If no switch request condition exists on the remote network element, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-99
Force VT1.5 Path Switch Complete

Probable cause

This alarm is raised when the VT1.5 path is force switched to the protection path.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 2 or higher user privilege code (UPC)

Step	Action
1	Confirm that maintenance is complete.
2	Release the forced protection switch. See 323-1059-311, Releasing a path switch in a UPSR on page 1-25.

—end—

Procedure 4-100
FPGA Load Mismatch

Probable cause

This alarm is raised against a Packet Edge, 2x100BT-P2P, or a 2xGigE/FC-P2P circuit pack when the field programmable gate array (FPGA) load file in the flash memory of the circuit pack is not compatible with the shelf processor. This alarm can raise after an upgrade.

> ***Note:*** After performing a shelf processor software upgrade, you must perform a cold restart of the shelf processor circuit pack. See Restarting the shelf processor on page 2-47. FPGA load mismatches that occur after the shelf processor software upgrade are detected only after a cold restart of the shelf processor.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

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

Step	Action
1	Upgrade the FPGA load on the Packet Edge, 2x100BT-P2P, or a 2xGigE/FC-P2P circuit pack. See 323-1059-302, Upgrading the FPGA load on a Packet Edge, 2x100BT-P2P, or 2xGigE/FC-P2P circuit pack on page 6-64.

—end—

Procedure 4-101
FPGA Upgrade in Progress

Probable cause

This alarm is raised against a Packet Edge, 2x100BT-P2P, or a 2xGigE/FC-P2P circuit pack when a field programmable gate array (FPGA) download is in progress. The alarm clears after the upgrade is complete.

Note: This alarm is for information only. Do not perform any actions other than the upgrade activity while it is active. The alarm clears after the upgrade is complete.

Impact

Minor, non-service-affecting (m, NSA) alarm

Step	Action
1	If the alarm does not clear after the upgrade is complete, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-102
FPGA Upgrade Failed

Probable cause

This alarm is raised against a Packet Edge, 2x100BT-P2P, or a 2xGigE/FC-P2P circuit pack when a field programmable gate array (FPGA) download from the network processor to the flash memory of the circuit pack fails.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

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

Step	Action
1	Upgrade the FPGA load on the Packet Edge, 2x100BT-P2P, or a 2xGigE/FC-P2P circuit pack. See 323-1059-302, Upgrading the FPGA load on a Packet Edge, 2x100BT-P2P, or 2xGigE/FC-P2P circuit pack on page 6-64.
2	If the alarm does not clear, replace the Packet Edge, 2x100BT-P2P, or a 2xGigE/FC-P2P circuit pack raising the alarm. See Replacing an OPTera Packet Edge circuit pack on page 3-15.

—end—

Procedure 4-103
FPGA Upgrade Not Committed

Probable cause

This alarm is raised against a circuit pack if there is a mismatch between the field programmable gate array (FPGA) load in the flash memory of the circuit pack and in the FPGA device of the circuit pack.

Impact

Minor, non-service affecting (m, NSA) alarm

Requirements

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

Step	Action
1	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Reseat the circuit pack or perform a cold restart of the circuit pack. See Reseating a circuit pack on page 3-4 or Restarting a circuit pack on page 2-45.

—end—

Procedure 4-104
ILAN1 Port Failure or ILAN2 Port Failure

Probable cause

This alarm is raised when the ILAN ports do not receive Ethernet packages. This occurs when there is a bad Ethernet cable connection, or when the ILAN ports are faulty.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 3 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Ensure that the Ethernet cable is correctly connected to the LOAM.
2	If you are not using an Ethernet cable on your system, disable the alarm. See Disabling alarm points on page 2-28.
3	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-105
ILANSP Port Failure

Probable cause

This alarm is raised when the ILANSP port does not receive any Ethernet packages. This occurs when there is a bad connection between the shelf processor and network processor, or when the ILANSP port does not work.

> ***Note:*** This alarm is sometimes raised on the shelf processor during an network processor restart. Wait 5 minutes to see if the alarm clears automatically.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 1 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Retrieve all active and disabled alarms to identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
3	If the alarm has not cleared automatically, replace the circuit pack raising the alarm. See Procedures for equipment replacement on page 3-1.
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-106
Incoming Network Access Violation

Probable cause

This alarm is raised when the shelf processor or network processor detects

- an attempted access by a denied node
- an incoming access violation due to an unauthorized remote node's attempted connection to a local node

The alarm must be cleared manually. If new access violations occur before this alarm is cleared they will be logged in the Security Log, but no additional SECU class (security) alarms will be generated on the network element.

Note: Clearing this alarm clears all other alarms of the SECU class. For example, the Intrusion Attempt alarm.

Impact

Major, non-service-affecting (M, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- be able to connect to the network processor or shelf processor
- use an account with level 4 or higher user privilege code (UPC)

Step	Action
1	Select the alarmed network element or network processor in the navigation tree.
2	Select Customer Managed Networks from the Security menu.
3	Decide, using your company policy, if the port should allow access.
4	**If** your decision in step 3 was to / **Then** allow access: **1** Click Clear Security Alarms. **2** Click Yes in the confirmation box. **3** Click Edit and define the required parameters to allow this node access. not allow access: Click Clear Security Alarm. ***Note:*** If the accessing node is on the deny list, the denied node will not be allowed access.

—end—

Procedure 4-107
Incomplete Load Lineup

Probable cause

This alarm is raised when a load file is missing.

> ***Note:*** If this alarm is raised during an upgrade activity contact your next level of support or your Nortel Networks support group.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

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

Step	Action
1	Log in to the shelf processor. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
2	Double-click on shelf processor in the Shelf Level View to verify the load release on the shelf processor.
3	Retrieve all active and disabled alarms on the system. See Retrieving active alarms for a network element on page 2-3. Record the current state of the system.
4	Perform a load upgrade. Refer to the following: • 323-1059-302, Upgrading the software load on a network element from a local computer on page 6-58 • 323-1059-302, Upgrading the software load on a network element using an Ethernet connection on page 6-61 ***Note:*** Load upgrade can take 3 hours. Contact your next level of support or your Nortel Networks support group for assistance if necessary.
5	Ensure that the system is restored to its original state by retrieving all conditions and alarms. If any alarm not recorded in step 3 is displayed, refer to the appropriate alarm clearing procedure.
6	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-108
Insufficient Link Capacity

Probable cause

This alarm is raised against the WAN facility on the 2xGigE/FC-P2P circuit pack when the bandwidth assigned to the WAN facility is insufficient to carry the provisioned Fibre Channel service. This alarm is applicable to full-rate Fibre Channel service.

Full-rate Fibre Channel service requires:

- STS-24c of bandwidth for concatenated signals
- STS1-19v or STS3c-6v of bandwidth for virtually concatenated signals

Note: To assign the full-rate bandwidth, the network element must be equipped with an STX-192 circuit pack.

Impact

Critical, service-affecting (C, SA) alarm

Requirements

Before you perform this procedure, you must

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

Step	Action	
1	**If** the Fibre Channel application	**Then**
	requires full-rate bandwidth	go to step 2.
	does not require full-rate bandwidth, and the bandwidth/distance requirements can be met using sub-rate extended reach Fibre Channel service	enable the sub-rate and extended reach Fibre Channel attributes. See 323-1059-350, Editing DS1, DS3, EC-1, 2x100BT-P2P or GE/FC SFP facility signal attributes on page 2-28. Go to step 3.
2	Assign additional bandwidth to the WAN facility of the 2xGigE/FC-P2P circuit pack reporting the alarm. You must assign sufficient bandwidth to the WAN facility to carry the bandwidth assigned to the corresponding Fibre Channel facility. See 323-1059-320, Adding a cross-connect on page 6-1. ***Note:*** See the probable cause for full-rate Fibre Channel requirements.	
3	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.	

—end—

Procedure 4-109
Intercard Failed

Probable cause

This alarm is raised when the shelf processor or the circuit pack reports communications bus failures (clock, parity, or interprocessor communication) and the module is convicted by software based on a majority conviction algorithm. This alarm raised against a VTX or STX module with all of the LEDs illuminated indicates that the circuit pack must be replaced due to a circuit pack power supply failure.

Note: If the Intercard Failed alarm is raised against a 2xGigE/FC-P2P circuit pack, and you replace the SFPs on the circuit pack, the SFP inventory displayed in the Equipment & Facility Provisioning window is not updated. To correctly display the SFP inventory, clear the alarm first, then replace the SFPs.

Impact

Critical, service-affecting (C, SA) alarm for an OCn BLSR or UPSR if cross-connects are provisioned
Critical, service-affecting (C, SA) alarm, if active, linear, protected, pass-through or unprotected mode with cross-connects provisioned
Critical, service-affecting (C, SA) alarm for a Packet Edge circuit pack if it is still attached to the ring
Minor, non-service-affecting (m, NSA) alarm, if there are no provisioned cross-connects, whether the circuit pack is active or inactive, or when the circuit pack is unprotected and inactive
Minor, non-service-affecting (m, NSA) alarm for a Packet Edge circuit pack if it is not attached to the ring

Note: Because of the loss of communications, the status of the circuit pack may be unknown. Additional failures can be service-affecting.

—continued—

Procedure 4-109 (continued)
Intercard Failed

The following table lists expected severities for each circuit pack if any cross-connects are provisioned.

Module	Inactive	Active	Unprotected Mode
DS1, DSM DS1x84 termination module	m, NSA	C, SA	C, SA
DS3x3, DS3x12, DS3x12e, DS3VTx12	m, NSA	C, SA	C, SA
EC-1x3, EC-1x12	m, NSA	C, SA	C, SA
ILAN	NA	m, NSA	NA
NPx	NA	m, NSA	NA
VTX-48, VTX-48e, STX-192 (see Note 1)	m, NSA	C, SA	C, SA
OC-3, OC-3x4 as host for DS1 service module	C, SA	C, SA	C, SA
linear (OC-3, OC-3x4, OC-12, OC-12x4 STS STS, OC-48 STS, OC-48, OC-192)	m, NSA	C, SA	C, SA
BLSR (OC-48, OC-192) (see Note 2)	m, NSA	C, SA	C, SA
UPSR (OC-3, OC-3x4, OC-12, OC-12x4 STS STS, OC-48 STS, OC-48, OC-192) (see Note 3)	C, SA	C, SA	C, SA
Packet Edge (see Note 4)	C, SA	C, SA	NA
2x100BT-P2P	m, NSA	C, SA	NA
2xGigE/FC-P2P	m, NSA	C, SA	NA
PSC	NA	M, NSA	NA
PSX	NA	m, NSA	NA
SPx (see Note 5)	NA	M, NSA	NA

Note 1: If the VTX or STX modules are removed, the alarm severity is C, SA on both slots.

Note 2: In a BLSR configuration, both circuit packs are active.

Note 3: If the circuit pack is inactive the alarm severity is m, NSA, except in the case of an OC-3, OC-3x4, OC-12, OC-12x4 STS STS, OC-48, OC-48 STS, or OC-192 UPSR ring configuration.

Note 4: If the alarmed OPTera Packet Edge circuit pack is attached to a ring, the alarm severity is C, SA. If the alarmed OPTera Packet Edge circuit pack is not attached to a ring, the alarm severity is m, NSA.

Note 5: A major audible alarm is the only indication if the shelf processor is missing.

—continued—

Procedure 4-109 (continued)
Intercard Failed

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52. ***Note:*** If the alarm is not against the VTX-48, VTX-48e, or STX-192 circuit pack, go to step 4.
3	If this alarm is against the VTX-48, VTX-48e, or STX-192 circuit pack and all the LEDs are illuminated, replace the circuit pack. See Replacing a VTX module on page 3-48 or Replacing an STX-192 circuit pack on page 3-51. If the alarm does not clear, contact your next level of support or your Nortel Networks support group for assistance.
4	Reseat the circuit pack. See Reseating a circuit pack on page 3-4.
5	If the alarm does not clear and the circuit pack was replaced in the past 48 hours, contact your next level of support or your Nortel Networks support group.
6	If the alarm does not clear and the circuit pack was not replaced in the past 48 hours, replace the circuit pack. See Procedures for equipment replacement on page 3-1.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-110
Intercard Serial Link Failed

This alarm is raised when the OC-48 or OC-192 serial communication channel fails between two OC-48 or two OC-192 circuit packs.

Impact

Minor, non-service-affecting (m, NSA) alarm, if the OC-48 or OC-192 circuit pack is provisioned for UPSR or 1+1 protection and the serial link fails

Major, service-affecting (M, SA), alarm, if the OC-48 or OC-192 circuit pack is provisioned for BLSR protection and the serial link fails

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2	Identify the OC-48 or OC-192 circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
3	Reseat the circuit pack. See Reseating a circuit pack on page 3-4.
4	If the alarm does not clear and the circuit pack was replaced in the past 48 hours, contact your next level of support or your Nortel Networks support group.
5	If the alarm does not clear and the circuit pack was not replaced in the past 48 hours, replace the circuit pack. See Procedures for equipment replacement on page 3-1.
6	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-111
Intercard Suspected

Probable cause

This alarm is raised when one of the following conditions occur

- the shelf processor or the circuit pack reports suspected communications bus (clock, parity, or interprocessor communication) failures. This alarm is raised against the circuit pack that is suspected of the problem.

  If this alarm is raised against a pair of DSM DS1x84 termination module mappers, the Host has detected a failure of the mate-to-mate link.

- there is a tributary card in the system that is not compatible with VTX or STX.

  Note: A Circuit Pack Incompatible alarm is raised when a VTX and an STX circuit pack are in the same system. If the VTX or STX has an unsupported tributary card, an Intercard Suspected alarm is raised as well. The Intercard Suspected alarm is cleared when the conditions causing the Circuit Pack Incompatible alarm are cleared.

Impact

Critical, service-affecting (C, SA) alarm for a Packet Edge circuit pack if it is still attached to the ring
Minor, non-service-affecting (m, NSA) alarm

Note: Status of the circuit pack may be unknown because of the loss of communications. Additional failures can be service-affecting.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201.

Step	Action
1	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

—continued—

Procedure 4-111 (continued)
Intercard Suspected

Step	Action
2	 **CAUTION** **Risk of traffic loss on both working and protection slots** Removal of either mapper results in traffic loss when this alarm is raised against both a working and protection mapper pair. Contact Nortel Networks support immediately. Identify the circuit pack raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
3	Reseat the circuit pack. See Reseating a circuit pack on page 3-4.
4	If the alarm does not clear and the circuit pack was replaced in the past 48 hours, contact your next level of support or your Nortel Networks support group.
5	If the alarm does not clear and the circuit pack was not replaced in the past 48 hours, replace the circuit pack. See Procedures for equipment replacement on page 3-1.
6	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-112
Intercard Suspected - Pluggable

Probable cause

This alarm is raised when a Small Form Factor Pluggable (SFP) optical transceiver module reports suspected communications bus failures. This alarm is raised against the SFP that is suspected of the problem.

Impact

Minor, non-service-affecting (m, NSA) alarm

Requirements

Before you perform this procedure, ensure you

- have all the documentation referenced in this procedure
- obtain a supported SFP optical transceiver module and, if required, a replacement 2xGigE/FC-P2P circuit pack
- observe all safety requirements described in Safety requirements on page 4-11, and in *Installation,* 323-1059-201.

Step	Action
1	Identify the 2xGigE/FC-P2P circuit pack and SFP port raising the alarm. The Unit field in the Active Alarms window specifies the circuit pack and port using the following format: GEFC-slot#-port#. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Replace the SFP optical transceiver module you identified in step 1. See Replacing a Small Form Factor Pluggable (SFP) optical transceiver module on page 3-21. ***Note:*** Refer to the Hardware feature descriptions chapter of the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM for the list of PECs of supported SFP optical transceiver modules.
3	If the alarm does not clear, replace the 2xGigE/FC-P2P circuit pack you identified in step 1. See Replacing a 2xGigE/FC-P2P circuit pack on page 3-18.
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 4-113
Intrusion Attempt

Probable cause

This alarm is raised when the shelf processor or network processor detects an intruder trying to gain access to the shelf. You will see this alarm when the maximum number of login attempts exceeds the provisioned number allowed.

The alarm is raised when an intrusion is detected and the channel/port locks. The alarm clears automatically after the lockout period expires, however, an administrator can clear the alarm manually before the lockout is cleared. If new Intrusion attempts occur before this alarm is cleared, they will be logged in the Security Log and the duration of the lockout will be extended for the lockout period of the latest intrusion attempt.

Note: Clearing this alarm clears all other alarms of the SECU class. For example, the Incoming Network Violation alarm.

Impact

Major, non-service-affecting (M, NSA) alarm

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- be able to connect to the network processor or shelf processor
- use an account with level 5 or higher user privilege code (UPC)

Step	Action
1	Allow the alarm to clear itself when the lockout time expires or go to step 2.
2	Select the alarmed network element or network processor in the navigation tree.
3	Select Intrusion attempt handling from the Security menu.
4	Click Clear Security Alarms. ***Note 1:*** Clearing the Intrusion alarm has no effect on the alarmed port. The port will continue to be locked out until valid login information is delivered. Clicking this button merely removes the alarm from the alarm list. ***Note 2:*** The channel is locked out and no one can login from the originating address for the duration of the lockout. The alarm will clear from the network element when the channel unlocks after the provisioned elapsed time.
5	Click Yes in the confirmation dialog box.
6	Follow your company policy for handling intrusion attempts.

—end—

Procedure 4-114
Invalid K-bytes

Probable cause

This alarm is raised when the OC-48 or OC-192 circuit pack at the far-end add/drop multiplexer (ADM) node detects a protection request with an invalid automatic protection switching (APS) identifier or an invalid request.

This alarm tracks the following APS codes detected at the receive (Rx) K-bytes on the OC-48 or OC-192 circuit pack:

- Unused Protection Channel Status (all codes)
- Unsupported Request (all codes)
- Reverse Request (long path indication)

This alarm is caused by one of the following conditions:

- incorrect provisioning of the ring APS identifiers at the far end
- equipment problem at the far end
- incorrect fiber-optic cable connections
- provisioning of protection is inconsistent between the alarmed node and the far-end node

Impact

Minor, non-service affecting (m, NSA) alarm

Requirements

Before you perform this procedure, you must

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

Step	Action
1	Perform a force audit on the ring. See 323-1059-320, Performing a BLSR audit and retrieving diagnostics on page 6-45.
2	Verify the BLSR provisioning. See 323-1059-320, Provisioning a BLSR (bidirectional) on page 4-2.
3	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
4	If the alarm does not clear, verify the fiber connections of the OC-48 optical interface circuit pack.

—continued—

Procedure 4-114 (continued)
Invalid K-bytes

Step	Action
5	At the far-end network element, reseat the OC-48 or OC-192 circuit pack raising the alarm. See Reseating a circuit pack on page 3-4.
6	If the alarm does not clear, replace the circuit pack. See Replacing an OC-48 or OC-192 optical interface circuit pack in a BLSR on page 3-41.
7	If the alarm does not clear, repeat step 5 and step 6 for the near-end network element.
8	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Nortel Networks

OPTera Metro 3500 Multiservice Platform

Alarm and Trouble Clearing—Part 1 of 2

323-1059-543
Standard Release 12.0 Issue 1
November 2003
Printed in Canada