NTN465GF 323-1059-543

Nortel Networks

OPTera Metro 3500 Multiservice Platform

Alarm and Trouble Clearing—Part 2 of 2

Standard Release 12.0 Issue 1 November 2003

What's inside...

See Part 1 for the following...

NORTEL NETWORKS™

Copyright © 2000–2003 Nortel Networks, All Rights Reserved

The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose the information only to its employees with a need to know, and shall protect the information, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

Nortel Networks, the Nortel Networks logo, the Globemark, OPTera, and Preside are trademarks of Nortel Networks.

Printed in Canada

Contents

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 2 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 to cover 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:

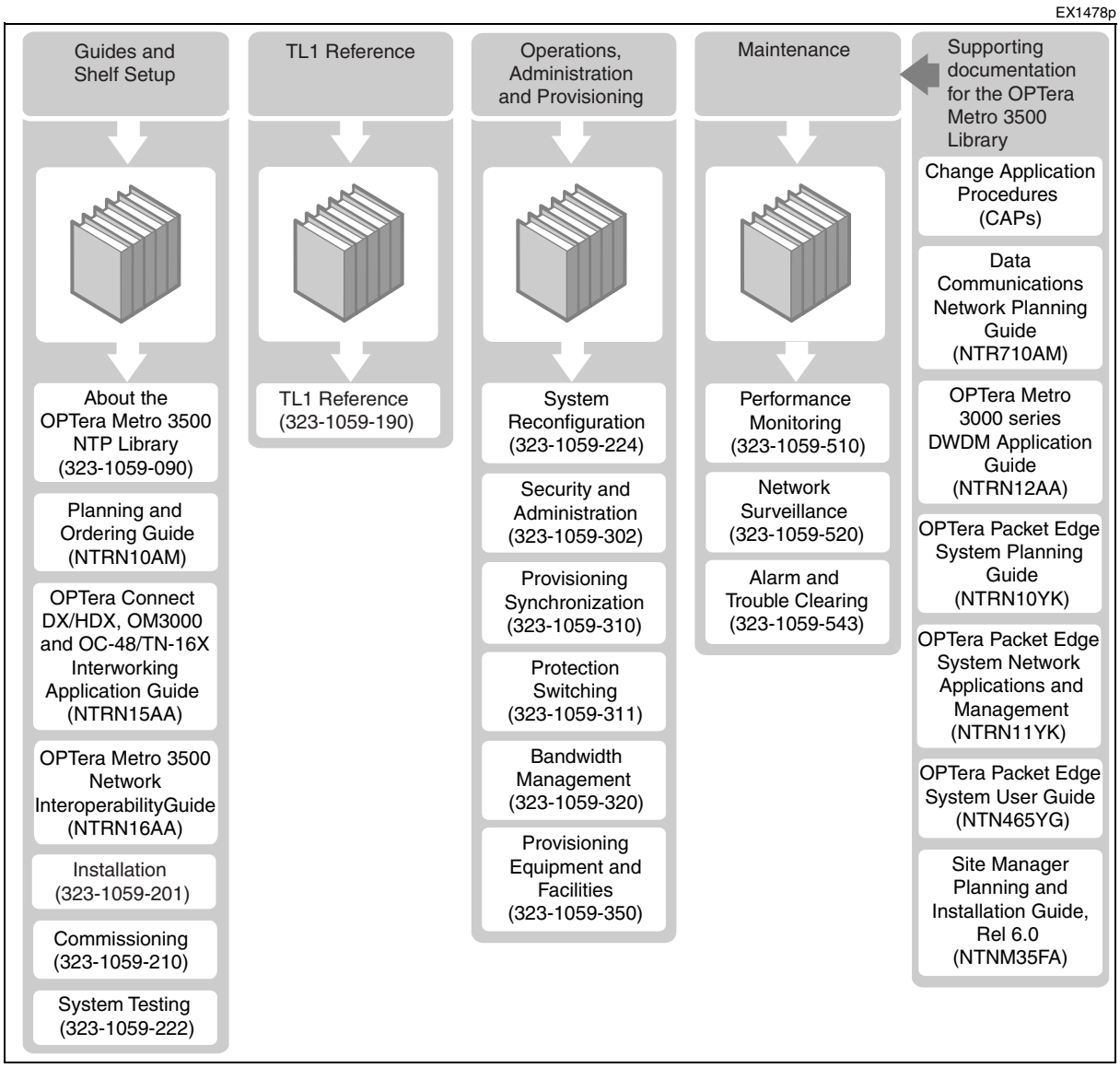
- The extended shelf processor (SPx) is referred to as the shelf processor.
- The extended network processor (NPx) is referred to as the network processor.

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 clearing L-Z

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 5-1
Latch Open

Probable cause

This alarm is raised when the locking levers on the VTX-48, VTX-48e, or STX-192 circuit pack are not fully closed after insertion of the circuit pack into a slot, or the latch on the circuit pack is broken.

Impact

Major, non-service-affecting (M, NSA) alarm, if unprotected
Minor, non-service-affecting (m, NSA) for first alarm occurrence if protected
Major, non-service-affecting (M, NSA) for second alarm occurrence if protected

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 5-11, 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 that the VTX-48, VTX-48e, or STX-192 circuit pack raising the alarm is pushed all the way in to its slot until the locking levers touch their latches.
4	Lock the circuit pack into its slot by pushing the upper locking lever down and the lower lever up at the same time. ***Note:*** Do not force the locking levers. If the levers do not close correctly, then remove the circuit pack. Go to step 6.
5	Retrieve all active and disabled alarms to determine if the alarm cleared. 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 5-2
Line PM Threshold Exceeded

Probable cause

This alarm is raised when a line PM threshold is exceeded for the specified facility. This alarm is raised at the first occurrence of a line PM threshold crossing in the collection period (1-day or 15-minutes).

This alarm is raised once in the collection period and it clears automatically at the end of the collection period. If the problems causing the threshold crossings are not corrected, then the alarm will be raised against the facility in subsequent collection periods at the first occurrence of a line PM threshold crossing.

This alarm is raised only when the PM threshold crossing report type is set to Alarm. You can disable the reporting of the threshold crossing alert (TCA) summary alarms. See 323-1059-510, Editing the Threshold Crossing Report Type for facilities on page 1-44.

> ***Note:*** The TCA summary alarms are as follows: Section PM Threshold Exceeded, Line PM Threshold Exceeded, and Path PM Threshold Exceeded.

You can also disable thresholding. See 323-1059-510, Editing the threshold status for facilities on page 1-43.

The TCA summary alarms can help you trouble clear and avoid potentially service-affecting problems, indicated by the following alarms:

- signal degrade
- signal fail
- loss of frame
- loss of signal

This alarm can be caused by the following conditions:

- a faulty upstream transmitter circuit pack
- incorrectly provisioned transmitting circuit pack
- a circuit pack with the wrong wavelength
- a faulty receive circuit pack
- an optical signal degradation

—continued—

Procedure 5-2 (continued)
Line PM Threshold Exceeded

- a bent optical fiber
- a dirty connector
- a dirty optical fiber
- incorrectly set attenuation
- a DWDM coupler incorrectly configured at the receiving end
- a DWDM coupler damaged at the receiving or transmitting end
- an out-of-service facility upstream

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 optical power meter with the same optical connectors as the network element
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201

Step	Action
1	Retrieve the PM counts for the facility and determine which thresholds are exceeded. See 323-1059-510, Procedures for facility PM counts on page 1-1 and 323-1059-510, Procedures for facility PM thresholds on page 1-2.
2	Retrieve alarms from the network element. See Retrieving active alarms for a network element on page 2-3.
3	Query the facility details (see 323-1059-350, Retrieving equipment and facility details on page 2-2) to determine if the alarm has been raised against a deleted facility.
4	**If** the alarm is raised against — **Then** a deleted facility — go to step 5 an existing facility — go to step 9
5	Add the facility (see 323-1059-350, Adding a facility on page 2-20). ***Note:*** It is not necessary to add the exact connection that caused the alarm. You can create a temporary connection to the facility (or facilities) with the active alarm.

—continued—

Procedure 5-2 (continued)
Line PM Threshold Exceeded

Step	Action
6	Ensure that Alarm is not selected as the Threshold Crossing Report Type. See 323-1059-510, Editing the Threshold Crossing Report Type for facilities on page 1-44.
7	Delete the facility (see 323-1059-350, Deleting a facility on page 2-22).

8

If	**Then**
the alarm clears	you have completed this procedure
the alarm does not clear	go to step step 9

9 If alarms of higher order are active against the facility at the near end and at the far end, clear these other alarms first using the appropriate procedures.

If errors are at	**Then**
near end only	continue with procedure
near end and far end	continue with procedure
far end only	go to the remote end and continue with the procedure. The far end now becomes the near end

10 Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	go to step 11

11 Measure the receive power of the near-end receiver circuit pack using an optical power meter.

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

If the receive power is	**Then** go to
below the minimum receive sensitivity	step 12
above the receiver overload	step 21
within the operating range (between the minimum receive sensitivity and the receiver overload)	step 23

Receive power below the minimum receive sensitivity for the circuit pack

12 Wear an antistatic wrist strap to protect the shelf from static damage. At the near-end network element, connect the wrist strap to the ESD jack on the shelf.

—continued—

Procedure 5-2 (continued)
Line PM Threshold Exceeded

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.

At the near end, check for bent optical fibers or damaged patch cords. See *Installation*, 323-1059-201.

13 At the near end, clean the optical fiber connector on the circuit pack and the optical fiber, then reattach the optical fiber. See *Installation*, 323-1059-201.

14 Measure the receive power of the near-end receiver circuit pack again:

If the receive power is	**Then** go to
still below the minimum receive sensitivity	step 15
within the operating range (between the minimum receive sensitivity and the receiver overload)	step 17

15 Adjust the attenuation, if equipped, of the near-end receiver circuit pack to try to get the receive power within the operating range of the circuit pack.

16 Measure the receive power of the near-end receiver circuit pack again:

If the receive power is	**Then** go to
within the operating range (between the minimum receive sensitivity and the receiver overload)	step 17
still below the minimum receive sensitivity	step 18

17 Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	step 23

—continued—

Procedure 5-2 (continued)
Line PM Threshold Exceeded

Step	Action
18	If you cannot get the receive power within the operating range, measure the transmit power at the far-end transmitter circuit pack.

If the transmit power is	**Then**
above the end of life transmit power	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 and clear the location of the problem. Then, go to step 20.
below the end of life transmit power	go to step 19

19	Clean the optical fiber connector on the transmitter circuit pack, then measure the transmit power again:

If the transmit power is	**Then**
still below the end of life transmit power	replace the circuit pack at the transmit end, then clean and reattach the optical fibers. See 323-1059-543, Procedures for equipment replacement on page 3-1 and *Installation*, 323-1059-201. Then, go to step 20.
within the operating range of the circuit pack	go to step 20

20	Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	go to step 23

Receive power is above the receiver overload for the circuit pack

21	Adjust the attenuation, if equipped, of the near-end receiver circuit pack to get the receive power within range.
22	Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	go to step 23

—continued—

Procedure 5-2 (continued)
Line PM Threshold Exceeded

Step	Action

Receive power within operating range for the circuit pack

23 Clean all connections at both ends of the optical fiber link, then reattach the optical fibers. See *Installation*, 323-1059-201.

24 Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	step 25

25 Check whether there is a defective circuit pack. Replace the near-end receiver circuit pack, then clean and reattach the optical fibers. See 323-1059-543, Procedures for equipment replacement on page 3-1 and *Installation*, 323-1059-201.

26 Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	go to step 27

27 If you have not already done so, replace the far-end transmitter circuit pack, then clean and reattach the optical fibers. See 323-1059-543, Procedures for equipment replacement on page 3-1 and *Installation*, 323-1059-201.

28 Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	contact your next level of support or your Nortel Networks support group for assistance

—end—

Procedure 5-3
Link Degrd and Virtual Ckt Fail

Probable cause

This alarm is raised on the network processor.

The Link degraded alarm is raised when more than 5% of data frames on the X.25 physical link contain receive or transmit errors over a period of 60 seconds.

The Virtual circuit failure alarm is raised while waiting for X.25-associated TL1 resources that are being recovered. The alarm clears when the resources are recovered.

Impact

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

Requirements

See Link Performance Degraded on page 5-28 and Virtual Circuit Failure on page 5-263 for requirements of each alarm clearing procedure.

Step	Action
1	See the Link Performance Degraded on page 5-28 and Virtual Circuit Failure on page 5-263 alarm clearing procedures.

—end—

Procedure 5-4
Link Down (2x100BT-P2P)

This alarm is raised when one of the following occurs

- the administrative state of an Ethernet or WAN port on a 2x100BT-P2P circuit pack is up but the operating state of the port is down.
- the magic number facility attribute is enabled, a loopback link is detected, and the PPP negotiation fails.

  Note 1: The magic number facility attribute is used during PPP negotiation only.

  Note 2: If the "Link Down" alarm is raised against the network processor, refer to Link Down (network processor) on page 5-26.

  Note 3: If the "Link Down alarm is raised against the 2xGigE/FC-P2P circuit pack, refer to Link Down (2xGigE/FC-P2P) on page 5-22.

Impact

Critical, service-affecting (C, SA) alarm

Step	Action
1	For an Ethernet port, clear the "Link Pulse Missing" alarm, if present. See Link Pulse Missing on page 5-29.
2	For a WAN port: **a.** Clear any STS path alarms on the optical interface circuit pack that connects to the 2x100BT-P2P circuit pack, such as an alarm indication signal, unequipped, loss of pointer, path trace mismatch, or signal label mismatch. **b.** If the alarm does not clear, verify that the port at the other end of the connection uses the same frame check size. If necessary, change the frame check size of the port. See 323-1059-350, Editing DS1, DS3, EC-1, 2x100BT-P2P or GE/FC SFP facility signal attributes. **c.** If the alarm does not clear, disable the magic number attribute of the WAN port, if enabled. See 323-1059-350, Editing DS1, DS3, EC-1, 2x100BT-P2P or GE/FC SFP facility signal attributes. If the alarm clears, it likely means that cross-connects were provisioned in such a way that the WAN port was in loopback mode. **d.** If the alarm does not clear, disable link connectivity monitoring at the WAN port, if enabled. See 323-1059-350, Editing DS1, DS3, EC-1, 2x100BT-P2P or GE/FC SFP facility signal attributes. If the alarm clears, it likely means that the port at the other end of the connection does not support link connectivity monitoring.

—continued—

Procedure 5-4 (continued)
Link Down (2x100BT-P2P)

Step	Action
3	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-5
Link Down (2xGigE/FC-P2P)

Probable cause

This alarm is raised against an Ethernet, Fibre Channel, or WAN facility of a 2xGigE/FC-P2P circuit pack.

Note 1: If the Link Down alarm is raised against the network processor, refer to Link Down (network processor) on page 5-26.

Note 2: If the Link Down alarm is raised against the 2x100BT-P2P circuit pack, refer to Link Down (2x100BT-P2P) on page 5-20.

This alarm is raised against an Ethernet facility when one of the following conditions occurs:

- a fiber is disconnected
- conditioning at the far end
- auto-negotiation between the 2xGigE/FC-P2P circuit pack and the subtending client equipment does not complete successfully
- auto-negotiation setting on the 2xGigE/FC-P2P circuit pack does not match the auto-negotiation setting on the subtending client equipment
- the administrative state of a facility on the 2xGigE/FC-P2P circuit pack is up but the operating state of the facility is down (the subtending equipment might be defective)

This alarm is raised against a Fibre Channel facility when one of the following conditions occurs:

- a fiber is disconnected
- conditioning at the far end (laser at the far-end circuit pack is shut down)
- the Fibre Channel link state is not active (the subtending equipment might be defective)

  Note: When the Rx Loss of Signal or Loss of Data Synch alarm is raised, the Link Down alarm is also raised against the Ethernet or Fibre Channel facility.

This alarm is raised against a WAN facility when the administrative state of a facility on the 2xGigE/FC-P2P circuit pack is up but the operating state of the facility is down.

When the Link Down alarm is raised against the WAN facility, the link cannot carry traffic.

—continued—

Procedure 5-5 (continued)
Link Down (2xGigE/FC-P2P)

Note: The Link Down alarm raised against a WAN facility masks the Link Down alarm against an Ethernet or Fibre Channel facility.

When one of the following alarms is raised, the Link Down alarm is raised against the WAN facility:

- STS Rx AIS
- STS Rx Unequipped
- STS Rx Path Trace Mismatch
- STS Rx Signal Label Mismatch
- STS Rx Loss of Multiframe
- STS Rx Loss of Sequence
- STS Rx Loss of Alignment
- Rx Loss of Frame Delineation

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 fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- use an account with level 3 or higher user privilege code (UPC)

Step	Action	
1	Retrieve alarms from the network element. See Retrieving active alarms for a network element on page 2-3.	
2	From the Class field in the Active Alarms window, determine if the Link Down alarm is raised against the Ethernet, Fibre Channel, or WAN facility.	
3	**If** the alarm is raised against the	**Then** go to
	Ethernet facility	step 4
	Fibre Channel facility	step 9
	WAN facility	step 15

—continued—

Procedure 5-5 (continued)
Link Down (2xGigE/FC-P2P)

Step	Action
	Alarm raised against the Ethernet facility
4	Clear any alarms raised against the WAN facility of the 2xGigE/FC-P2P circuit pack.
5	Ensure that the subtending client equipment is correctly provisioned, functioning, and transmitting a valid signal.
6	Ensure that the fiber between the subtending equipment and the LAN port is properly connected and is not damaged.
7	Ensure that the auto-negotiation setting provisioned on the subtending equipment matches the auto-negotiation setting provisioned on the 2xGigE/FC-P2P circuit pack. To determine the auto-negotiation setting of the 2xGigE/FC-P2P circuit pack, see 323-1059-350, Retrieving equipment and facility details on page 2-2.
8	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.
	Alarm raised against the Fibre Channel facility
9	Clear any alarms raised against the WAN facility of the 2xGigE/FC-P2P circuit pack.
10	Ensure that the subtending client equipment is correctly provisioned, functioning, and transmitting a valid signal.
11	Ensure that the fiber between the subtending equipment and the LAN port is properly connected and is not damaged.
12	If the alarm does not clear, retrieve the facility details for the Fibre Channel facility on the 2xGigE/FC-P2P circuit pack reporting the alarm: • 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 FC facility on the 2xGigE/FC-P2P circuit pack raising the alarm. • From the Facility area, select FC from the Facility Type drop-down list box.
13	**If** the Link State parameter in the Facility table displays — **Then** LINKFAILURE, OFFLINE, UNKNOWN, or LINKRECOVERY — use your company procedure to determine if a problem exists on the local link partner equipment. ACTIVE — go to the next step.
14	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—continued—

Procedure 5-5 (continued)
Link Down (2xGigE/FC-P2P)

Step	Action

Alarm raised against the WAN facility

15 Use the appropriate alarm clearing procedure to clear any STS path alarms on the optical interface circuit pack that connects to the 2xGigE/FC-P2P circuit pack. The STS path alarms include STS Rx Signal Degrade, STS Rx Excessive BIP Error Rate, STS Rx Loss of Alignment, STS Rx Loss of Multiframe, and STS Rx Loss of Sequence alarms.

16 If the alarm does not clear, ensure that the WAN facility on the 2xGigE/FC-P2P circuit pack raising the alarm and the WAN facility at the other end of the connection use the same frame check sum size.

a. Retrieve the frame check sum size setting of the port raising the alarm:

— 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 WAN facility of the 2xGigE/FC-P2P circuit pack raising the alarm.

— From the Facility area, select WAN from the Facility Type drop-down list box. The Frame check sum size is displayed in the Facility table.

b. Retrieve the frame check sum size setting of the WAN facility at the other end of the connection.

c. If necessary, modify the frame check sum size of the incorrectly provisioned WAN facility. See 323-1059-350, Editing DS1, DS3, EC-1, 2x100BT-P2P or GE/FC SFP facility signal attributes.

17 If the Loss of Frame Delineation alarm is raised, clear this alarm using the Loss of Frame Delineation alarm clearing procedure.

18 If the Rx Loss of Signal or Link Down alarm is raised against an Ethernet or Fibre Channel facility of the far-end 2xGigE/FC-P2P circuit pack, clear the alarm using the alarm appropriate clearing procedure.

19 If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-6
Link Down (network processor)

Probable cause

This alarm is raised on the network processor when the X.25 facility detects that the link access procedure balanced (LAPB) datalink layer is disconnected. This means it is down or out of service. After a 60-second debounce period, the alarm clears when the LAPB datalink layer recovers its connection.

Note: If the "Link Down" alarm is raised against the 2x100BT-P2P circuit pack, refer to Link Down (2x100BT-P2P) on page 5-20.

Impact

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

Note: No X.25 calls can be made to the network processor while the LAPB layer is disconnected.

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)
- have access to physical connections and cabling

Step	Action
1	In the navigation tree, select the network processor.
2	Log in to the network processor. See 323-1059-302, Procedures for logging in to a network processor on page 2-1.
3	Verify that the LAPB datalink layer (lower layer X.25) is configured with the correct values at each end of the LAPB link. See 323-1059-520, Editing X.25 parameters on page 3-6.
4	At either end of the LAPB link, adjust the parameters to match or select the correct values using the procedure for provisioning lower layer X.25 parameters. See 323-1059-520, Editing X.25 parameters on page 3-6.
5	If the alarm does not clear, verify the X.25 port configuration and make any required modifications. See 323-1059-520, Editing X.25 parameters on page 3-6.
6	If the alarm does not clear, verify that the required signals are passing through to the X.25 connector. Correct the signals if necessary.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-7
Link Down 1/1, Link Down 1/2, Link Down 1/3, Link Down 1/4, Link Down 2/1, or Link Down 2/2

This alarm is raised against an Ethernet port (1/1, 1/2, 1/3, 1/4) or WAN port (2/1, 2/2) port of a Packet Edge circuit pack when the administrative state of the port is up but the operating state of the port is down.

Note: Ethernet ports 1/3 and 1/4 only apply to the 4x100BT and 4x100FX circuit packs.

Impact

Major, service-affecting (M, SA) alarm

Step	Action
1	For an Ethernet port, make sure the cable between the LAN port and the interconnecting device is properly connected and is not damaged.
2	Ensure the corresponding I/O module is fully inserted and locked into position.
3	For a WAN port, make sure of the following: • there are no broken connections, such as a fiber cut, around the ring • the administrative state of the WAN port at the other end of the connection is up • there is more than one circuit pack in the Resilient Packet Ring (RPR) • the neighboring Packet Edge circuit pack in the RPR is not missing, out of service, or faulty
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-8
Link Performance Degraded

Probable cause

This alarm is raised on the network processor when greater than 5% of data frames on the X.25 physical link contain receive or transmit errors over a period of 60 seconds.

Impact

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

Note: The X.25 link can become too degraded to maintain or permit new X.25 calls until the degraded condition clears.

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 5-11, and in *Installation,* 323-1059-201
- have access to physical connections and cabling

Step	Action
1	Verify that the correct signals are passing through to the network processor X.25 connector on the LOAM. Correct the signals if necessary.
2	If the problems continues, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-9
Link Pulse Missing

Probable cause

This alarm is raised when there is a problem with the Ethernet cable connected to a 2x100BT-P2P circuit pack or there is no link pulse received by the 2x100BT-P2P circuit pack.

Impact

Critical, service-affecting (C, SA) alarm

Step	Action
1	Verify that you are using the correct cable type (cross-over or straight-through) for the connection.
2	Verify that the cable is plugged into the correct port on the 2x100BT-P2P circuit pack and on the connecting equipment.
3	Ensure the corresponding I/O module is fully inserted and locked into position.
4	Verify that the port on the connecting equipment is in-service.
5	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-10
Load Installation Failed

Probable cause

This alarm is raised in the event of a failure to install a software load onto the shelf processor. This alarm continues until the shelf processor is moved to a different system (shelf signature must be different than that of the original installation location system) or a cancel operation is successful.

This alarm is raised if the following occurs during:

- the load procedure, the transport load files from the remote source cannot be retrieved or put into the file system
- the load procedure, you cannot get and program the shelf processor loads into the bank opposite to where it is running
- the invoke procedure, you cannot perform a restart and start running from the opposite bank
- the commit procedure, you cannot program the opposite bank with the new shelf processor loads

Impact

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

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 5-11, and in *Installation,* 323-1059-201

Step	Action
1	Cancel the installation. 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. ***Note:*** The cancel load installation command can take as much as 2 hours to complete.
2	Retrieve the software version of the shelf processor by clicking on the shelf processor in Shelf Level View from the Configuration menu. ***Note:*** If you do not know which software release is running on the shelf, contact your next level of support or your Nortel Networks support group.
3	Try to install the software load on the shelf processor again.

—continued—

Procedure 5-10 (continued)
Load Installation Failed

Step	Action
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-11
Load Installation in Progress

Probable cause

This alarm is raised against the shelf to indicate that a load installation is in progress.

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 5-11, and in *Installation,* 323-1059-201

Step	Action
1	Select Active Alarms from the Faults menu.
2	Verify that only the load installation in progress alarm exists.
3	Allow enough time to complete the load installation. ***Note:*** Load installation can take up to 2 or 3 hours.
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-12
Loads Mismatch

CAUTION
Risk of traffic loss
Do not perform circuit pack replacements while this alarm is active; provisioning information will be lost and traffic may be affected.

Probable cause

This alarm is raised:

- against the shelf processor if at least one of the transport circuit packs has a different software release than the shelf processor
- against the network processor when the co-located shelf processor is running a load from a different release than the load on the network processor

  Note: When this alarm is active, do not make any provisioning changes to the network processor.

Impact

Major, non-service-affecting (M, NSA) alarm (shelf processor)
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 5-11, and in *Installation,* 323-1059-201

—continued—

Procedure 5-12 (continued)
Loads Mismatch

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.

If the alarm is on the	**Then** go to
shelf processor circuit pack	step 2
network processor circuit pack	step 6
both the shelf processor and network processor circuit packs	step 2 ***Note:*** You must clear the alarm on the shelf processor first, and then clear the alarm on the network processor.

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	Retrieve the software version of the shelf processor and of all the transport circuit packs (for example, OC-n, VTX, DS3) from the Shelf Level View. See 323-1059-302, Displaying details for a shelf circuit pack on page 5-3.
4	If the transport circuit packs are all running the same software version and the shelf processor circuit pack is running a different software version, then go to step 5. Otherwise, contact your next level of support or your Nortel Networks support group.
5	Upgrade the software on the shelf processor or replace the shelf processor with a shelf processor that is running the same load as the rest of the shelf. • To upgrade the software on the shelf processor, see 323-1059-302, Installing a software load on a shelf processor using an Ethernet connection on page 6-52 or 323-1059-302, Installing a software load on a shelf processor from a local computer on page 6-49. • To replace the shelf processor, see Replacing the shelf processor on page 3-7. ***Note:*** If you are performing an upgrade on the NE, the local shelf processor is specified as the Load Source.

If the alarm	**Then**
was on the shelf processor only	you have completed this procedure
is also on the network processor	go to step 6

6	Install a software release on the network processor that matches the software release running on the network element. See 323-1059-302, Upgrading the software load on a network processor on page 6-55.

—end—

Procedure 5-13
Lockout of Protection Complete

Probable cause

This alarm is raised when a lockout of protection is initiated on an optical channel or on the DS1 protection circuit pack.

Note 1: You cannot perform a lockout on a DSM DS1x84 termination module mapper.

Note 2: You cannot perform a lockout on a Host OC-3 or OC-3x4 circuit pack.

Note 3: The BLSR lockout of protection is for the entire span.

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	When maintenance is complete, release the circuit pack from lockout mode. See 323-1059-311, Releasing an optical line switch on page 1-30 or Releasing a protection switch on a tributary circuit pack on page 1-21.

—end—

Procedure 5-14
Lockout of Protection Complete-Remote

Probable cause

This alarm is raised when a lockout request comes from the far end of the link and a lockout of protection switch occurs on the linear or BLSR protected optical interface pair.

Note 1: You cannot perform a lockout on a DSM DS1x84 termination module mapper.

Note 2: You cannot perform a lockout on a Host OC-3 or OC-3x4 circuit pack.

Impact

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

Note: This is a secondary alarm caused by a Lockout switch request from the remote end.

Step	Action
1	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 5-15
Lockout of Working Complete

Probable cause

This alarm is raised when a lockout of working occurs on a DS1 mapper or on an OC-48 or OC-192 optical interface circuit pack in a BLSR configuration.

This is an advisory message warning that the working circuit pack will not switch to protection even if the working circuit pack fails.

Note 1: You cannot perform a lockout on a DSM DS1x84 termination module mapper.

Note 2: You cannot perform a lockout on a Host OC-3 or OC-3x4 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
- use an account with level 2 or higher user privilege code (UPC)

Step	Action
1	When maintenance is complete, release the circuit pack from lockout mode. See 323-1059-311, Releasing an optical line switch on page 1-30 or Releasing a protection switch on a tributary circuit pack on page 1-21.

—end—

Procedure 5-16
Loss of BITSout-A Pri. Timing Ref. or Loss of BITSout-B Pri. Timing Ref. or Loss of BITSout-A Sec. Timing Ref. or Loss of BITSout-B Sec. Timing Ref.

Probable cause

This alarm is raised when the VTX-48, VTX-48e, or STX-192 circuit pack detects an error (LOS, LOF, or AIS) on the primary or secondary timing reference provisioned for BITSOUT-A or BITSOUT-B.

Impact

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

Note: This is a secondary alarm. Another alarm should be raised against the facility (DS1, EC-1, OC-3, OC-12, OC-48, OC-192, BITSin) that is supplying the failed reference.

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 5-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

Step	Action
1	Retrieve all active and disabled alarms. See Retrieving active alarms for a network element on page 2-3.
2	This is a secondary alarm caused by a fault on the facility that was the timing source for the BITSout-A or B. Clear the facility alarms first, if they exist.
3	From the loss of BITSout primary or secondary timing reference alarms, determine which output reference is failing: BITSOUTA or BITSOUTB.
4	Retrieve the timing references in use on the shelf. See 323-1051-310, Retrieving synchronization data for a network element on page 1-2.
5	Retrieve all active and disabled alarms. See Retrieving active alarms for a network element on page 2-3.
6	Locate an alarm for the source you recorded in step 4.
7	Clear any alarms using the appropriate procedure. If there are no alarms and the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-17
Loss of Shelf Pri. Timing Ref. or Loss of Shelf Sec. Timing Ref.

Probable cause

This alarm is raised when the primary or secondary timing reference signal fails.

Loss of shelf timing reference or a timing reference degradation can cause traffic to fall out of synchronization. The frames and payloads drift and can affect traffic.

The VTX-48, VTX-48e, or STX-192 circuit pack will automatically switch the network element to the secondary timing reference if the primary reference is lost, and to holdover mode under any of the following circumstances:

- both primary and secondary references are lost
- when primary is lost and secondary was set to NONE
- if timing references are deprovisioned using a TL1 command
- if the network element is synchronized to the adjacent network element that is line-timed and sends a DUS synchronization message

The VTX-48, VTX-48e, or STX-192 circuit pack operates as if it is set to FREERUN if both primary and secondary timing references are set to NONE.

Impact

Major, non-service-affecting (M, NSA) alarm (unprotected)
Minor, non-service-affecting (m, NSA) alarm (protected)

Note 1: The shelf may be unable to maintain synchronization with the remainder of the network. The system will sync-switch to the other source if available.

Note 2: This is a secondary alarm. Another alarm should be raised against the facility (DS1, EC-1, OC-3, OC-12, OC-48, OC-192, BITSin) that is supplying the failed reference.

—continued—

Procedure 5-17 (continued)
Loss of Shelf Pri. Timing Ref. or Loss of Shelf Sec. Timing Ref.

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 5-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

Step	Action
1	Retrieve all active and disabled alarms. See Retrieving active alarms for a network element on page 2-3.
2	Look for any shelf timing reference fail alarms. Determine which reference failed: primary or secondary. Also, the HLDOVRSYNC condition can exist in the list. This condition indicates that the network element switched to holdover mode.
3	Retrieve the timing reference. See 323-1051-310, Retrieving synchronization data for a network element on page 1-2.
4	Record the source of the reference (primary or secondary).
5	Retrieve all active and disabled alarms. See Retrieving active alarms for a network element on page 2-3.
6	Locate an alarm for the source you identified in step 4. • Clear any alarms. • If there are no alarms and the alarm does not clear, contact your next level of support or your Nortel Networks group.

—end—

Procedure 5-18
Loss of Traffic

Probable cause

This alarm is raised for the following reasons:

- node is isolated from the network
- node is receiving a combination of VT/STS AIS or VT/STS RFI on all paths of a ring or on the active path of a linear system.
- combination of an optical interface loss of signal alarm and an optical interface unequipped alarm in a UPSR ring on one shelf

  Note: It is possible that these VT alarms are masked by one of the following alarms on the STS-1 path, but the VT AIS condition will still raise the Loss of traffic alarm:

  — STS Rx loss of pointer

  — STS Rx unequipped

  — STS Rx signal label mismatch

Impact

Critical, service-affecting (C, SA) alarm if traffic is affected for more than five DS1s or one or more DS3s
Major, service-affecting (M, SA) alarm if one to five DS1s are affected

Note 1: The alarm status is critical, service-affecting when this alarm is raised for a UPSR ring by the combination of an optical interface Loss of Signal alarm and an optical interface Unequipped alarm on one shelf.

Note 2: The alarm status is critical, service-affecting when the cumulative amount of DS1 facilities reporting VT Rx RFI faults and VT Rx AIS faults is at least six.

Note 3: The Loss of Traffic alarm may be cleared and replaced by additional alarms, such as LOF or LOS, if the AIS and RFI conditions indicate a Major 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 5-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

—continued—

Procedure 5-18 (continued)
Loss of Traffic

Step	Action
1	Retrieve all active and disabled alarms. See Retrieving active alarms for a network element on page 2-3.
2	Clear any of the following alarms: • STS Rx AIS • STS Rx loss of pointer • STS Rx RFI • STS Rx signal label mismatch • STS Rx unequipped • VT Rx AIS • VT Rx RFI
3	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-19
Low Voltage

Probable cause

This alarm is raised when a power brownout occurs because battery voltage to the shelf drops below a minimum level, approximately -40 V dc.

A brownout occurs at approximately -40 V dc. The shelf remains in brownout state until the voltage rises above -42 V dc. The shelf continues to carry traffic, but without alarm capacity as long as the battery voltage remains below -42 V dc. If the battery voltage drops below approximately -37 V dc, the shelf fails and stops carrying traffic.

Note 1: If the battery voltage was more than -42 V dc before the brownout, each circuit pack undergoes a cold restart when the battery voltage recovers and rises above – 42 V dc. The cold restart causes a brief loss of traffic on the shelf.

Note 2: The difference (hysteresis) in the detection and recovery voltages makes it possible for the battery voltage to drop below the brownout voltage on multiple occasions without causing the circuit packs to restart each time.

Note 3: A power brownout may occur at different voltages for different circuit packs.

Impact

Critical, service-affecting (C, SA) alarm

Note: The alarm status is critical because it is service-affecting if the battery voltage drops below -37 V dc.

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 5-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

—continued—

Procedure 5-19 (continued)
Low Voltage

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	Verify the power supply to the shelf raising the alarm. Use your company procedure to clear the power supply problem. If the alarm does not clear, go to the next step.

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.

Step	Action
3	

CAUTION
Risk of provisioning data loss and traffic loss
Ensure that the voltage is correct at the shelf and that all circuit packs are operating correctly before continuing. Replacing the shelf processor on a partially functioning network element can result in a loss of provisioning data and a loss of traffic.

Replace the shelf processor. See Replacing the shelf processor on page 3-7.

Step	Action
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-20
Manual Switch Complete

Probable cause

This alarm is raised when a manual switch occurs on a DS1 mapper or on an OC-48 or OC-192 optical interface circuit pack in a BLSR configuration.

Impact

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

Note: An actual failure will override a manual switch, but the switch time can be lengthened slightly in some cases.

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 manual switch. See 323-1059-311, Releasing a protection switch on a tributary circuit pack on page 1-21 or Releasing an optical line switch on page 1-30.

—end—

Procedure 5-21
Manual Switch Complete-Remote

Probable cause

This alarm is raised when a manual switch occurs on an OC-48 or OC-192 optical inteface circuit pack (BLSR configuration) in a far-end network element.

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 and release the switch. See 323-1059-311, Releasing an optical line switch on page 1-30.

—end—

Procedure 5-22
Max OPE Nodes on Ring Exceeded

Probable cause

This alarm is raised when the maximum number of the OPE circuit packs allowed on a Resilient Packet Ring is exceeded.

A maximum of 12 OPE circuit packs can be attached to a Resilient Packet Ring when at least one of the OPE circuit packs is either a 4x100BT or 4x100FX circuit pack. A maximum of 16 OPE circuit packs can be attached to a Resilient Packet Ring when all of the OPE circuit packs are 2xGigE.

Impact

Minor, non-service affecting (m, NSA) alarm for Packet Edge circuit packs

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	Detach one or more Packet Edge circuit packs from the Resilient Packet Ring until the number of attached circuit packs is equal than the maximum allowed (refer to the Probable cause). See 323-1059-320, Detaching an OPTera Packet Edge circuit pack from an RPR on page 5-24.
2	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-23
NE Prov Script File Load Failed

Probable cause

This alarm is raised when the command to load and execute a TL1 script file on a network element fails.

If this alarm is raised, no other save or restore can be performed on the same network element until this alarm is cleared.

Impact

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

Step	Action
1	Log in to a TL1 session and cancel this command by entering: `CANC-TL1SCRPT-NE:[TID]::CTAG;`
2	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-24
Node ID mismatch

Probable cause

This alarm is raised when:

- the source and destination node IDs are not a neighboring pair according to the provisioned BLSR configuration on the OC-48 or OC-192 circuit pack and
- the node ID does not match any other entry in the BLSR configuration
- a network element detects a message sent by another network element that is not identified as a neighbor according to the locally stored BLSR configuration
- an invalid BLSR configuration
- an incorrect fiber-optic cable connection

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 network processor. See 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Verify the BLSR provisioning. See 323-1059-320, Provisioning a BLSR (bidirectional) on page 4-2.
3	Perform a ring audit. See 323-1059-320, Performing a BLSR audit and retrieving diagnostics on page 6-45.
4	If the alarm does not clear, change the state of the OC-48 or OC-192 circuit pack raising the alarm to 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 to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
6	Replace the OC-48 or OC-192 circuit pack. See Replacing an OC-48 or OC-192 optical interface circuit pack in a BLSR on page 3-41.
7	Change the state of the OC-48 or OC-192 circuit pack to in-service. See 323-1059-350, Putting circuit pack equipment in service (IS) on page 2-16.

—end—

Procedure 5-25
OAM Not Available

Probable cause

This alarm is raised when an OAM link does not exist between the Host shelf and a working DSM DS1x84 termination module (TM) mapper and there is no connection through the DSM DS1x84 TM mate. The following scenarios illustrate seven common examples of how this alarm is raised:

- In a protected scenario, one of the Host OCn or a DSM DS1x84 TM mapper is misconnected. For example, connected to another network element or to a different DSM DS1x84 TM.
- In a protected scenario, a Host OCn experiences an SDCC failure.
- If a fiber cut occurs between an unprotected DSM DS1x84 TM mapper and the Host OCn, or if both fibers are cut in a protected scenario. An OCn Rx Loss Of Signal (C, SA) alarm is raised and the Host OCn raises the SDCC link failure alarm.
- In a protected scenario, both Host OC-3 circuit packs experience a cold restart.
- In an unprotected scenario, the Host OC-3 circuit pack undergoes a cold restart.
- In an unprotected scenario, the Host OC-3 or OC-3x4 circuit pack undergoes either a warm or cold restart.
- The fiber link may be intact but SDCC is not functioning because of a circuit pack mismatch or circuit pack failure.

  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 this alarm provided it has a mate with an OAM link (the mate informs the shelf processor that the circuit pack is missing).

Impact

Critical, service-affecting (C, SA) alarm, if carrying traffic
Minor, non-service-affecting (m, NSA) alarm, if carrying no traffic

—continued—

Procedure 5-25 (continued)
OAM Not Available

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 5-11, and in *Installation,* 323-1059-201
- 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 Host OC-3 circuit pack and DSM DS1x84 TM mapper raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
3	If the shelf processor, OCn circuit pack, or DSM DS1x84 TM mapper have been replaced or have undergone a restart, wait at least 7 minutes for the discovery process to complete.
4	Retrieve alarms and look for an OCn Rx Loss Of Signal (C, SA) alarm or SDCC link failure alarm on the Host OCn. The presence of these alarms indicate a fiber cut.
5	If the fibers have been cut, replace the fibers. If the fibers are not linked, connect them as required.
6	If this is a protected scenario and the alarm has not cleared, verify that the provisioned OCn line facilities in both the working and mate Host slots are linked by fiber to the OCn line facilities of the appropriate DSM DS1x84 TM mappers. Ensure there is no misconnection.
7	If this is an unprotected scenario and the alarm has not cleared, verify that the provisioned OCn line facilities in the Host slot are linked by fiber to the OCn line facilities of the appropriate DSM DS1x84 TM mapper. Ensure there is no misconnection.
8	Ensure the SDCC is functioning on the Host OCn circuit packs. See 323-1059-350, Enabling or disabling the lower layer SDCC parameters on page 2-39.
9	Verify the LEDs on the circuit packs to ensure none are failed. If one or both circuit packs have failed, replace the circuit pack. See Procedures for equipment replacement on page 3-1.

—continued—

Procedure 5-25 (continued)
OAM Not Available

Step	Action
10	If the alarm does not clear, restart the DSM DS1x84 TM mapper in slot 1. If the alarm does not clear, restart the protection DSM DS1x84 TM mapper in slot 2.
11	If the alarm does not clear, restart the Host OCn connected to the DSM DS1x84 TM mapper in slot 1. If the alarm does not clear, restart the Host OCn connected to the DSM DS1x84 TM mapper in slot 2.
12	Select Inventory from the Configuration menu to verify the existence of an OAM link to a DSM DS1x84 TM mapper in the Inventory window. • Find the grouping of DSM data based on the site address shown in the shelf column. • Select the DSM DS1x84 TM and search the circuit pack details for a valid Age or ONSC parameter value. ***Note:*** A DSM DS1x84 TM mapper has an OAM link if it has a valid AGE or ONSC parameter value.
13	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-26
OC3 Loopback Active, OC12 Loopback Active, OC48 Loopback Active, or OC192 Loopback Active

Probable cause

This alarm is raised when an operate loopback command is executed on an OC-3, OC-12, non-DWDM OC-48, or non-DWDM OC-192 facility. Execute loopback only during system testing. The loopback active alarm is an important advisory message. For example, if more than one user logs into a network element and one user activates loopback mode, the other users get this message.

Note: If a facility is not out-of-service, then you cannot put it in loopback mode. Also, loopback mode is not permitted when the circuit pack is not physically present or when the facility is in-service.

Impact

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

Note: Since the facility must be OOS (not carrying traffic) to operate the loopback, releasing the circuit does not affect the shelf function.

Requirements

To perform this procedure, you must:

- have an account with a level 2 or higher user privilege code (UPC)
- have the fiber connection information (that is, how the optical modules on each network element connect to other network elements).

Step	Action
1	Ensure you are logged into the network element. See 323-1059-302, Procedures for interface login and logout.
2	Identify the OC-n facility in loopback mode. See 323-1059-543, Retrieving active alarms for a network element.
3	Select Equipment & Facility Provisioning from the Configuration menu.
4	Under Equipment, select the OC-n equipment associated with the OC-n facility identified in step 2.
5	Under Facility, select the OC-n facility identified in step 2.
6	Click Test.
7	In the Test Functions dialog box, select Loopback in the Test Type list.
8	Click Release.

—end—

Procedure 5-27
OC3 Rx Line AIS

Probable cause

This alarm is raised when the network element detects an OC-3 alarm indication signal (AIS) in the SONET overhead.

This alarm is caused by one of the following conditions on the circuit pack that is the source of the alarmed signal:

- facility out of service
- circuit pack failed on the OC-3 or OC-3x4 circuit pack or on the DSM DS1x84 termination module (TM) mapper
- site address for the DS1 service module (DSM) is not defined

Impact

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, if inactive linear, protected linear, or without cross-connects

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)
- have the optical fiber connection information (that is, how the optical circuit packs on each network element connect to other network elements and how each OC-3 connects to the DSM)
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201

—continued—

Procedure 5-27 (continued)
OC3 Rx Line AIS

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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the Rx AIS alarm cleared. See Retrieving active alarms for a network element on page 2-3.
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	**If** the shelf is — **Then** go to equipped with a DSM — step 6 not equipped with a DSM — step 9
6	If a DSM is connected to the alarmed OC-3 or OC-3x4 circuit pack, retrieve the active alarms from the network element and verify if the DS1 service module SITE provisioning required alarm is also raised. If yes, use the appropriate procedure to clear the alarm.
7	Retrieve alarms from the network element to verify if the OC3 Rx Line AIS alarm cleared. See Retrieving active alarms for a network element on page 2-3. If the alarm clears, you have completed this procedure. If the alarm does not clear, go to the next step.
8	Use the optical fiber connection information to identify the transmit and receive sites of the alarmed signal.
9	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 from the local network element, you can travel to the remote site.
10	Retrieve all alarms from the remote network element. See Retrieving active alarms for a network element on page 2-3.

—continued—

Procedure 5-27 (continued)
OC3 Rx Line AIS

Step	Action
11	Look for an alarm message for the circuit pack connected to the original shelf. • If there are no alarms, ensure that the equipment and facility of the remote circuit pack are in service. Refer to the procedures for modifying the equipment primary state or modifying the facility primary state. See 323-1059-350, Changing a facility state to In Service (IS) on page 2-26 and 323-1059-350, Changing a facility state to Out of Service (OOS) on page 2-25. • If the alarm is OC-3 Rx RFI or circuit pack failed, replace the optical interface or DSM DS1x84 TM mapper 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 the DSM DS1x84 termination module mapper on page 3-26. • If there are other alarms, refer to the appropriate alarm clearing procedures
12	Retrieve all alarms from the remote network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
13	If the alarm does not clear, replace the optical interface or DSM DS1x84 TM mapper reporting 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 the DSM DS1x84 termination module mapper on page 3-26.
14	Retrieve all alarms from the original network element to see if the alarm cleared.
15	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-28
OC3 Rx Loss of Frame

Probable cause

This alarm is raised when the OC-3 or OC-3x4 circuit pack is unable to detect the framing bytes in the received signal.

This alarm is caused by one of the following conditions:

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

The network element cannot clear a Loss of Signal alarm until a framed OC-3 signal is detected. The first time an optical fiber is disconnected, the Loss Of Frame alarm clears and a Loss of Signal alarm is raised that will not change back to OC3 Rx loss of frame when the optical fiber is reattached.

Impact

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, if inactive linear, protected linear, or without cross-connects

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) at all nodes that are alarmed
- have the optical fiber connection information (that is, how the optical circuit packs on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element

—continued—

Procedure 5-28 (continued)
OC3 Rx Loss of Frame

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 optical fiber connection information to identify the transmit and receive sites of the alarmed signal.
3	Retrieve all alarms at the transmit end. Clear any alarms of higher order by following the appropriate procedure.
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	**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. Use the optical power meter to measure the receive power.
6	If the power is below the receiver sensitivity for this circuit pack, perform the following steps for OC3 Rx loss of frame: ***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 5-28 (continued)
OC3 Rx Loss of Frame

Step	Action
	e. If the power is below the launch power (minimum), replace the OC-3 or OC-3x4 circuit pack at the transmit end. 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.
	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.
	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.
7	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.
8	If the alarm does not clear, replace the optical interface circuit pack raising the alarm.
9	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-29
OC3 Rx Loss of Signal

Probable cause

This alarm is raised when the OC-3 or OC-3x4 circuit pack can no longer detect a signal on the optical fiber.

This alarm is caused by one of the following conditions on the network element or DS1 service module (DSM):

- circuit pack missing
- circuit pack mismatch
- optical fiber cut
- dirty optical fibers
- dirty connectors
- excessive attenuation
- incorrect optical fiber cross-connect

The network element cannot clear a Loss of Signal alarm until a framed OC-3 or DS1 (DS1 from the DSM DS1x84 termination module mapper) signal is detected.

Impact

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, if inactive linear, protected linear, or without cross-connects

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 circuit packs on each network element connect to other network elements and how each OC-3 or OC-3x4 circuit pack connects to the DSM)
- have an optical power meter with the same optical connectors as the network element

—continued—

Procedure 5-29 (continued)
OC3 Rx Loss of Signal

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 optical fiber connection information to identify the transmit and receive sites of the alarmed signal.
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	Retrieve all alarms at the transmit end. If the system configuration is UPSR, and if the shelf processor at the transmit site has service affecting alarms against tributary circuit packs, place the optical circuit pack at the transmit site out-of-service. If the service affecting alarms begin to clear within 5 minutes, replace that optical circuit pack. If the service affecting alarms do not begin to clear within 5 minutes, place the optical circuit pack back in-service. Clear any alarms of higher order by following the appropriate procedure.
5	**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. Use the optical power meter to measure the receive power.

—continued—

Procedure 5-29 (continued)
OC3 Rx Loss of Signal

Step	Action
6	If the power is below the receiver sensitivity for this circuit pack, perform the following steps for OC3 Rx loss of signal: ***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 OC-3 or OC-3x4 circuit pack at the transmit end. 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. **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. **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.
7	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.
8	If the alarm does not clear, replace the optical interface circuit pack raising the alarm.
9	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-30
OC3 Rx RFI

Probable cause

This alarm is raised when the network element detects an OC-3 remote fault indication (RFI) in the SONET overhead because of a fault on another network element, or an optical fiber has been cut. Also, this alarm is raised if the site address for an attached DS1 service module (DSM) is not defined.

Impact

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, if inactive linear, protected linear, or without cross-connects

Note: This is a secondary alarm. An alarm of higher severity should be raised on the matching optic circuit pack on the next network element.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- have all the optical fiber connection information (that is, how the optical circuit packs on each network element connect to other network elements and how each OC-3 or OC-3x4 circuit pack connects to the DSM)
- use an account with level 1 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	**If** the shelf is … **Then** go to: equipped with a DSM → step 3; not equipped with a DSM → step 7
3	If a DSM is connected to the alarmed OC-3 or OC-3x4 circuit pack, retrieve the active alarms from the network element and verify if the DSM SITE provisioning required alarm is also raised. If yes, use the appropriate procedure to clear the alarm.
4	Wait 2 to 5 minutes.

—continued—

Procedure 5-30 (continued)
OC3 Rx RFI

Step	Action
5	Retrieve alarms from the network element to verify if the OC3 Rx RFI alarm cleared. See Retrieving active alarms for a network element on page 2-3. If the alarm clears, you have completed this procedure. If the alarm does not clear, go to the next step.
6	Use the optical fiber connection information to identify the network element and the module that is the source of the signal into the module reporting the alarm.
7	Log into the remote network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1. ***Note:*** If you cannot log in from the local network element, you can travel to the remote site.
8	Retrieve all alarms from the remote network element. See Retrieving active alarms for a network element on page 2-3.
9	Look for an alarm message for the OC-3 or OC-3x4 circuit pack that connects to the original shelf.
10	Clear any alarms using the appropriate procedure.
11	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-31
OC3 Rx section trace mismatch

Probable cause

This alarm is raised when the section trace message on the received facility does not match the expected facility section trace message.

Note: This alarm is only raised if the section trace failure mode is Alarms on or Alarms on, with traffic protection.

Impact

Major, service-affecting (M, SA) alarm, if in Alarms on mode
Major, service-affecting (M, SA) alarm (UPSR ring with cross-connects), if in Alarms on, with traffic protection mode
Major, service-affecting (M, SA) alarm, if active linear or unprotected with cross-connects, if in Alarms on, with traffic protection mode
Minor, non-service-affecting (m, NSA) alarm, if inactive linear, protected linear, or without cross-connects, if in Alarms on, with traffic protection mode

Note: This alarm has dual severity in Alarms on, with traffic protection mode with 1+1 protection.

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 5-11, 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	Verify that the optical fiber connections are correct on the optical interface circuit pack that is raising the alarm, that is, on the receive network element.

—continued—

Procedure 5-31 (continued)
OC3 Rx section trace mismatch

Step	Action
3	Retrieve the section trace values on OC-3 facilities. See 323-1059-520, Retrieving section trace messages on page 2-2.
4	Verify if the OC-48 interworking is set correctly according to the following setting:

If the far-end network element is	**Then** ensure that the OC-48 interworking check box is
an S/DMS TransportNode OC-48 network element	selected
not an S/DMS TransportNode OC-48 network element	not selected

5	If the OC-48 interworking is not set correctly, change the setting. See 323-1059-520, Editing section trace messages on page 2-4.
6	If the alarm does not clear, retrieve and take note of the section trace messages of the OC-3 signal at the transmit network element and at the alarmed receive network element. See 323-1059-520, Retrieving section trace messages on page 2-2.
7	Compare the section trace Format parameter (Number or String) of the transmit signal at the transmit network element with that of the receive signal at the alarmed receive network element. If the values are different, change the Format value of the receive signal at the alarmed receive network element to match the Format value of the transmit signal. See 323-1059-520, Editing section trace messages on page 2-4.
8	Compare the Transmitted section trace value of the transmit signal at the transmit network element with the Expected Rx section trace value of the receive signal at the receive network element. If the values are different, change the Expected Rx section trace value of the receive signal at the alarmed network element to match the Transmitted section trace value of the transmit signal. See 323-1059-520, Editing section trace messages on page 2-4.
9	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-32
OC3 Rx Signal Degrade

Probable cause

This alarm is raised when the received signal is significantly degraded.

One of the following conditions cause this alarm:

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

Impact

Minor, service-affecting (m, SA) alarm for a UPSR with cross-connects
Minor, service-affecting (m, SA) alarm, if active linear or unprotected with cross-connects
Minor, non-service-affecting (m, NSA) alarm, if inactive linear, protected linear, or without cross-connects

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 5-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)
- have an optical power meter with the same optical connectors as the network element

—continued—

Procedure 5-32 (continued)
OC3 Rx Signal Degrade

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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the signal degrade alarm cleared.
4	If the alarm does not clear, identify the circuit pack raising the alarm.
5	Use the optical fiber connection information to identify the network element and the module that is the source of the signal in to the module reporting the alarm. See Retrieving active alarms for a network element on page 2-3.
6	Retrieve all alarms at the transmit end: • Clear any higher order alarms using the appropriate procedures. • If OC-3 Rx RFI is the only alarm, go to the next step.
7	Retrieve the line signal degrade threshold (SDTH) and compare the SDTH with the network diagram. See 323-1059-311, Retrieving the line SDTH of an optical facility on page 1-36. Edit the SDTH, as required. See 323-1059-311, Editing the line SDTH of an optical facility on page 1-37.
8	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
9	 **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. Use the optical power meter to measure the receive power at the receive end.

—continued—

Procedure 5-32 (continued)
OC3 Rx Signal Degrade

Step	Action
10	If the power is below the receiver sensitivity for this circuit pack, perform the following steps for OC3 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 OC-3 or OC-3x4 circuit pack at the transmit end. 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. **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. **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, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-33
OC3 Rx Signal Failure

Probable cause

This alarm is raised when the received optical signal is degraded to the point where it is unusable.

One of the following conditions causes this alarm:

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

Impact

Critical, service-affecting (C, SA) alarm (UPSR ring with cross-connects)
Critical, service-affecting (C, SA) alarm (active linear, or unprotected with cross-connects)
Minor, non-service-affecting (m, NSA) alarm (linear, protected linear, or without cross-connects)

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)
- have an optical power meter with the same optical connectors as the network element
- use an account with level 1 or higher user privilege code (UPC)

—continued—

Procedure 5-33 (continued)
OC3 Rx Signal Failure

Step	Action
1	Retrieve all 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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the signal failure alarm cleared. See Retrieving active alarms for a network element on page 2-3.
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 the receive sites of the alarmed signal.
6	Retrieve alarms at the transmit end: • Clear any higher order alarms using the appropriate procedure. • If OC3 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.
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. Use the optical power meter to measure the receive power.

—continued—

Procedure 5-33 (continued)
OC3 Rx Signal Failure

Step	Action
9	If the power is below the receiver sensitivity for this circuit pack, perform the following steps for OC3 Rx signal failure: ***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 OC-3 or OC-3x4 circuit pack at the transmit end. 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. **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. **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.
10	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.
11	If the alarm does not clear, replace the circuit pack reporting the alarm.
12	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-34
OC12 Rx Line AIS

Probable cause

This alarm is raised when the network element detects an OC-12 alarm indication signal (AIS) in the SONET overhead.

This alarm is caused by one of the following conditions on the circuit pack that is the source of the alarmed signal:

- facility out-of-service
- circuit pack failed

Impact

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, if inactive linear, protected linear, or without cross-connects

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)
- have the optical fiber connection information (that is, how the optical circuit packs on each network element connect to other network elements)
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201

—continued—

Procedure 5-34 (continued)
OC12 Rx Line AIS

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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the Rx AIS alarm cleared. See Retrieving active alarms for a network element on page 2-3.
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	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 from the local network element, you can travel to the remote site.
7	Retrieve all alarms from the remote network element. See Retrieving active alarms for a network element on page 2-3.
8	Look for an alarm message for the circuit pack connected to the original shelf.
9	If there are no alarms, ensure that the equipment and facility of the remote circuit pack are in-service. Refer to the procedures for modifying the equipment primary state or modifying the facility primary state. See 323-1059-350, Changing a facility state to Out of Service (OOS) on page 2-25.
10	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
11	If the alarm is OC12 Rx RFI or circuit pack failed, replace the OC-12 or OC-12x4 STS circuit pack at the transmit end. See Detailed procedures for active alarms on page 4-1.
12	If there are other alarms, refer to the appropriate alarm clearing procedures.
13	Retrieve all alarms from the remote 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, replace the optical interface circuit pack reporting the alarm. See Detailed procedures for active alarms on page 4-1.
15	Retrieve all alarms from the original network element to see if the alarm cleared.
16	If the alarm does not clear, contact your next level of support or your Nortel Networks support group

—end—

Procedure 5-35
OC12 Rx Loss of Frame

Probable cause

This alarm is raised when the OC-12 or OC-12x4 STS circuit pack is unable to detect the framing bytes in the received signal.

This alarm is caused by one of the following conditions:

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

The network element cannot clear a Loss of Signal alarm until a framed OC-12 signal is detected. The first time a optical fiber is disconnected, the Loss Of Frame alarm clears and a Loss of Signal alarm is raised. The alarm will not change back to OC12 Rx loss of frame when the optical fiber is reattached.

Impact

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, if inactive linear, protected linear, or without cross-connects

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)
- have the optical fiber connection information (that is, how the optical circuit packs on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element

—continued—

Procedure 5-35 (continued)
OC12 Rx Loss of Frame

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 optical fiber connection information to identify the transmit and receive sites of the alarmed signal.
3	Retrieve all alarms at the transmit end. Clear any alarms of higher order by following the appropriate procedure.
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	**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. Use the optical power meter to measure the receive power.

—continued—

Procedure 5-35 (continued)
OC12 Rx Loss of Frame

Step	Action
6	If the power is below the receiver sensitivity for this circuit pack, perform the following steps for OC12 Rx loss of frame: ***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 OC-12 or OC-12x4 STS circuit pack at the transmit end. 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. **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. **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.
7	If the power is above the receiver sensitivity for this circuit pack, clean and reattach both optical fibers. See *Installation*, 323-1059-201.
8	If the alarm does not clear, replace the OC-12 or OC-12x4 STS circuit pack.
9	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-36
OC12 Rx Loss of Signal

Probable cause

This alarm is raised when the OC-12 or OC-12x4 STS circuit pack can no longer detect a signal on the optical fiber.

This alarm is caused by one of the following conditions:

- circuit pack missing
- circuit pack mismatch
- optical fiber cut
- dirty optical fibers
- dirty connectors
- excessive attenuation
- incorrect optical fiber cross-connect

The network element cannot clear a Loss of Signal alarm until a framed OC-12 signal is detected.

Impact

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, if inactive linear, protected linear, or without cross-connects

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)
- have an optical power meter with the same optical connectors as the network element
- use an account with level 1 or higher user privilege code (UPC)

—continued—

Procedure 5-36 (continued)
OC12 Rx Loss of Signal

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 optical fiber connection information to identify the transmit and receive sites of the alarmed signal.
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	Retrieve all alarms at the transmit end. If the system configuration is UPSR, and if the shelf processor at the transmit site has service affecting alarms against tributary circuit packs, place the optical circuit pack at the transmit site out-of-service. If the service affecting alarms begin to clear within 5 minutes, replace that optical circuit pack. If the service affecting alarms do not begin to clear within 5 minutes, place the optical circuit pack back in-service. Clear any alarms of higher order by following the appropriate procedure.
5	**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. Use the optical power meter to measure the receive power.

—continued—

Procedure 5-36 (continued)
OC12 Rx Loss of Signal

Step	Action
6	If the power is below the receiver sensitivity for this circuit pack, perform the following steps for OC12 Rx loss of signal: ***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 or Replacing an optical interface circuit pack in a UPSR on page 3-38. **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. **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.
7	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.
8	If the alarm does not clear, replace the optical interface circuit pack raising the alarm.
9	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-37
OC12 Rx RFI

Probable cause

This alarm is raised when the network element detects an OC-12 remote fault indication (RFI) in the SONET overhead because of a fault on another network element or a optical fiber has been cut.

Impact

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, if inactive linear, protected linear, or without cross-connects

Note: This is a secondary alarm. An alarm of higher severity should be raised on the matching optic circuit pack on the next network element.

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)
- use an account with level 1 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	Use the optical fiber connection information to identify the network element and the module that is the source of the signal in to the module reporting the alarm.
3	Log into the remote network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1 ***Note:*** If you cannot log in from the local network element, you can travel to the remote site.
4	Retrieve all alarms from the remote network element. See Retrieving active alarms for a network element on page 2-3.
5	Look for an alarm message for the OC-12 or OC-12x4 STS circuit pack that connects to the original shelf.

—continued—

Procedure 5-37 (continued)
OC12 Rx RFI

Step	Action
6	Clear any alarms using the appropriate procedure.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-38
OC12 Rx Section Trace Mismatch

Probable cause

This alarm is raised when the section trace message on the received facility does not match the expected facility section trace message.

Note: This alarm is only raised if the section trace failure mode is Alarms on or Alarms on, with traffic protection.

Impact

Major, service-affecting (M, SA) alarm, if in Alarms on mode
Major, service-affecting (M, SA) alarm (UPSR ring with cross-connects), if in Alarms on, with traffic protection mode
Major, service-affecting (M, SA) alarm, if active linear or unprotected with cross-connects, if in Alarms on, with traffic protection mode
Minor, non-service-affecting (m, NSA) alarm, if inactive linear, protected linear, or without cross-connects, if in Alarms on, with traffic protection mode

Note: This alarm has dual severity in Alarms on, with traffic protection mode with 1+1 protection.

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 5-11, 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	Verify that the optical fiber connections are correct on the optical interface circuit pack that is raising the alarm, that is, on the receive network element.

—continued—

Procedure 5-38 (continued)
OC12 Rx Section Trace Mismatch

Step	Action
3	If the alarm does not clear, retrieve and take note of the section trace messages of the OC-12 signal at the transmit network element and at the alarmed receive network element. See 323-1059-520, Retrieving section trace messages on page 2-2.
4	Compare the section trace Format parameter (Number or String) of the transmit signal at the transmit network element with that of the receive signal at the alarmed receive network element. If the values are different, change the Format value of the receive signal at the alarmed receive network element to match the Format value of the transmit signal. See 323-1059-520, Editing section trace messages on page 2-4.
5	Compare the Transmitted section trace value of the transmit signal at the transmit network element with the Expected Rx section trace value of the receive signal at the receive network element. If the values are different, change the Expected Rx section trace value of the receive signal at the alarmed network element to match the Transmitted section trace value of the transmit signal. See 323-1059-520, Editing section trace messages on page 2-4.
6	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-39
OC12 Rx Signal Degrade

Probable cause

This alarm is raised when the received signal is degraded significantly.

This alarm is caused by one of the following conditions:

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

Impact

Minor, service-affecting (m, SA) alarm for a UPSR with cross-connects
Minor, service-affecting (m, SA) alarm, if active linear or unprotected with cross-connects
Minor, non-service-affecting (m, NSA) alarm, if inactive linear, protected linear, or without cross-connects

> ***Note:*** The alarm status is service-affecting on a ring system because the OC-12 line is not protected. 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.

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 5-11, and in *Installation,* 323-1059-201.
- use an account with level 1 or higher user privilege code (UPC)
- have an optical power meter with the same optical connectors as the network element

—continued—

Procedure 5-39 (continued)
OC12 Rx Signal Degrade

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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the signal degrade alarm cleared.
4	If the alarm does not clear, identify the circuit pack raising the alarm.
5	Use the optical fiber connection information to identify the network element and the module that is the source of the signal in to the module reporting the alarm. See Retrieving active alarms for a network element on page 2-3.
6	Retrieve all alarms at the transmit end: • Clear any higher order alarms using the appropriate procedures. • If OC-12 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.
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. Use the optical power meter to measure the receive power at the receive end.

—continued—

Procedure 5-39 (continued)
OC12 Rx Signal Degrade

Step	Action
9	If the power is below the receiver sensitivity for this circuit pack, perform the following steps for OC12 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 OC-12 or OC-12x4 STS circuit pack at the transmit end. 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. **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. **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.
10	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.
11	If the alarm does not clear, replace the OC-12 or OC-12x4 STS circuit pack raising the alarm. 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.
12	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-40
OC12 Rx Signal Failure

Probable cause

This alarm is raised when the received optical signal is degraded to the point where it is unusable.

One of the following conditions causes this alarm:

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

Impact

Critical, service-affecting (C, SA) alarm UPSR ring with cross-connects
Critical, service-affecting (C, SA) alarm, active linear or unprotected with cross-connects
Minor, non-service-affecting (m, NSA) alarm inactive linear, protected linear, or without cross-connects

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)
- have an optical power meter with the same optical connectors as the network element
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

—continued—

Procedure 5-40 (continued)
OC12 Rx Signal Failure

Step	Action
1	Retrieve all 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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the signal failure alarm cleared. See Retrieving active alarms for a network element on page 2-3.
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 the receive sites of the alarmed signal.
6	Retrieve alarms at the transmit end: • Clear any higher order alarms using the appropriate procedure. • If OC12 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.
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. Use the optical power meter to measure the receive power.

—continued—

Procedure 5-40 (continued)
OC12 Rx Signal Failure

Step	Action
9	If the power is below the receiver sensitivity for this circuit pack, perform the following steps for OC12 Rx signal failure: ***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 OC-12 or OC-12x4 STS circuit pack at the transmit end. 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. **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. **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.
10	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.
11	If the alarm does not clear, replace the circuit pack reporting the alarm. 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.
12	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-41
OC48 Rx Line AIS

Probable cause

This alarm is raised when the network element detects an OC-48 alarm indication signal (AIS) in the SONET overhead.

This alarm is caused by one of the following conditions on the circuit pack that is the source of the alarmed signal:

- facility out of service
- circuit pack failed

Impact

Critical, service-affecting (C, SA) alarm for a UPSR if cross-connects are provisioned
Critical, service-affecting (C, SA) alarm for an unprotected BLSR
Critical, service-affecting (C, SA) alarm, if active linear or unprotected with cross-connects
Minor, non-service-affecting (m, NSA) alarm if inactive linear, protected linear, or without cross-connects
Minor, non-service-affecting (m, NSA) alarm for a protected BLSR

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)
- have the optical fiber connection information (that is, how the optical circuit packs on each network element connect to other network elements)

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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	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.
4	Use the optical fiber connection information to identify the transmit and receive sites of the alarmed signal.
5	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.

—continued—

Procedure 5-41 (continued)
OC48 Rx Line AIS

Step	Action
6	Retrieve all alarms from the remote network element. See Retrieving active alarms for a network element on page 2-3.
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	Look for an alarm message for the circuit pack connected to the original shelf. • If there are no alarms, ensure that the equipment and facility of the remote circuit pack are in service. Refer to the procedures for modifying the equipment primary state or modifying the facility primary state. See 323-1059-350, Changing a facility state to In Service (IS) on page 2-26. • If the alarm is OC-48 Rx RFI or circuit pack failed, replace the optical interface 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. • If there are other alarms, refer to the appropriate alarm clearing procedures
9	Retrieve all alarms from the remote network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
10	If the alarm does not clear, replace the optical interface circuit pack reporting 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.
11	Retrieve all alarms from the original network element to see if the alarm cleared.
12	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-42
OC48 Rx Loss of Frame

Probable cause

This alarm is raised when the OC-48 or OC-48 STS circuit pack is unable to detect the framing bytes in the received signal.

This alarm is caused by one of the following conditions:

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

The network element cannot clear a Loss of Signal alarm until a framed OC-48 signal is detected. The first time an optical fiber is disconnected, the Loss Of Frame alarm clears and a Loss of Signal alarm is raised that will not change back to OC48 Rx loss of frame when the optical fiber is reattached.

Impact

Critical, service-affecting (C, SA) alarm for a UPSR with cross-connects
Critical, service-affecting (C, SA) alarm, if active linear or unprotected with cross-connects
Critical, service-affecting (C, SA) alarm for an unprotected BLSR
Minor, non-service-affecting (m, NSA) alarm if inactive linear, protected linear, or without cross-connects
Minor, non-service-affecting (m, NSA) alarm for a protected BLSR

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)
- have an optical power meter with the same optical connectors as the network element
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

—continued—

Procedure 5-42 (continued)
OC48 Rx Loss of Frame

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 optical fiber connection information to identify the transmit and receive sites of the alarmed signal.
3	Retrieve all alarms at the transmit end. Clear any alarms of higher order by following the appropriate procedure.
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	**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. Use the optical power meter to measure the receive power.
6	Measure the receive power using an optical power meter. If the power is below the receiver sensitivity for this circuit pack, perform the following steps for OC48 Rx loss of frame: ***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 5-42 (continued)
OC48 Rx Loss of Frame

Step	Action
	e. If the power is below the launch power (minimum), replace the OC-48 or OC-48 STS circuit pack at the transmit end. 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, 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.
	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.
7	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.
8	If the alarm does not clear, replace the optical interface circuit pack.
9	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-43
OC48 Rx Loss of Signal

Probable cause

This alarm is raised when the OC-48 or OC-48 STS circuit pack can no longer detect a signal on the optical fiber.

This alarm is caused by one of the following conditions:

- circuit pack missing
- circuit pack mismatch
- optical fiber cut or disconnect
- dirty optical fibers
- dirty connectors
- excessive attenuation
- incorrect optical fiber cross-connect

The network element cannot clear a Loss of Signal alarm until a framed OC-48 signal is detected.

Impact

Critical, service-affecting (C, SA) alarm for a UPSR with cross-connects
Critical, service-affecting (C, SA) alarm, if active linear or unprotected with cross-connects
Critical, service-affecting (C, SA) alarm for an unprotected BLSR
Minor, non-service-affecting (m, NSA) alarm if inactive linear, protected linear, or without cross-connects
Minor, non-service-affecting (m, NSA) alarm for a protected BLSR

Note: In BLSR systems, alarm may escalate to critical, service-affecting (C, SA) when the SPx is restarted.

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)
- have an optical power meter with the same optical connectors as the network element
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201

—continued—

Procedure 5-43 (continued)
OC48 Rx Loss of Signal

- use an account with level 1 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	Use the optical fiber connection information to identify the transmit and receive sites of the alarmed signal.
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	Retrieve all alarms at the transmit end. If the system configuration is UPSR, and if the shelf processor at the transmit site has service affecting alarms against tributary circuit packs, place the optical circuit pack at the transmit site out-of-service. If the service affecting alarms begin to clear within 5 minutes, replace that optical circuit pack. If the service affecting alarms do not begin to clear within 5 minutes, place the optical circuit pack back in-service.Clear any alarms of higher order by following the appropriate procedure.
5	**CAUTION** **Risk of traffic loss** Ensure that the correct module is identified. Removing the incorrect 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. Use the optical power meter to measure the receive power.
6	Measure the receive power using an optical power meter. If the power is below the receiver sensitivity for this circuit pack, perform the following steps for OC48 Rx loss of signal: ***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.

—continued—

Procedure 5-43 (continued)
OC48 Rx Loss of Signal

Step	Action
	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 OC-48 or OC-48 STS circuit pack at the transmit end. 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, 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.
	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.
7	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.
8	If the alarm does not clear, replace the optical interface circuit pack.
9	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-44
OC48 Rx RFI

Probable cause

This alarm is raised when the network element detects an OC-48 remote fault indication (RFI) in the SONET overhead because of a fault on another network element, or an optical fiber has been cut.

Impact

Critical, service-affecting (C, SA) alarm for a UPSR with cross-connects
Critical, service-affecting (C, SA) alarm, if active linear or unprotected with cross-connects
Critical, service-affecting (C, SA) if on an active BLSR
Minor, non-service-affecting (m, NSA) alarm, if inactive linear, protected linear, or without cross-connects
Minor, non-service-affecting (m, NSA) for a non-active BLSR

Note: This is a secondary alarm. An alarm of higher severity is raised on the matching optical interface circuit pack on the next network element.

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)

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 optical fiber connection information to identify the network element and the module that is the source of the signal in to the circuit pack reporting the alarm.
3	Log into the remote network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1. ***Note:*** If you cannot log in from the local network element, you can travel to the remote site.
4	Retrieve all alarms from the remote network element. See Retrieving active alarms for a network element on page 2-3.
5	Look for an alarm message for the OC-48 or OC-48 STS circuit pack that connects to the original shelf.
6	Clear any alarms using the appropriate procedure.

—continued—

Procedure 5-44 (continued)
OC48 Rx RFI

Step	Action
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-45
OC48 Rx Section Trace Mismatch

Probable cause

This alarm is raised when the section trace message on the received facility does not match the expected facility section trace message.

> ***Note:*** This alarm is only raised if the section trace failure mode is Alarms on or Alarms on, with traffic protection.

Impact

Major, service-affecting (M, SA) alarm, if in Alarms on mode
Major, service-affecting (M, SA) alarm (UPSR ring with cross-connects), if in Alarms on, with traffic protection mode
Major, service-affecting (M, SA) alarm, if active linear, active BLSR, or unprotected with cross-connects, if in Alarms on, with traffic protection mode
Minor, non-service-affecting (m, NSA) alarm, if inactive linear, inactive BLSR, protected linear, protected BLSR, or without cross-connects, if in Alarms on, with traffic protection mode

> ***Note:*** This alarm has dual severity in Alarms on, with traffic protection mode with 1+1 protection.

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 5-11, 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	Verify that the optical fiber connections are correct on the optical interface circuit pack that is raising the alarm, that is, on the receive network element.
3	If the alarm does not clear, retrieve and take note of the section trace messages of the OC-48 signal at the transmit network element and at the alarmed receive network element. See 323-1059-520, Retrieving section trace messages on page 2-2.

—continued—

Procedure 5-45 (continued)
OC48 Rx Section Trace Mismatch

Step	Action
4	Compare the section trace Format parameter (Number or String) of the transmit signal at the transmit network element with that of the receive signal at the alarmed receive network element. If the values are different, change the Format value of the receive signal at the alarmed receive network element to match the Format value of the transmit signal. See 323-1059-520, Editing section trace messages on page 2-4.
5	Compare the Transmitted section trace value of the transmit signal at the transmit network element with the Expected Rx section trace value of the receive signal at the receive network element. If the values are different, change the Expected Rx section trace value of the receive signal at the alarmed network element to match the Transmitted section trace value of the transmit signal. See 323-1059-520, Editing section trace messages on page 2-4.
6	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-46
OC48 Rx Signal Degrade

Probable cause

This alarm is raised when the received signal is significantly degraded.

One of the following conditions cause this alarm:

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

Impact

Minor, service-affecting (m, SA) alarm for a UPSR with cross-connects
Minor, service-affecting (m, SA) alarm, if active linear or unprotected with cross-connects
Minor, non-service-affecting (m, NSA) alarm, if inactive linear, protected linear, or without cross-connects
Minor, non-service-affecting (m, NSA) alarm for an inactive BLSR
Minor, service-affecting (m, SA) alarm for an active BLSR

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)
- have an optical power meter with the same optical connectors as the network element
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

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. Alarm hierarchies on page 5-9.

—continued—

Procedure 5-46 (continued)
OC48 Rx Signal Degrade

Step	Action
3	Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
4	Retrieve alarms to determine if the signal degrade alarm cleared.
5	If the alarm does not clear, identify the circuit pack raising the alarm.
6	Use the optical fiber connection information to identify the network element and the module that is the source of the signal in to the module reporting the alarm. See Retrieving active alarms for a network element on page 2-3.
7	Retrieve all alarms at the transmit end: • Clear any higher order alarms using the appropriate procedures. • If OC-48 Rx RFI is the only alarm, go to the next step.
8	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
9	**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. Use the optical power meter to measure the receive power at the receive end.
10	Measure the receive power using an optical power meter. If the power is below the receiver sensitivity for this circuit pack, perform the following steps for OC48 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.

—continued—

Procedure 5-46 (continued)
OC48 Rx Signal Degrade

Step	Action
	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 OC-48 or OC-48 STS circuit pack at the transmit end. 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, 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.
	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, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-47
OC48 Rx Signal Failure

Probable cause

This alarm is raised when the received optical signal is degraded to the point where it is unusable.

One of the following conditions causes this alarm:

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

Impact

Critical, service-affecting (C, SA) alarm for a UPSR with cross-connects
Critical, service-affecting (C, SA) alarm, if active linear or unprotected with cross-connects
Critical, service-affecting (C, SA) if on an active BLSR
Minor, non-service-affecting (m, NSA) alarm, if inactive linear, protected linear, or without cross-connects
Minor, non-service-affecting (m, NSA) for a non-active BLSR

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)
- have an optical power meter with the same optical connectors as the network element
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

—continued—

Procedure 5-47 (continued)
OC48 Rx Signal Failure

Step	Action
1	Retrieve all 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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the signal failure alarm cleared. See Retrieving active alarms for a network element on page 2-3.
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 the receive sites of the alarmed signal.
6	Retrieve alarms at the transmit end: • Clear any higher order alarms using the appropriate procedure. • If OC48 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.
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. Use the optical power meter to measure the receive power.

—continued—

Procedure 5-47 (continued)
OC48 Rx Signal Failure

Step	Action
9	Measure the receive power using an optical power meter. If the power is below the receiver sensitivity for this circuit pack, perform the following steps for OC48 Rx signal failure: ***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 OC-48 or OC-48 STS circuit pack at the transmit end. 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, 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. **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.
10	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.
11	If the alarm does not clear, replace the circuit pack reporting the alarm.
12	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-48
OC192 Rx Line AIS

Probable cause

This alarm is raised when the network element detects an OC-192 alarm indication signal (AIS) in the SONET overhead.

This alarm is caused by one of the following conditions on the circuit pack that is the source of the alarmed signal:

- facility out of service
- circuit pack failed

Impact

Critical, service-affecting (C, SA) alarm for a UPSR if cross-connects are provisioned
Critical, service-affecting (C, SA) alarm for an unprotected BLSR
Critical, service-affecting (C, SA) alarm, if active linear or unprotected with cross-connects
Minor, non-service-affecting (m, NSA) alarm if inactive linear, protected linear, or without cross-connects
Minor, non-service-affecting (m, NSA) alarm for a protected BLSR

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)
- have the optical fiber connection information (that is, how the optical circuit packs on each network element connect to other network elements)

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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	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.
4	Use the optical fiber connection information to identify the transmit and receive sites of the alarmed signal.
5	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.

—continued—

Procedure 5-48 (continued)
OC192 Rx Line AIS

Step	Action
6	Retrieve all alarms from the remote network element. See Retrieving active alarms for a network element on page 2-3.
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	Look for an alarm message for the circuit pack connected to the original shelf. • If there are no alarms, ensure that the equipment and facility of the remote circuit pack are in service. Refer to the procedures for modifying the equipment primary state or modifying the facility primary state. See 323-1059-350, Changing a facility state to In Service (IS) on page 2-26. • If the alarm is OC-192 Rx RFI or circuit pack failed, replace the optical interface 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. • If there are other alarms, refer to the appropriate alarm clearing procedures
9	Retrieve all alarms from the remote network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
10	If the alarm does not clear, replace the optical interface circuit pack reporting 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.
11	Retrieve all alarms from the original network element to see if the alarm cleared.
12	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-49
OC192 Rx Loss of Frame

Probable cause

This alarm is raised when the OC-192 circuit pack is unable to detect the framing bytes in the received signal.

This alarm is caused by one of the following conditions:

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

The network element cannot clear a Loss of Signal alarm until a framed OC-192 signal is detected. The first time an optical fiber is disconnected, the Loss Of Frame alarm clears and a Loss of Signal alarm is raised that will not change back to OC192 Rx loss of frame when the optical fiber is reattached.

Impact

Critical, service-affecting (C, SA) alarm for a UPSR with cross-connects
Critical, service-affecting (C, SA) alarm, if active linear or unprotected with cross-connects
Critical, service-affecting (C, SA) alarm for an unprotected BLSR
Minor, non-service-affecting (m, NSA) alarm if inactive linear, protected linear, or without cross-connects
Minor, non-service-affecting (m, NSA) alarm for a protected BLSR

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)
- have an optical power meter with the same optical connectors as the network element
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

—continued—

Procedure 5-49 (continued)
OC192 Rx Loss of Frame

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 optical fiber connection information to identify the transmit and receive sites of the alarmed signal.
3	Retrieve all alarms at the transmit end. Clear any alarms of higher order by following the appropriate procedure.
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	**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. Use the optical power meter to measure the receive power.
6	Measure the receive power using an optical power meter. If the power is below the receiver sensitivity for this circuit pack, perform the following steps for OC192 Rx loss of frame: ***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 5-49 (continued)
OC192 Rx Loss of Frame

Step	Action
	e. If the power is below the launch power (minimum), replace the OC-192 circuit pack at the transmit end. 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, 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.
	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.
7	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.
8	If the alarm does not clear, replace the optical interface circuit pack.
9	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-50
OC192 Rx Loss of Signal

Probable cause

This alarm is raised when the OC-192 circuit pack can no longer detect a signal on the optical fiber.

This alarm is caused by one of the following conditions:

- circuit pack missing
- circuit pack mismatch
- optical fiber cut
- dirty optical fibers
- dirty connectors
- excessive attenuation
- incorrect optical fiber cross-connect

  Note: This includes when an OC-192 LR or OC-192 DWDM card is connected to a OC-192 IR circuit pack or connected to a OC-192 DWDM TR card (OPTera Connect DX).

- the EOI has shut down because the optical power input exceeds the specified maximum for the circuit pack

  Note: This applies to OC-192 LR and OC-192 DWDM circuit packs only.

The network element cannot clear a Loss of Signal alarm until a framed OC-192 signal is detected.

Impact

Critical, service-affecting (C, SA) alarm for a UPSR with cross-connects
Critical, service-affecting (C, SA) alarm, if active linear or unprotected with cross-connects
Critical, service-affecting (C, SA) alarm for an unprotected BLSR
Minor, non-service-affecting (m, NSA) alarm if inactive linear, protected linear, or without cross-connects
Minor, non-service-affecting (m, NSA) alarm for a protected BLSR

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)

—continued—

Procedure 5-50 (continued)
OC192 Rx Loss of Signal

- have an optical power meter with the same optical connectors as the network element
- observe all safety requirements described in Safety requirements on page 5-11, 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 raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	**If** the circuit pack raising the alarm **Then** **is** an OC-192 LR or OC-192 DWDM connected to an OC-192 IR: replace the OC-192 IR circuit pack with one that supports G.709 FEC such as OC192 LR or OC-192 DWDM. See 323-1059-543, Equipment replacement on page 3-1. **is not** an OC-192 LR or OC-192 DWDM connected to an OC-192 IR: go to step 3
3	Use the optical fiber connection information to identify the transmit and receive sites of the alarmed signal.
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	Retrieve all alarms at the transmit end. If the system configuration is UPSR, and if the shelf processor at the transmit site has service affecting alarms against tributary circuit packs, place the optical circuit pack at the transmit site out-of-service. If the service affecting alarms begin to clear within 5 minutes, replace that optical circuit pack. If the service affecting alarms do not begin to clear within 5 minutes, place the optical circuit pack back in-service.Clear any alarms of higher order by following the appropriate procedure.

—continued—

Procedure 5-50 (continued)
OC192 Rx Loss of Signal

Step	Action

6

CAUTION
Risk of traffic loss
Ensure that the correct module is identified. Removing the incorrect 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.

Measure the receive power using an optical power meter.

If the optical power measurement	**Then** go to
is **too low**	step 7
is **too high**	step 8

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

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

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

b. Measure the transmit power at the far end.

c. 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.

d. If the power is below the launch power (minimum), replace the OC-192 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.

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

—continued—

Procedure 5-50 (continued)
OC192 Rx Loss of Signal

Step	Action
	f. If the alarm does not clear, replace the optical interface circuit pack reporting the alarm.
	g. 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.
	h. If the alarm does not clear, contact your next level of support or your Nortel Networks support group.
8	If the power is above the receiver sensitivity for this circuit pack, use an attenuator to reduce the power to the appropriate level.
	a. clean all connections at both ends of the optical fiber link following your company standards and reattach the optical fibers.
	b. if the EOI was shut down, you will have to perform a cold restart on the OC-192 LR or OC-192 DWDM circuit pack on which the alarm was raised. See 323-1059-543, Restarting a circuit pack on page 2-45
9	If the alarm does not clear, replace the optical interface circuit pack.
10	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-51
OC192 Rx RFI

Probable cause

This alarm is raised when the network element detects an OC-192 remote fault indication (RFI) in the SONET overhead because of a fault on another network element, or an optical fiber has been cut.

Impact

Note: Critical, service-affecting (C, SA) alarm for a UPSR with cross-connects
Critical, service-affecting (C, SA) alarm, if active linear or unprotected with cross-connects
Critical, service-affecting (C, SA) if on an active BLSR
Minor, non-service-affecting (m, NSA) alarm, if inactive linear, protected linear, or without cross-connects
Minor, non-service-affecting (m, NSA) for a non-active BLSR

Note: This is a secondary alarm. An alarm of higher severity is raised on the matching optical interface circuit pack on the next network element.

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)

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 optical fiber connection information to identify the network element and the module that is the source of the signal in to the circuit pack reporting the alarm.
3	Log into the remote network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1. ***Note:*** If you cannot log in from the local network element, you can travel to the remote site.
4	Retrieve all alarms from the remote network element. See Retrieving active alarms for a network element on page 2-3.
5	Look for an alarm message for the OC-192 circuit pack that connects to the original shelf.

—continued—

Procedure 5-51 (continued)
OC192 Rx RFI

Step	Action
6	Clear any alarms using the appropriate procedure.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-52
OC192 Rx Section Trace Mismatch

Probable cause

This alarm is raised when the section trace message on the received facility does not match the expected facility section trace message.

> ***Note:*** This alarm is only raised if the section trace failure mode is Alarms on or Alarms on, with traffic protection.

Impact

Major, service-affecting (M, SA) alarm, if in Alarms on mode
Major, service-affecting (M, SA) alarm (UPSR ring with cross-connects), if in Alarms on, with traffic protection mode
Major, service-affecting (M, SA) alarm, if active linear, active BLSR, or unprotected with cross-connects, if in Alarms on, with traffic protection mode
Minor, non-service-affecting (m, NSA) alarm, if inactive linear, inactive BLSR, protected linear, protected BLSR, or without cross-connects, if in Alarms on, with traffic protection mode

> ***Note:*** This alarm has dual severity in Alarms on, with traffic protection mode with 1+1 protection.

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 5-11, 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	Verify that the optical fiber connections are correct on the optical interface circuit pack that is raising the alarm, that is, on the receive network element.
3	If the alarm does not clear, retrieve and take note of the section trace messages of the OC-192 signal at the transmit network element and at the alarmed receive network element. See 323-1059-520, Retrieving section trace messages on page 2-2.

—continued—

Procedure 5-52 (continued)
OC192 Rx Section Trace Mismatch

Step	Action
4	Compare the section trace Format parameter (Number or String) of the transmit signal at the transmit network element with that of the receive signal at the alarmed receive network element. If the values are different, change the Format value of the receive signal at the alarmed receive network element to match the Format value of the transmit signal. See 323-1059-520, Editing section trace messages on page 2-4.
5	Compare the Transmitted section trace value of the transmit signal at the transmit network element with the Expected Rx section trace value of the receive signal at the receive network element. If the values are different, change the Expected Rx section trace value of the receive signal at the alarmed network element to match the Transmitted section trace value of the transmit signal. See 323-1059-520, Editing section trace messages on page 2-4.
6	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-53
OC192 Rx Signal Degrade

Probable cause

This alarm is raised when the received signal is significantly degraded.

One of the following conditions cause this alarm:

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

Impact

Minor, service-affecting (m, SA) alarm for a UPSR with cross-connects
Minor, service-affecting (m, SA) alarm, if active linear or unprotected with cross-connects
Minor, non-service-affecting (m, NSA) alarm, if inactive linear, protected linear, or without cross-connects
Minor, non-service-affecting (m, NSA) alarm for an inactive BLSR
Minor, service-affecting (m, SA) alarm for an active BLSR

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)
- have an optical power meter with the same optical connectors as the network element
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

Step	Action
1	Retrieve alarms from the network element. See Retrieving active alarms for a network element on page 2-3.

—continued—

Procedure 5-53 (continued)
OC192 Rx Signal Degrade

Step	Action
2	Verify if there are alarms of higher order from the alarm hierarchy. Alarm hierarchies on page 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the signal degrade alarm cleared.
4	If the alarm does not clear, identify the circuit pack raising the alarm.
5	Use the optical fiber connection information to identify the network element and the module that is the source of the signal in to the module reporting the alarm. See Retrieving active alarms for a network element on page 2-3.
6	Retrieve all alarms at the transmit end: • Clear any higher order alarms using the appropriate procedures. • If OC-192 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.
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. Use the optical power meter to measure the receive power at the receive end.
9	Measure the receive power using an optical power meter. If the power is below the receiver sensitivity for this circuit pack, perform the following steps for OC192 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.

—continued—

Procedure 5-53 (continued)
OC192 Rx Signal Degrade

Step	Action
	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.If the power is below the launch power (minimum), replace the OC-192 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.
	e. Retrieve all alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
	f. If the alarm does not clear, replace the optical interface circuit pack reporting the alarm.
	g. Clean and reattach both optical fibers. See *Installation*, 323-1059-201.
	h. 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.
10	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.
11	If the alarm does not clear, replace the optical interface circuit pack raising the alarm.
12	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-54
OC192 Rx Signal Failure

Probable cause

This alarm is raised when the received optical signal is degraded to the point where it is unusable.

One of the following conditions causes this alarm:

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

Impact

Critical, service-affecting (C, SA) alarm for a UPSR with cross-connects
Critical, service-affecting (C, SA) alarm, if active linear or unprotected with cross-connects
Critical, service-affecting (C, SA) if on an active BLSR
Minor, non-service-affecting (m, NSA) alarm, if inactive linear, protected linear, or without cross-connects
Minor, non-service-affecting (m, NSA) for a non-active BLSR

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)
- have an optical power meter with the same optical connectors as the network element
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

—continued—

Procedure 5-54 (continued)
OC192 Rx Signal Failure

Step	Action
1	Retrieve all 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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the signal failure alarm cleared. See Retrieving active alarms for a network element on page 2-3.
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 the receive sites of the alarmed signal.
6	Retrieve alarms at the transmit end: • Clear any higher order alarms using the appropriate procedure. • If OC192 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.
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. Use the optical power meter to measure the receive power.

—continued—

Procedure 5-54 (continued)
OC192 Rx Signal Failure

Step	Action
9	Measure the receive power using an optical power meter. If the power is below the receiver sensitivity for this circuit pack, perform the following steps for OC192 Rx signal failure: ***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 OC-192 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. **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.
10	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.
11	If the alarm does not clear, replace the circuit pack reporting the alarm.
12	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-55
Path PM Threshold Exceeded

Probable cause

This alarm is raised when a path PM threshold is exceeded for the specified facility. This alarm is raised at the first occurrence of a path PM threshold crossing in the collection period (1-day or 15-minutes).

This alarm is raised once in the collection period and it clears automatically at the end of the collection period. If the problems causing the threshold crossings are not corrected, then the alarm will be raised against the facility in subsequent collection periods at the first occurrence of a path PM threshold crossing.

This alarm is raised only when the PM threshold crossing report type is set to Alarm. You can disable the reporting of the threshold crossing alert (TCA) summary alarms. See 323-1059-510, Editing the Threshold Crossing Report Type for facilities on page 1-44.

> ***Note:*** The TCA summary alarms are as follows: Section PM Threshold Exceeded, Line PM Threshold Exceeded, and Path PM Threshold Exceeded.

You can also disable thresholding. See 323-1059-510, Editing the threshold status for facilities on page 1-43.

The TCA summary alarms can help you trouble clear and avoid potentially service-affecting problems, indicated by the following alarms:

- signal degrade
- signal fail
- loss of frame
- loss of signal

This alarm can be caused by the following conditions:

- a faulty upstream transmitter circuit pack upstream in the path
- incorrectly provisioned transmitting circuit pack upstream in path
- a circuit pack with the wrong wavelength
- a faulty receive circuit pack
- an optical signal degradation
- a bent optical fiber
- a dirty connector

—continued—

Procedure 5-55 (continued)
Path PM Threshold Exceeded

- a dirty optical fiber
- incorrectly set attenuation
- a DWDM coupler incorrectly configured at the receiving end
- a DWDM coupler damaged at the receiving or transmitting end
- an out-of-service facility upstream in 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
- have an optical power meter with the same optical connectors as the network element
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201

Step	Action
1	Retrieve the PM counts for the facility and determine which thresholds are exceeded. See 323-1059-510, Procedures for facility PM counts on page 1-1 and 323-1059-510, Procedures for facility PM thresholds on page 1-2.
2	Retrieve alarms from the network element. See Retrieving active alarms for a network element on page 2-3.
3	Query the cross-connect details (see 323-1059-320, Retrieving cross-connects on page 6-3) to determine if the alarm has been raised against a deleted cross-connect.
4	**If** the alarm is raised against / **Then** a deleted cross connect — go to step 5 an existing cross connect — go to step 9
5	Add the cross-connect (see 323-1059-320, Adding a cross-connect on page 6-1).
6	It is not necessary to add the exact connection that caused the alarm. You can create a temporary cross-connection to clear the active alarm.Ensure that Alarm is not selected as the Threshold Crossing Report Type. See 323-1059-510, Editing the Threshold Crossing Report Type for facilities on page 1-44.

—continued—

Procedure 5-55 (continued)
Line PM Threshold Exceeded

Step	Action
7	Delete the cross-connect (see 323-1059-320, Deleting a cross-connect on page 6-4).
8	**If** / **Then** the alarm clears — you have completed this procedure the alarm does not clear — go to step step 9
9	If alarms of higher order are active against the facility at the near end and at the far end, clear these other alarms first using the appropriate procedures. **If** errors are at / **Then** near end only — continue with procedure near end and far end — continue with procedure far end only — go to the remote end and continue with the procedure. The far end now becomes the near end
10	Check the PM counts for the facility: **If** PM counts for exceeded thresholds / **Then** have cleared or stopped increasing — you completed this procedure are still increasing — go to step 11
11	Measure the receive power of the near-end receiver circuit pack using an optical power meter. ***Note:*** For information about circuit pack technical specifications, see the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM. **If** the receive power is / **Then** go to below the minimum receive sensitivity — step 12 above the receiver overload — step 22 within the operating range (between the minimum receive sensitivity and the receiver overload) — step 24

Receive power below the minimum receive sensitivity for the circuit pack

12	Wear an antistatic wrist strap to protect the shelf from static damage. At the near-end network element, connect the wrist strap to the ESD jack on the shelf.

—continued—

Procedure 5-55 (continued)
Line PM Threshold Exceeded

Step	Action

13

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.

At the near end, check for bent optical fibers or damaged patch cords. See *Installation*, 323-1059-201.

14 At the near end, clean the optical fiber connector on the circuit pack and the optical fiber, then reattach the optical fiber. See *Installation*, 323-1059-201.

15 Measure the receive power of the near-end receiver circuit pack again:

If the receive power is	**Then** go to
still below the minimum receive sensitivity	step 16
within the operating range (between the minimum receive sensitivity and the receiver overload)	step 18

16 Adjust the attenuation, if equipped, of the near-end receiver circuit pack to try to get the receive power within the operating range of the circuit pack.

17 Measure the receive power of the near-end receiver circuit pack again:

If the receive power is	**Then** go to
within the operating range (between the minimum receive sensitivity and the receiver overload)	step 18
still below the minimum receive sensitivity	step 19

18 Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	step 24

—continued—

Procedure 5-55 (continued)
Path PM Threshold Exceeded

Step	Action
19	If you cannot get the receive power within the operating range, measure the transmit power at the far-end transmitter circuit pack.

If the transmit power is	**Then**
above the end of life transmit power	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 and clear the location of the problem. Then, go to step 21.
below the end of life transmit power	go to step 20

20	Clean the optical fiber connector on the transmitter circuit pack, then measure the transmit power again:

If the transmit power is	**Then**
still below the end of life transmit power	replace the circuit pack at the transmit end, then clean and reattach the optical fibers. See 323-1059-543, Procedures for equipment replacement on page 3-1 and *Installation*, 323-1059-201. Then, go to step 21.
within the operating range of the circuit pack	go to step 21

21	Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	go to step 24

Receive power is above the receiver overload for the circuit pack

22	Adjust the attenuation, if equipped, of the near-end receiver circuit pack to get the receive power within range.
23	Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	go to step 24

—continued—

Procedure 5-55 (continued)
Path PM Threshold Exceeded

Step	Action

Receive power within operating range for the circuit pack

24 Clean all connections at both ends of the optical fiber link, then reattach the optical fibers. See *Installation*, 323-1059-201.

25 Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	step 26

26 Check whether there is a defective circuit pack. Replace the near-end receiver circuit pack, then clean and reattach the optical fibers. See 323-1059-543, Procedures for equipment replacement on page 3-1 and *Installation*, 323-1059-201.

27 Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	go to step 28

28 If you have not already done so, replace the far-end transmitter circuit pack, then clean and reattach the optical fibers. See 323-1059-543, Procedures for equipment replacement on page 3-1 and *Installation*, 323-1059-201.

29 Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	contact your next level of support or your Nortel Networks support group for assistance

—end—

Procedure 5-56
PLL Not Locked to Timing Ref.

Probable cause

This alarm is raised when all of the following conditions occur:

- shelf timing mode is external (EXT) or line-timed (LINE)
- shelf primary timing reference or secondary timing reference is provisioned
- phase-locked loop (PLL) is not locked to a timing reference

  Note: The cause is a loss of all user provisioned timing references, or the degradation of synchronization status messages on these references.

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)

Step	Action
1	Verify the shelf timing mode. See 323-1051-310, Retrieving synchronization data for a network element on page 1-2.
2	Verify the shelf primary and secondary timing references. See 323-1051-310, Retrieving synchronization data for a network element on page 1-2.
3	Retrieve all active and disabled alarms. See Retrieving active alarms for a network element on page 2-3.
4	Clear the Loss of Shelf Pri. Timing Reference and the Loss of Shelf Sec. Timing Reference alarms if they are raised.
5	Wait 2 to 5 minutes to see if the alarm clears.
6	Retrieve all events. See Retrieving events for a network element on page 2-11.
7	If the Shelf Pri Ref Rx Degraded SSM or the Shelf Sec Ref Rx Degraded SSM events are raised, verify the timing sources to find out why the synchronization quality is lower than the network element internal clock quality.

—end—

Procedure 5-57
Power failure - A or Power failure - B

Probable cause

This alarm is raised when the shelf processor detects that low or no voltage exists on the A or B backplane power bus. Although a power source has failed, shelf traffic is not affected.

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 5-11, and in *Installation,* 323-1059-201
- have use a standard multimeter
- have a spare module to replace each module in the shelf

  Note: You do not have to replace each module with a new module. Use a single spare module of the correct type to replace each module in turn.

- use an account with level 1 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	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 shelf.
3	If 48 V dc is not on both of the power inputs, and if the 30 A breaker is good, then the bay power supply is faulty. Use your company procedures to clear the problem.
4	If the breaker tripped, switch the breaker back to reset it.

—continued—

Procedure 5-57 (continued)
Power failure - A or Power failure - B

Step	Action
5	If the breaker pops back after you reset it, then the backplane power bus shorted in a module PUPS (point of use power supply), or one of the backplane pins is bent and shorted. • Remove each power module in the shelf one at a time and examine the backplane connectors for bent pins. • If you find a bent pin, contact your next level of support or your Nortel Networks support group. • After each replacement, try to reset the A feed breaker. See Replacing the power A and power B modules on page 3-77. If the breaker remains set, verify that the alarm cleared.
6	If you have replaced all the power modules and the breaker does not remain set, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-58
Primary RADIUS Server Unavailable

Probable cause

This alarm is raised when all requests to the primary RADIUS server of a network processor time out.

Impact

Major, service-affecting (M, NSA) if a secondary RADIUS server is not provisioned or the secondary RADIUS server is also unavailable
Minor, non-service-affecting (m, NSA) if primary and secondary RADIUS servers are provisioned and only the primary server is unavailable

Requirements

Before you perform this procedure, you must

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

Step	Action
1	Make sure the primary RADIUS server of the network processor is enabled and has a valid IP address. See 323-1059-302, Centralized security administration on page 3-2.
2	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-59
Primary Security Gateway Unavailable

Probable cause

This alarm is raised when the network processor provisioned as the primary security gateway of a shelf processor is not accessible. The shelf processor cannot find a connection to the gateway network processor or the gateway network processor does not respond to an authentication request from the shelf processor.

Impact

Major, service-affecting (M, NSA) if a secondary security gateway is not provisioned or the secondary gateway is also unavailable
Minor, non-service-affecting (m, NSA) if primary and secondary security gateways are provisioned and only the primary gateway is unavailable

Requirements

Before you perform this procedure, you must

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

Step	Action
1	Make sure the network processor is running Release 11.0 or higher. If not, upgrade the network processor or change the primary gateway of the shelf processor to a network processor running Release 11.0 or higher.
2	If present, clear any alarms that point to a loss of communication between the shelf processor and network processor, such as the “SDCC Link Failure”, “ILANSP Failure”, or “OC-n Loss of Signal” alarm.
3	Make sure remote authentication is enabled on the network processor. See 323-1059-302, Centralized security administration on page 3-2.
4	Make sure the RADIUS servers of the network processor are enabled and have valid IP addresses. See 323-1059-302, Centralized security administration on page 3-2.
5	Make sure the network processor is on the routing table of the shelf processor. If not, add the required section data communications channel (SDCC) connection or change the primary gateway of the shelf processor to a network processor that appears on its routing table.
6	Make sure the shelf processor is in the network processor span of control. If not, add the shelf processor to the network processor span of control. See 323-1059-520, Procedures for span of control on page 4-1.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-60
Protection Exerciser Failed

Probable cause

This alarm is raised when the high-speed exerciser has failed to complete the exercise routine on the selected equipment or facilities.

This alarm is caused by one of the following conditions:

- faulty circuit pack
- exerciser is running somewhere else in the bidirectional line-switched ring (BLSR)
- active protection switch

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	Ensure that there is no active protection switch on the BLSR. See 323-1059-311, Retrieving protection status details on page 1-15.

If protection switches on the BLSR are	**Then** go to
idle	step 2
not idle	step 6

2	Verify if any exerciser is scheduled to run on another network element in the BLSR at approximately the same time. See 323-1059-311, Retrieving the exerciser schedule on page 1-43.
3	If the exerciser is running on another network element in the BLSR, inhibit the exerciser. See 323-1059-311, Inhibiting the exerciser to run as scheduled on page 1-48.
4	Initiate the exerciser on the selected equipment. See 323-1059-311, Running the exerciser manually on page 1-44.
5	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 5-60 (continued)
Protection Exerciser Failed

Step	Action
6	Clear the following alarms, if active, using the appropriate procedures: • OC48 Rx Line AIS on page 5-91 • OC48 Rx Loss of Frame on page 5-93 • OC48 Rx Loss of Signal on page 5-96 • OC48 Rx Section Trace Mismatch on page 5-101 • OC48 Rx Signal Degrade on page 5-103 • OC48 Rx Signal Failure on page 5-106 • OC192 Rx Line AIS on page 5-109 • OC192 Rx Loss of Frame on page 5-111 • OC192 Rx Loss of Signal on page 5-114 • OC192 Rx Section Trace Mismatch on page 5-120 • OC192 Rx Signal Degrade on page 5-122 • OC192 Rx Signal Failure on page 5-125
7	Release all user-initiated protection switches. See 323-1059-311, Releasing an optical line switch on page 1-30.
8	If the wait to restore is active, you will see the Wait to restore event active in the BLSR. Wait for the event it to clear.
9	Initiate the exerciser on the selected equipment. See 323-1059-311, Running the exerciser manually on page 1-44.
10	If the alarm does not clear, repeat step 2 through step 5.

—end—

Procedure 5-61
Protection Mode Mismatch

Probable cause

This alarm is raised when the received channel protection switching control bytes (K1/K2) on the protection optical interface circuit pack show a different protection switch mode than is provisioned on the local network element. When switching protection mode from 1+1 unidirectional to 1+1 bidirectional, or from 1+1 bidirectional to 1+1 unidirectional, the Protection mode mismatch alarm will be raised against the node that was changed to, or remained as, bidirectional 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 3 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	Retrieve the switch mode of the optical interface pair. See 323-1059-311, Retrieving protection scheme and protection switch mode for a pair of optical facilities on page 1-3.
3	Determine the network element and optical interface modules that are on the remote end of the link.
4	Log into the remote terminal.
5	Retrieve the switch mode of the optical interface pair on the remote terminal. See 323-1059-311, Retrieving protection scheme and protection switch mode for a pair of optical facilities on page 1-3.

—continued—

Procedure 5-61 (continued)
Protection Mode Mismatch

Step	Action
6	Compare the switch modes reported with each other and with the company records. • If both of the optic pairs report the same switch mode, contact your next level of support or your Nortel Networks support group. • If the two switch modes are different, determine from the company records which is correct and change the switch mode of the other optical interface pair. See 323-1059-311, Changing the linear protection switch mode for a pair of optical facilities on page 1-4. ***Note:*** Changing the protection switch mode for one of the optical interface circuit packs in a pair will automatically change the protection switch mode for the other circuit pack in the pair. **—end—**

Procedure 5-62
Protection Scheme Mismatch

Probable cause

This alarm is raised when the protection scheme on the network element from another vendor does not match the 1+1 protection scheme of the network element.

Impact

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

Step	Action
1	Contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-63
Protection Switch Fail

Probable cause

This alarm is raised when the system attempts to switch traffic from the working to the protection channels and fails.

This alarm is raised when one of the following conditions occurs on either the local or remote network element:

- faulty circuit pack
- degraded signal
- higher priority switch status exists
- incorrect BLSR provisioning

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	Verify the BLSR provisioning. See 323-1059-320, Provisioning a BLSR configuration on page 6-34.
2	If you updated the BLSR provisioning: • operate a lockout of protection on the circuit pack that raised the alarm, see 323-1059-311, Operating a lockout of protection in a BLSR on page 1-35 and • release the lockout of protection, see 323-1059-311, Releasing an optical line switch on page 1-30
3	If the alarm does not clear, ensure the lockout of working is active at both ends of the span. See 323-1059-311, Retrieving protection status details on page 1-15. If the lockout of working is not active at both ends of the span, operate a lockout of working. See 323-1059-311, Operating a lockout of working in a BLSR on page 1-33.
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-64
Remote Alarm(s)

Probable cause

This alarm is raised in the following situations:

- if any alarm condition exists on the network processor
- when the communication channel between the shelf processor and network processor is down

Impact

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

Note: If this condition exists and the failure is longer than 10 minutes, the network processor Circuit Pack Failed alarm is raised and the Remote Alarm(s) alarm clears.

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)

Step	Action
1	Log into the network processor. See 323-1059-302, Procedures for logging in to a network processor on page 2-1. ***Note 1:*** If a network processor restart occurred, you cannot access the network processor until the network processor database is released. ***Note 2:*** If you log in to an network processor using an account with a level 5 UPC, you automatically log into all the network elements in the network processor span of control.
2	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 5-64 (continued)
Remote Alarm(s)

Step	Action	
3	**If**	**Then**
	you cannot log in to the network processor	continue to try to log in for up to 10 minutes, or until the Circuit pack failed alarm is raised against the network processor. If this alarm is raised, see Circuit Pack Failed (network processor) on page 4-61.
	the Circuit pack failed alarm is not raised and you cannot log in	replace the network processor. See Replacing the network processor on page 3-10.
	you logged into the network processor without a problem	retrieve all alarms and continue to the next step. See Retrieving active alarms for a network element on page 2-3.
4	Clear all the alarm raised on the network processor.	
5	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.	

—end—

Procedure 5-65
Remote Fail

Probable cause

This alarm is raised on the network processor if any of the following conditions exist:

- 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
- there is no receive link activity 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 1: This alarm should clear on its own when the condition clears or when the affected facility is deprovisioned.

Note 2: 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
- use an account with level 3 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 5-11, 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 failed facility. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.

If the failed facility is	**Then** go to
X.25-related	step 3
ILAN1, ILAN2, or COLAN	step 4
ILANNP	step 5
ILANSP	step 6

—continued—

Procedure 5-65 (continued)
Remote Fail

Step	Action
3	If the failed facility is X.25-related, perform the following: **a.** If the alarm is a result of provisioning the X.25 facility, deprovision the X.25 facility and then reprovision it. See 323-1059-520, Editing X.25 parameters on page 3-6. **b.** If the alarm is a result of provisioning the X.25 or virtual circuit parameters, reprovision the X.25 or virtual circuit parameters. See 323-1059-520, Editing X.25 parameters on page 3-6, Editing the SVC parameter values on page 3-14, and Editing the PVC parameter values on page 3-12. **c.** If the alarm does not clear, verify that the X.25 cable and far-end equipment are working. **d.** If the alarm does not clear, contact your next level of support or your Nortel Networks support group. You have completed this procedure.
4	If the failed facility is ILAN1, ILAN2, or COLAN, perform the following: **a.** Verify that the Ethernet cable and the far-end equipment are working. If there are no problems, replace the network processor circuit pack. See Replacing the network processor on page 3-10. **b.** If the alarm does not clear, contact your next level of support or your Nortel Networks support group.
5	If the failed facility is ILANNP, replace the network processor circuit pack. See Replacing the network processor on page 3-10. You have completed this procedure.

—continued—

Procedure 5-65 (continued)
Remote Fail

Step	Action
6	If the failed facility is ILANSP, perform the following: **a.** Verify if the shelf processor is restarting. If so, the alarm clears automatically. **b.** If the alarm does not clear, verify that the network processor and the co-located shelf processor share at least one MANAREA address by trying to log in to the co-located shelf processor. See 323-1059-520, Retrieving the manual area addresses of the network processor on page 3-16 and Adding or editing a manual area address on page 3-17. — If the login is successful, retrieve all alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3. — If the login fails, or if the alarm does not clear replace the network processor circuit pack. See Replacing the network processor on page 3-10. **c.** Retrieve all alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3. **d.** If the alarm does not clear, replace the shelf processor circuit pack. See Replacing the shelf processor on page 3-7. **e.** If the alarm does not clear, contact your next level of support or your Nortel Networks support group. **—end—**

Procedure 5-66
Rollover in Progress

Probable cause

This alarm is raised when there is an inservice traffic rollover in progress.

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 5-11, and in *Installation,* 323-1059-201

Step	Action
1	Retrieve all active and disabled alarms. See Retrieving active alarms for a network element on page 2-3.
2	Retrieve the rollovers in progress. See 323-1059-320, Selecting Show in-service traffic rollover on page 6-51.
3	Clear this alarm by backing out of the rollover, or by completing the rollover. **If** you want to — **Then** go to back out of the rollover in progress — step 4 complete the rollover in progress — step 6
4	If the rollover is in the switched state, back out to the bridged state by clicking Backout. The state changes from switched to bridged.
5	If the rollover is in the bridged state, back out to the idle state by clicking Backout. The state changes from bridged to idle. You have completed this procedure.
6	If the rollover is in the bridged state, roll the connection to the switched state by clicking Switch. The state changes from bridged to switched.
7	If the rollover is in the switched state, click Commit to complete the rollover.

—end—

Procedure 5-67
Rx Excessive Error Ratio

Probable cause

This alarm is raised against an Ethernet, Fibre Channel, or WAN facility of a 2xGigE/FC-P2P circuit pack.

This alarm is raised against an Ethernet or Fibre Channel facility when one of the following conditions occurs:

- For Ethernet facilities, this alarm is raised when at least 20 percent of the received frames are errored per second, for 3 consecutive seconds.
- For Fibre Channel facilities, this alarm is raised when at least 20 percent of the received 8B/10B codes are errored (including symbol or disparity errors) per second, for 3 consecutive seconds.

This alarm is raised against a WAN facility when one of the following conditions occurs:

- For GFP-F or POS encapsulation, this alarm is raised when at least 20 percent of the received frames are errored per second, for 3 consecutive seconds.
- For GFP-T encapsulation, this alarm is raised when at least 20 percent of the received superblocks are errored per second, for 3 consecutive seconds.

This alarm clears when these defects do not occur for 10 consecutive seconds.

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
- have an optical power meter with the same optical connectors as the network element
- if required, obtain a supported SFP optical transceiver module
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201

—continued—

Procedure 5-67 (continued)
Rx Excessive Error Ratio

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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the alarm cleared. If the alarm cleared, you have completed this procedure. Otherwise, go to the next step.
4	From the Class field in the Active Alarms window, determine if the alarm is raised against the Ethernet, Fibre Channel, or WAN facility.

5

If this alarm is raised against the	**Then**
Ethernet or Fibre Channel facility	go to step 6
WAN facility	go to step 20

Alarm raised against the Ethernet or Fibre Channel facility

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

CAUTION
Risk of traffic loss
Ensure that the correct module is identified. Removing the wrong optical fiber causes a traffic loss on an in-service facility.

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

Use the optical power meter to measure the receive power at the LAN port.

Note: For information about technical specifications (minimum and maximum receive optical power) for the SFPs supported with the 2xGigE/FC-P2P circuit pack, see the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM.

8

If the receive power at the LAN port is	**Then** go to
below the minimum receive optical power	step 9
between the minimum and maximum receive optical power	step 13
above the maximum receive optical power	step 14

—continued—

Procedure 5-67 (continued)
Rx Excessive Error Ratio

Step	Action

Receive power is below the minimum receive optical power

9 Decrease the local attenuation, if equipped, to try to increase the receive power to a value above the minimum receive optical power (but below the maximum receive optical power).

10

If the adjusted receive power is	**Then** go to
still below the minimum receive optical power	step 11
within range (between the minimum and the maximum receive optical power)	step 13

11 Remove the Tx optical fiber from the far-end subtending client equipment.

12 Measure the transmit power at the far-end subtending client equipment.

- If the transmit power of the far-end equipment is above the minimum launch power, the optical fiber attenuation is too high, the optical fiber connections are dirty, or the optical fiber is damaged.
- If the transmit power of the far-end equipment is below the minimum launch power, there is a problem with the far-end equipment.

Use your company procedure to determine and clear the problem. Then, go to step 15.

Receive power is between the minimum and the maximum receive optical power

13 Clean all connections at both ends of the optical fiber link following your company standards and reattach the optical fibers.

Go to step 15.

Receive power is above the maximum receive optical power

14 Add the necessary attenuation to try to reduce the receive power to a value below the maximum receive optical power (but above the minimum receive optical power).

Determining if the alarm cleared

15 Retrieve all alarms 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, replace the SFP that corresponds to the facility raising the alarm. See Replacing a Small Form Factor Pluggable (SFP) optical transceiver module on page 3-21.

17 If the alarm does not clear, replace the 2xGigE/FC-P2P circuit pack reporting the alarm. See Replacing a 2xGigE/FC-P2P circuit pack on page 3-18.

18 Clean and reattach the optical fibers. See *Installation*, 323-1059-201.

19 If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—continued—

Procedure 5-67 (continued)
Rx Excessive Error Ratio

Step	Action

Alarm raised against the WAN facility

20 Retrieve the performance monitoring counts for the STS paths connected to the WAN facility to determine if the ES-P counts are increasing.

21 If the ES-P counts are increasing, use the appropriate alarm clearing procedure to clear any STS path alarms on the optical interface circuit pack that connects to the 2xGigE/FC-P2P circuit pack. The STS path alarms include STS Rx Signal Degrade, STS Rx Excessive BIP Error Rate, STS Rx Loss of Alignment, STS Rx Loss of Multiframe, and STS Rx Loss of Sequence alarms.

22 If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-68
Rx Loss of Data Synch

Probable cause

This alarm is raised against an Ethernet or Fibre Channel facility of a 2xGigE/FC-P2P circuit pack when one of the following conditions occurs:

- the circuit pack cannot establish bit synchronization or transmission word synchronization
- the incorrect type of Small Form Factor Pluggable (SFP) optical transceiver module (SX or LX) is installed
- the client service on the subtending equipment does not match the client service provisioned on the corresponding port of the 2xGigE/FC-P2P circuit pack (for example, a Fibre Channel signal is connected to a 2xGigE/FC-P2P circuit pack port that is provisioned for Ethernet)

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 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 5-11, and in *Installation,* 323-1059-201
- if required, obtain a replacement SFP
- use an account with level 3 or higher user privilege code (UPC)

—continued—

Procedure 5-68 (continued)
Rx Loss of Data Synch

Step	Action
1	Determine the facility (Ethernet or Fibre Channel) provisioned on the port of the 2xGigE/FC-P2P circuit pack reporting the alarm: • 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 the 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). ***Note:*** To view the details of any provisioned facilities, select the facility from the Facility Type drop-down list.
2	**If** the subtending equipment — **Then** go to is not provisioned with the same service (Ethernet or Fibre Channel) you noted in step 1 — step 3 is provisioned with the same service (Ethernet or Fibre Channel) you noted in step 1 — step 6
3	Ensure that the correct optical fiber is connected to the corresponding port on the 2xGigE/FC-P2P circuit pack. (The fibers connected to the LAN ports on the 2xGigE/FC-P2P circuit pack might be reversed.)
4	If the incorrect facility (ETH or FC) is provisioned, 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. • Add the required cross-connect. See 323-1059-320, Adding a cross-connect on page 6-1.
5	Retrieve all alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
6	If the alarm does not clear, ensure that the Small Form Factor Pluggable (SFP) optical transceiver module is the correct type. Use an SX SFP for multi-mode fiber-optic cables or an LX SFP for single-mode fiber-optic cables. If required, replace the SFP optical transceiver module. See Replacing a Small Form Factor Pluggable (SFP) optical transceiver module on page 3-21.
7	When connected to a pair of fibre channel devices that support the autonegotiation (AN) of 1G and 2G link speeds, the speed of the ports connected to the 2xGE/FC card must be manually set to 1G (FC-100).

—continued—

Procedure 5-68 (continued)
Rx Loss of Data Synch

Step	Action
8	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-69
Rx Loss of Frame Delineation

Probable cause

This alarm is raised against the WAN facility of a 2xGigE/FC-P2P circuit pack when the GFP layer cannot detect valid GFP frames.

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	Retrieve alarms from the network element. See Retrieving active alarms for a network element on page 2-3.
2	Use the appropriate alarm clearing procedure to clear any STS path alarms on the optical interface circuit pack that connects to the 2xGigE/FC-P2P circuit pack. The STS path alarms include STS Rx Signal Degrade, STS Rx Excessive BIP Error Rate, STS Rx Loss of Alignment, STS Rx Loss of Multiframe, and STS Rx Loss of Sequence.
3	Trace the cross-connect information to ensure that the same number of STS-1 or STS-3c cross-connects are provisioned on the 2xGigE/FC-P2P circuit packs on both sides of the connection. See 323-1059-320, Procedures for nodal cross-connect management on page 6-1.
4	Ensure that the subtending client equipment is transmitting a valid GFP-F (for Gigabit Ethernet) or GFP-T (for Fibre Channel) signal, as required.
5	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-70
Rx Loss of Signal

Probable cause

This alarm is raised against an Ethernet or Fibre Channel facility of a 2xGigE/FC-P2P circuit pack when the circuit pack cannot detect an input signal on the LAN-side facility.

This alarm is caused by one of the following conditions:

- optical fiber cut
- dirty optical fibers
- dirty connectors
- excessive attenuation

Note: When this alarm is raised, the Link Down alarm is also raised.

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 5-11, and in *Installation,* 323-1059-201
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element
- if required, obtain a supported SFP optical transceiver module
- use an account with level 1 or higher user privilege code (UPC)

—continued—

Procedure 5-70 (continued)
Rx Loss of Signal

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

CAUTION
Risk of traffic loss
Ensure that the correct module is identified. Removing the wrong optical fiber causes a traffic loss on an in-service facility.

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

Use the optical power meter to measure the receive power at the LAN port.

Note: For information about technical specifications (minimum and maximum receive optical power) for the SFPs supported with the 2xGigE/FC-P2P circuit pack, see the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM.

3

If the receive power at the LAN port is	**Then** go to
below the minimum receive optical power	step 4
between the minimum and maximum receive optical power	step 8
above the maximum receive optical power	step 9

Receive power is below the minimum receive optical power

4 Decrease the local attenuation, if equipped, to try to increase the receive power to a value above the minimum receive optical power (but below the maximum receive optical power).

5

If the adjusted receive power is	**Then** go to
still below the minimum receive optical power	step 6
within range (between the minimum and the maximum receive optical power)	step 8

6 Remove the Tx optical fiber from the far-end subtending client equipment.

—continued—

Procedure 5-70 (continued)
Rx Loss of Signal

Step	Action
7	Measure the transmit power at the far-end subtending client equipment. • If the transmit power of the far-end equipment is above the minimum launch power, the optical fiber attenuation is too high, the optical fiber connections are dirty, or the optical fiber is damaged. • If the transmit power of the far-end equipment is below the minimum launch power, there is a problem with the far-end equipment. Use your company procedure to determine and clear the problem. Then, go to step 10.
Receive power is between the minimum and the maximum receive optical power	
8	Clean all connections at both ends of the optical fiber link following your company standards and reattach the optical fibers. Go to step 10.
Receive power is above the maximum receive optical power	
9	Add the necessary attenuation to try to reduce the receive power to a value below the maximum receive optical power (but above the minimum receive optical power).
Determining if the alarm cleared	
10	Retrieve all alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
11	If the alarm does not clear, replace the SFP that corresponds to the facility raising the alarm. See Replacing a Small Form Factor Pluggable (SFP) optical transceiver module on page 3-21.
12	If the alarm does not clear, replace the 2xGigE/FC-P2P circuit pack reporting the alarm. See Replacing a 2xGigE/FC-P2P circuit pack on page 3-18.
13	Clean and reattach the optical fibers. See *Installation*, 323-1059-201.
14	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-71
Rx Signal Degrade

Probable cause

This alarm is raised against an Ethernet, Fibre Channel, or WAN facility of a 2xGigE/FC-P2P circuit pack when the received signal is severely degraded.

This alarm is raised against the Ethernet or Fibre Channel facility when the following occurs:

- For Ethernet facilities, this alarm is raised when at least 1 percent of the received frames are errored per second, for 3 consecutive seconds.
- For Fibre Channel facilities, this alarm is raised when at least one symbol or disparity error occurs per second, for 3 consecutive seconds.

This alarm is raised against the WAN facility when the following occurs:

- For GFP-F or POS encapsulation, this alarm is raised when at least 1 percent of the received frames are errored per second, for 3 consecutive seconds.
- For GFP-T encapsulation, this alarm is raised when at least 1 percent of the received superblocks are errored per second, for 3 consecutive seconds.

This alarm clears when these defects do not occur for 10 consecutive seconds.

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
- have an optical power meter with the same optical connectors as the network element
- if required, obtain a supported SFP optical transceiver module
- observe all safety requirements described in Safety requirements on page 5-11, 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.

—continued—

Procedure 5-71 (continued)
Rx Signal Degrade

Step	Action
2	Verify if there are alarms of higher order from the alarm hierarchy. See Alarm hierarchies on page 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the alarm cleared. If the alarm cleared, you have completed this procedure. Otherwise, go to the next step.
4	From the Class field in the Active Alarms window, determine if the alarm is raised against the Ethernet, Fibre Channel, or WAN facility.

5

If this alarm is raised against the	**Then** go to
Ethernet or Fibre Channel facility	step 6
WAN facility	step 20

Alarm raised against the Ethernet or Fibre Channel facility

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

CAUTION
Risk of traffic loss
Ensure that the correct module is identified. Removing the wrong optical fiber causes a traffic loss on an in-service facility.

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

Use the optical power meter to measure the receive power at the LAN port.

Note: For information about technical specifications (minimum and maximum receive optical power) for the SFPs supported with the 2xGigE/FC-P2P circuit pack, see the *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM.

8

If the receive power at the LAN port is	**Then** go to
below the minimum receive optical power	step 9
between the minimum and maximum receive optical power	step 13
above the maximum receive optical power	step 14

—continued—

Procedure 5-71 (continued)
Rx Signal Degrade

Step	Action

Receive power is below the minimum receive optical power

9 Decrease the local attenuation, if equipped, to try to increase the receive power to a value above the minimum receive optical power (but below the maximum receive optical power).

10

If the adjusted receive power is	**Then** go to
still below the minimum receive optical power	step 11
within range (between the minimum and the maximum receive optical power)	step 13

11 Remove the Tx optical fiber from the far-end subtending client equipment.

12 Measure the transmit power at the far-end subtending client equipment.

- If the transmit power of the far-end equipment is above the minimum launch power, the optical fiber attenuation is too high, the optical fiber connections are dirty, or the optical fiber is damaged.
- If the transmit power of the far-end equipment is below the minimum launch power, there is a problem with the far-end equipment.

Use your company procedure to determine and clear the problem. Then, go to step 15.

Receive power is between the minimum and the maximum receive optical power

13 Clean all connections at both ends of the optical fiber link following your company standards and reattach the optical fibers.

Go to step 15.

Receive power is above the maximum receive optical power

14 Add the necessary attenuation to try to reduce the receive power to a value below the maximum receive optical power (but above the minimum receive optical power).

Determining if the alarm cleared

15 Retrieve all alarms 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, replace the SFP that corresponds to the facility raising the alarm. See Replacing a Small Form Factor Pluggable (SFP) optical transceiver module on page 3-21.

17 If the alarm does not clear, replace the 2xGigE/FC-P2P circuit pack reporting the alarm. See Replacing a 2xGigE/FC-P2P circuit pack on page 3-18.

18 Clean and reattach the optical fibers. See *Installation*, 323-1059-201.

19 If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—continued—

Procedure 5-71 (continued)
Rx Signal Degrade

Step	Action

Alarm raised against the WAN facility

20 Retrieve the performance monitoring counts for the STS paths connected to the WAN facility to determine if the ES-P counts are increasing.

21 If the ES-P counts are increasing, use the appropriate alarm clearing procedure to clear any STS path alarms on the optical interface circuit pack that connects to the 2xGigE/FC-P2P circuit pack. The STS path alarms include STS signal degrade, excessive BIP error rate, loss of alignment, loss of multiframe, and loss of sequence alarms.

22 If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-72
SDCC Link Failure

Probable cause

This alarm is raised when one of the following conditions occurs:

- The shelf processor cannot communicate with the devices at the far end of a SONET link through the SONET data communications channel (SDCC) (Bytes D1-D3 of the section overhead).

  Note: Overhead communications across a SONET link are down. Remote login sessions may be dropped. This condition does not affect traffic.

- The protection and working optical fibers on a 1+1 protected optical interface link are reversed (working optical interface on network element 1 to protection optical interface on network element 2).
- SDCC has not been enabled at the far-end network element.
- fibre-optic cables or coax cables may be disconnected
- SDCC may be provisioned on an EC-1x12 circuit pack

Impact

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

Note: An SDCC link failure may disrupt the map topology feature on the network processor.

Requirements

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- have the network fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- clear all remote alarms present against the optical fiber
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201
- use an account with level 3 or higher user privilege code (UPC)

Step	Action
1	Identify the facility raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Use the network fiber connection information to identify the network element and the module that is the source of the signal into the module reporting the alarm.

—continued—

Procedure 5-72 (continued)
SDCC Link Failure

Step	Action
3	Wait 5 minutes for the alarm to clear in case a shelf processor restart at the remote terminal caused the alarm.Verify the optical fibers on the network element (this applies to a 1+1 protected optical interface): • the odd slot transmit must connect to the odd slot receive on the far end network element • the even slot transmit must connect to the even slot receive on the far end network element • reconnect any fault connections
4	Retrieve all active and disabled alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
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, log in to the remote network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1. • If the login is successful, go to the next step. • If the login fails, replace the shelf processor at the remote site. See Replacing the shelf processor on page 3-7. Wait 5 minutes for the processor to boot, then log in.
7	Verify that both network elements have the same protection scheme. See 323-1059-311, Retrieving protection status details on page 1-15. **a.** If FFP is provisioned for both network elements and the alarm continues, return to the main procedure. **b.** If FFP is enabled only at one of the two network elements, one of the network elements is not correctly configured. Verify from your company record and repair the incorrectly provisioned protection scheme. **c.** Retrieve all active and disabled alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3. **d.** If the alarm does not clear, go to step 8.

—continued—

Procedure 5-72 (continued)
SDCC Link Failure

Step	Action
8	If the alarm does not clear, verify that all lower layer SDCC parameters provisioned at both network elements match. See 323-1059-350, Retrieving equipment and facility details on page 2-2. **a.** If the alarm does not clear, retrieve lower layer SDCC at the network element that originally reported the alarm. **b.** Record settings of all lower layer SDCC parameters. **c.** Retrieve lower layer SDCC at the remote network element: **d.** Record settings of all lower layer SDCC parameters. **e.** Compare all lower layer SDCC parameter settings. Ensure all parameters provisioned at both network elements match. Repair any incorrectly provisioned parameters. See 323-1059-350, Editing the lower layer SDCC on page 2-40. **f.** Retrieve all active and disabled alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
9	If the alarm does not clear, reseat the shelf processor. Wait 5 minutes for it to restart. See Reseating a circuit pack on page 3-4.
10	Retrieve all active and disabled alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
11	If the alarm does not clear, replace the shelf processor at the site that originally reported the alarm. See Replacing the shelf processor on page 3-7.
12	Wait 5 minutes for the shelf processor to restart.Retrieve all active and disabled alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
13	If the alarm does not clear, replace the shelf processor at the remote site you determined in step 2. See Replacing the shelf processor on page 3-7.
14	Wait 5 minutes for the shelf processor to restart.
15	Retrieve all active and disabled alarms 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, replace the required circuit pack at the remote site determined in step 2. 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.
17	Retrieve all active and disabled alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.

—continued—

Procedure 5-72 (continued)
SDCC Link Failure

Step	Action
18	If the alarm does not clear, replace the required circuit pack at the network element originally reporting 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.
19	Retrieve all active and disabled alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
20	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-73
Secondary RADIUS Server Unavailable

Probable cause

This alarm is raised when all requests to the secondary RADIUS server of a network processor time out.

Impact

Major, service-affecting (M, NSA) if a primary RADIUS server is not provisioned or the primary RADIUS server is also unavailable
Minor, non-service-affecting (m, NSA) if primary and secondary RADIUS servers are provisioned and only the secondary server is unavailable

Requirements

Before you perform this procedure, you must

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

Step	Action
1	Make sure the secondary RADIUS server of the network processor is enabled and has a valid IP address. See 323-1059-302, Centralized security administration on page 3-2.
2	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-74
Secondary Security Gateway Unavailable

Probable cause

This alarm is raised when the network processor provisioned as the secondary security gateway of a shelf processor is not accessible. The shelf processor cannot find a connection to the gateway network processor or the gateway network processor does not respond to an authentication request from the shelf processor.

Impact

Major, service-affecting (M, NSA) if a primary security gateway is not provisioned or the primary gateway is also unavailable
Minor, non-service-affecting (m, NSA) if primary and secondary security gateways are provisioned and only the secondary gateway is unavailable

Requirements

Before you perform this procedure, you must

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

Step	Action
1	Make sure the network processor is running Release 11.0 or higher. If not, upgrade the network processor or change the secondary gateway of the shelf processor to a network processor running Release 11.0 or higher.
2	If present, clear any alarms that point to a loss of communication between the shelf processor and network processor, such as the “SDCC Link Failure”, “ILANSP Failure”, or “OC-n Loss of Signal” alarm.
3	Make sure remote authentication is enabled on the network processor. See 323-1059-302, Centralized security administration on page 3-2.
4	Make sure the RADIUS servers of the network processor are enabled and have valid IP addresses. See 323-1059-302, Centralized security administration on page 3-2.
5	Make sure the network processor is on the routing table of the shelf processor. If not, add the required section data communications channel (SDCC) connection or change the secondary gateway of the shelf processor to a network processor that appears on its routing table.
6	Make sure the shelf processor is in the network processor span of control. If not, add the shelf processor to the network processor span of control. See 323-1059-520, Procedures for span of control on page 4-1.
7	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-75
Section PM Threshold Exceeded

Probable cause

This alarm is raised when a section PM threshold is exceeded for the specified facility. This alarm is raised at the first occurrence of a section PM threshold crossing in the collection period (1-day or 15-minutes).

This alarm is raised once in the collection period and it clears automatically at the end of the collection period. If the problems causing the threshold crossings are not corrected, then the alarm will be raised against the facility in subsequent collection periods at the first occurrence of a section PM threshold crossing.

This alarm is raised only when the PM threshold crossing report type is set to Alarm. You can disable the reporting of the threshold crossing alert (TCA) summary alarms. See 323-1059-510, Editing the Threshold Crossing Report Type for facilities on page 1-44.

> ***Note:*** The TCA summary alarms are as follows: Section PM Threshold Exceeded, Line PM Threshold Exceeded, and Path PM Threshold Exceeded.

You can also disable thresholding. See 323-1059-510, Editing the threshold status for facilities on page 1-43.

The TCA summary alarms can help you trouble clear and avoid potentially service-affecting problems, indicated by the following alarms:

- signal degrade
- signal fail
- loss of frame
- loss of signal

This alarm can be caused by the following conditions:

- a faulty upstream transmitter circuit pack
- incorrectly provisioned transmitting circuit pack
- a circuit pack with the wrong wavelength
- a faulty receive circuit pack
- an optical signal degradation

—continued—

Procedure 5-75 (continued)
Section PM Threshold Exceeded

- a bent optical fiber
- a dirty connector
- a dirty optical fiber
- incorrectly set attenuation
- a DWDM coupler incorrectly configured at the receiving end
- a DWDM coupler damaged at the receiving or transmitting end

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 optical power meter with the same optical connectors as the network element
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201

Step	Action
1	Retrieve the PM counts for the facility and determine which thresholds are exceeded. See 323-1059-510, Procedures for facility PM counts on page 1-1 and 323-1059-510, Procedures for facility PM thresholds on page 1-2.
2	Retrieve alarms from the network element. See Retrieving active alarms for a network element on page 2-3.
3	Query the facility details (see 323-1059-350, Retrieving equipment and facility details on page 2-2) to determine if the alarm has been raised against a deleted facility.
4	**If** the alarm is raised against / **Then** a deleted facility — go to step 5 an existing facility — go to step 9
5	Add the facility (see 323-1059-350, Adding a facility on page 2-20). ***Note:*** It is not necessary to add the exact connection that caused the alarm. You can create a temporary connection to the facility (or facilities) with the active alarm.
6	Ensure that Alarm is not selected as the Threshold Crossing Report Type. See 323-1059-510, Editing the Threshold Crossing Report Type for facilities on page 1-44.

—continued—

Procedure 5-75 (continued)
Section PM Threshold Exceeded

Step	Action
7	Delete the facility (see 323-1059-350, Deleting a facility on page 2-22).
8	**If** / **Then** the alarm clears — you have completed this procedure the alarm does not clear — go to step step 9
9	If alarms of higher order are active against the facility at the near end, clear these other alarms first using the appropriate procedures.
10	Check the PM counts for the facility: **If** PM counts for exceeded thresholds — **Then** have cleared or stopped increasing — you completed this procedure are still increasing — go to step 11
11	Select your next step: **If** — **Then** only section PM counts are increasing — the near-end receiver circuit pack or the far-end transmitter circuit pack is faulty. Go to step 12 both section and line PM counts are increasing — go to step 16

Section PM counts are increasing

12	Replace the near-end receiver circuit pack, then clean and reattach the optical fibers. See 323-1059-543, Procedures for equipment replacement on page 3-1 and *Installation*, 323-1059-201.
13	Check the PM counts for the facility: **If** PM counts for exceeded thresholds — **Then** have cleared or stopped increasing — you completed this procedure are still increasing — go to step 14
14	Replace the far-end transmitter circuit pack, then clean and reattach the optical fibers. See 323-1059-543, Procedures for equipment replacement on page 3-1 and *Installation*, 323-1059-201.
15	Check the PM counts for the facility: **If** PM counts for exceeded thresholds — **Then** have cleared or stopped increasing — you completed this procedure are still increasing — contact your next level of support or your Nortel Networks support group for assistance

—continued—

Procedure 5-75 (continued)
Section PM Threshold Exceeded

Step	Action

Section and line PM counts are increasing

16 Measure the receive power of the near-end receiver circuit pack using an optical power meter.

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

If the receive power is	**Then** go to
below the minimum receive sensitivity	step 17
above the receiver overload	step 27
within the operating range (between the minimum receive sensitivity and the receiver overload)	step 29

Receive power below the minimum receive sensitivity for the circuit pack

17 Wear an antistatic wrist strap to protect the shelf from static damage. At the near-end network element, connect the wrist strap to the ESD jack on the shelf.

18

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.

At the near end, check for bent optical fibers or damaged patch cords. See *Installation*, 323-1059-201.

19 At the near end, clean the optical fiber connector on the circuit pack and the optical fiber, then reattach the optical fiber. See *Installation*, 323-1059-201.

—continued—

Procedure 5-75 (continued)
Section PM Threshold Exceeded

Step	Action
20	Measure the receive power of the near-end receiver circuit pack again:

If the receive power is	**Then** go to
still below the minimum receive sensitivity	step 21
within the operating range (between the minimum receive sensitivity and the receiver overload)	step 23

21	Adjust the attenuation, if equipped, of the near-end receiver circuit pack to try to get the receive power within the operating range of the circuit pack.
22	Measure the receive power of the near-end receiver circuit pack again:

If the receive power is	**Then** go to
within the operating range (between the minimum receive sensitivity and the receiver overload)	step 23
still below the minimum receive sensitivity	step 24

23	Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	step 29

24	If you cannot get the receive power within the operating range, measure the transmit power at the far-end transmitter circuit pack.

If the transmit power is	**Then**
above the end of life transmit power	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 and clear the location of the problem. Then, go to step 26.
below the end of life transmit power	go to step 25

—continued—

Procedure 5-75 (continued)
Section PM Threshold Exceeded

Step	Action

25 Clean the optical fiber connector on the transmitter circuit pack, then measure the transmit power again:

If the transmit power is	**Then**
still below the end of life transmit power	replace the circuit pack at the transmit end, then clean and reattach the optical fibers. See 323-1059-543, Procedures for equipment replacement on page 3-1 and *Installation*, 323-1059-201. Then, go to step 26.
within the operating range of the circuit pack	go to step 26

26 Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	go to step 29

Receive power is above the receiver overload for the circuit pack

27 Adjust the attenuation, if equipped, of the near-end receiver circuit pack to get the receive power within range.

28 Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	go to step 29

Receive power within operating range for the circuit pack

29 Clean all connections at both ends of the optical fiber link, then reattach the optical fibers. See *Installation*, 323-1059-201.

30 Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	step 31

31 Check whether there is a defective circuit pack. Replace the near-end receiver circuit pack, then clean and reattach the optical fibers. See 323-1059-543, Procedures for equipment replacement on page 3-1 and *Installation*, 323-1059-201.

—continued—

Procedure 5-75 (continued)
Section PM Threshold Exceeded

Step	Action
32	Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	go to step 33

33	If you have not already done so, replace the far-end transmitter circuit pack, then clean and reattach the optical fibers. See 323-1059-543, Procedures for equipment replacement on page 3-1 and *Installation*, 323-1059-201.
34	Check the PM counts for the facility:

If PM counts for exceeded thresholds	**Then**
have cleared or stopped increasing	you completed this procedure
are still increasing	contact your next level of support or your Nortel Networks support group for assistance

—end—

Procedure 5-76
SOC Software Version Mismatch

Probable cause

This alarm is raised on the network processor when network elements of a certain type in the span of control (SOC) are not running the same software version.

If the SOC has network elements of more than one type, a version check is performed on the network elements of the same type. The alarm is raised if all the network elements of a particular type are not running the same software version.

This alarm is raised when

- a network element of the same type is changed to a different software version
- a new network element of the same type is added to the SOC and is running a different software version
- a shelf processor circuit pack is replaced with a shelf processor that is running a different software version
- network elements in the same SOC are using different software modes (SONET and SONET and J-SDH)

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 5-11 and in *Installation,* 323-1059-201
- use an account with level 3 or higher user privilege code (UPC)

—continued—

Procedure 5-76 (continued)
SOC Software Version Mismatch

Step	Action
1	Retrieve all active and disabled alarms. See Retrieving active alarms for a network element on page 2-3.
2	Log in to all the network elements in the span of control (SOC) for the network processor.
3	Select a network element from the navigation tree.
4	Select Node Information from the Configuration menu and verify the software version on the network element.
5	Repeat step 3 and step 4 for each network element in the SOC.
6	**If** the network element is — **Then** running a lower version software — go to step 7 running a higher version software — go to step 8 not in use — remove the network element from the SOC running different software modes in the same SOC — contact your Nortel Networks support group.
7	Upgrade the specified network element to the software version currently installed on the other network elements in the network processor span of control. See 323-1059-302, Upgrading the software load on a network element from a local computer on page 6-58 or Upgrading the software load on a network element using an Ethernet connection on page 6-61. Go to step 9.
8	Upgrade the software version of all the other network elements in the span of control to the version currently installed on the network element with the highest software version. See 323-1059-302, Upgrading the software load on a network element from a local computer on page 6-58 or Upgrading the software load on a network element using an Ethernet connection on page 6-61.
9	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-77
Software Configuration Unknown

Probable cause

This alarm is raised when the shelf processor software fails to install the software control information.

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 5-78
Software Degradation

Probable cause

This alarm is raised when the BLSR configuration audit task fails to initiate. Without this task, no mechanism exists to determine if the BLSR configuration is accurate throughout the network.

Impact

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

Step	Action
1	Contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-79
SP Database Restore Fail

Probable cause

This alarm is raised when the command to restore provisioning data from a remote location directly to a shelf processor fails.

If this alarm is raised, no other save or restore can be performed on the same network element until this alarm is cleared.

Impact

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

Step	Action
1	Log in to a TL1 session and cancel the restore command by entering: `CANC-PROV-SP:[TID]::CTAG:::[TRGTID=Domain];`
2	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-80
SP Version Mismatch

Probable cause

This alarm is raised when the system detects that a shelf processor is in a shelf that requires an extended shelf processor functionality.

Impact

Major, service-affecting (M, SA) alarm

Note: Although traffic is not affected, once this alarm is raised all provisioning operations are denied until you replace the shelf processor.

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 5-11 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 shelf processor (slot 15) with an SPx. See Replacing the shelf processor on page 3-7.
3	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-81
STS Rx AIS

Probable cause

This alarm is raised when the optical interface circuit pack, EC-1x3, EC-1x12, or Packet Edge circuit pack receives an STS-1 alarm indication signal (AIS) in the SONET overhead of an STS-1 signal.

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

- incoming signal missing or errored at the far end
- circuit pack failed (tributary) at the far end
- loss of pointer alarm at a pass-through connection to the optical interface
- on a Packet Edge circuit pack if a ring has been created, cross-connects added, but no cards have been attached to the ring
- traffic is destined for an unreachable node in a BLSR configuration
- 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 in UPSR

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 5-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

Step	Action
1	Retrieve all active and disabled 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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	If the alarm does not clear, verify if the Traffic squelched alarm was raised. See Traffic Squelched on page 5-254.

—continued—

Procedure 5-81 (continued)
STS Rx AIS

Step	Action
4	Retrieve alarms to determine if STS Rx AIS cleared.
5	If the alarm does not clear, identify the circuit pack raising the alarm.
6	If the alarm is against the Packet Edge circuit pack, verify that all connections on that circuit pack for the ring number are properly provisioned. See 323-1059-320, Retrieving end-to-end connections on page 1-2.
7	Obtain the required topology for the network and identify the network elements using that use ring number.
8	If the connections for the ring number are not properly provisioned, delete the cross-connect and add them again. See 323-1059-320, Deleting an end-to-end connection on page 1-23.
9	Verify that all connections for the ring number are properly provisioned. See 323-1059-320, Retrieving end-to-end connections on page 1-2.
10	Retrieve alarms and verify if the alarm cleared. If the alarm does not clear, go to the next step.
11	Use the network connection information to identify the transmit and receive ends of the alarmed signal.
12	If the network element is not connected to an OPTera Metro 3500 network element at the remote end, and if the network element is part of a mid-span meet with a remote network element from another vendor, use the alarm system of the other vendor to find the problem.
13	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.
14	Retrieve all active and disabled alarms from the transmit end. See Retrieving active alarms for a network element on page 2-3.
15	If there is a loss of signal or circuit pack failed alarm on the DS3x3 or DS3x12 circuit pack at the transmit end, refer to the appropriate alarm clearing procedures.
16	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
17	Verify if there are alarms of higher order from the alarm hierarchy. See Alarm hierarchies on page 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
18	Clear the Rx unequipped, Rx signal label mismatch, or Rx loss of pointer alarms for the optical interface on the STS-1 path, if they exist.
19	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.

—continued—

Procedure 5-81 (continued)
STS Rx AIS

Step	Action
20	If the alarm does not clear, verify the facility state at the transmit end, if applicable. If the 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.
21	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
22	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-82
STS Rx Excessive BIP Error Rate

Probable cause

This alarm is raised when the received STS-1 is degraded to the point where it is unusable.

This alarm is caused by one of the following conditions:

- excessive attenuation
- dirty optical fibers
- dirty connectors
- improper connector seating
- transmit laser degrade
- network element provisioned with STS-1, but receives an STS-3c, STS-12c, STS-24c, or STS-48c signal

Impact

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

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)
- have the network connection information (that is, how the optical circuit packs on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201

—continued—

Procedure 5-82 (continued)
STS Rx Excessive BIP Error Rate

Step	Action
1	Retrieve all active and disabled alarms from the network element. See Retrieving active alarms for a network element on page 2-3.
2	Verify the alarm hierarchy. See Alarm hierarchies on page 5-9. 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 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: • Clear any alarms of higher order using the appropriate procedure. • If Rx Excessive BIP Error Rate is the only alarm, go to the next step.
7	Ensure that the cross-connect signal rate on the entire path matches the network connection information.
8	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
9	**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.

—continued—

Procedure 5-82 (continued)
STS Rx Excessive BIP Error Rate

Step	Action
10	Measure the receive power using an optical power meter. If the power is below the receiver sensitivity for this circuit pack, perform the following steps for STS 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. **e.** If the power is below the launch power (minimum), replace the optical interface 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. **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, clean the receive optical fibers and connections.
13	If the alarm does not clear, replace the optical interface circuit pack raising the alarm.
14	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-83
STS Rx Loss of Alignment or STS3C Rx Loss of Alignment

Probable cause

This alarm is raised when the STS members in a virtually concatenated group cannot be aligned because of excessive differential delay between the STS members. This alarm is raised against the slowest STS in the virtually concatenated group that connects to the WAN facility of a 2xGigE/FC-P2P 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)
- have the fiber connection information (that is, how the optical modules on each network element connect to other network elements)

Step	Action
1	Identify the STS on the optical interface circuit pack raising the alarm. The Unit field in the Active Alarms window specifies the circuit pack, slot, port (if applicable), and STS number. See Identifying the circuit pack or facility that has raised an alarm on page 2-52.
2	Trace the route of the STS raising the alarm. See 323-1059-320, Retrieving end-to-end connections on page 1-2.
3	Reprovision the path of the alarmed STS to a path similar to the other STS members in the virtually concatenated group. See 323-1059-320, Procedures for nodal cross-connect management on page 6-1.
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-84
STS Rx Loss of Multiframe or STS3C Rx Loss of Multiframe

Probable cause

This alarm is raised when the multiframe indicator for an STS member of a virtually concatenated group cannot be located. This alarm is raised against an STS that connects to the WAN facility of a 2xGigE/FC-P2P 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
- have the fiber connection information (that is, how the optical modules on each network element connect to other network elements)

Step	Action
1	Use the appropriate alarm clearing procedure to clear any other STS path alarms on the optical interface circuit pack that connects to the 2xGigE/FC-P2P circuit pack. The STS path alarms include STS Rx Signal Degrade, STS Rx Excessive BIP Error Rate, STS Rx Loss of Alignment, and STS Rx Loss of Sequence alarms.
2	Ensure that the virtual concatenation attribute is provisioned to the same setting at the near end and far end 2xGigE/FC-P2P circuit packs. **a.** Retrieve the virtual concatenation setting of the WAN facility for the 2xGigE/FC-P2P circuit pack raising the alarm: — 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 WAN facility of the 2xGigE/FC-P2P circuit pack raising the alarm. — From the Facility area, select WAN from the Facility Type drop-down list box. The virtual concatenation setting is displayed in the Facility table. **b.** Retrieve the virtual concatenation setting of the WAN facility at the other end of the connection. **c.** If necessary, modify the virtual concatenation attribute of the incorrectly provisioned WAN port. See 323-1059-350, Editing DS1, DS3, EC-1, 2x100BT-P2P or GE/FC SFP facility signal attributes.

—continued—

Procedure 5-84 (continued)
STS Rx Loss of Multiframe or STS3C Rx Loss of Multiframe

Step	Action
3	Trace the cross-connect information to ensure that the same number of STS1 or STS3c cross-connects are provisioned on the 2xGigE/FC-P2P circuit packs on both sides of the connection. See 323-1059-320, Procedures for nodal cross-connect management on page 6-1.
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-85
STS Rx Loss of Pointer

Probable cause

This alarm is raised when one of the following conditions occurs:

Note: In a BLSR configuration, if the state of the network element changes to be a passthrough network element while this alarm is active, the alarm will clear and the STS Rx unequipped alarm will be raised.

- pointer value in the SONET overhead of an STS-1 is out of a valid range
- pointer value in the SONET overhead of an STS-1 is not stable
- improper network synchronization
- squelching in a BLSR
- an STS-3c, STS-12c, STS-24c, or STS-48c signal is received instead of an STS-1 signal

Note: Both network elements must have corresponding cross-connects.

Impact

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

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)
- have the network connection information (that is, how the optical circuit packs on each network element connect to other network elements)

Step	Action
1	Retrieve all active and disabled 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 including the Traffic Squelched alarm. See Alarm hierarchies on page 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.

—continued—

Procedure 5-85 (continued)
STS Rx Loss of Pointer

Step	Action
3	Retrieve alarms and verify if the alarm cleared. If the alarm does not clear, go to the next step.
4	Use the network connection information to identify the receive and transmit ends of the alarmed signal. 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.
5	Retrieve all active and disabled alarms from the transmit end. See Retrieving active alarms for a network element on page 2-3.
6	Look for an alarm message for the required circuit pack that connects to the original shelf. • If you retrieve any alarms, verify if there are alarms of higher order from the alarm hierarchy. See Alarm hierarchies on page 5-9. Refer to the appropriate alarm clearing procedure for any higher order alarms. • If there is Rx RFI, or if there are no alarms, go to the next step.
7	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
8	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.
9	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
10	If the alarm does not clear, verify the connection rate for the entire path to ensure that it is correct. See 323-1059-320, Procedures for end-to-end connection management on page 1-1. If the connection rate is not correct, edit the cross-connects to the correct rates. See 323-1059-320, Editing an end-to-end connection on page 1-20.
11	Retrieve all active and disabled 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, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-86
STS Rx Loss of Sequence or STS3C Rx Loss of Sequence

Probable cause

This alarm is raised when the received sequence number of an STS in a virtually concatenated group does not match the expected sequence number. This alarm is raised against an STS that connects to the WAN facility of a 2xGigE/FC-P2P circuit pack.

Note: Sequence numbers specify the order of the STS members in a virtually concatenated group.

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)
- have the network connection information (that is, how the optical modules on each network element connect to other network elements)

Step	Action
1	Log in to each of the network elements on the STS-1 or STS-3c path as required and retrieve the cross-connects. See 323-1059-302, Procedures for logging in to a network element on page 2-1. See 323-1059-320, Procedures for end-to-end connection management on page 1-1.
2	Verify the connection information for the entire path to ensure the path is provisioned correctly.
3	Ensure that all STS members of the virtually concatenated group originate from the same 2xGigE/FC-P2P circuit pack.
4	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-87
STS Rx Path Trace Mismatch or STS3C Rx Path Trace Mismatch, STS 12c Rx Path Trace Mismatch, STS 24c Rx Path Trace Mismatch

Probable cause

This alarm is raised when incoming path trace values and expected values are different.

> ***Note 1:*** The path trace monitoring parameter turns alarm monitoring ON and OFF. The default is OFF. When monitoring is ON, the outgoing path trace message at one end and the expected path trace message at the other end must be the same or the alarm is raised. In 1+1 mode, path trace mismatch alarms are raised against the working optical interface circuit pack or DSM DS1x84 termination module mapper.
>
> ***Note 2:*** Path trace alarms are not raised when the STX-192 circuit pack is provisioned.

This alarm is also raised if connection mismatch or optical fiber connection mismatch exists.

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
- use an account with level 3 or higher user privilege code (UPC)

Step	Action
1	Retrieve all active and disabled 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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if STS Rx path trace mismatch cleared.
4	Use the optical fiber connection information to identify the transmit and receive ends of the STS or VT path.

—continued—

Procedure 5-87 (continued)
STS Rx Path Trace Mismatch or STS3C Rx Path Trace Mismatch, STS 12c Rx Path Trace Mismatch, STS 24c Rx Path Trace Mismatch

Step	Action
5	For an STS path, verify the path trace provisioning at both ends. See 323-1059-520, Retrieving path trace messages on page 2-6. For a VT path, verify the path trace provisioning at each node with a VT connection. See 323-1059-520, Retrieving path trace messages on page 2-6.
6	Ensure that path trace is provisioned correctly at each network element: ***Note 1:*** By default, when the STS-1 path is provisioned, the path trace monitoring feature is disabled. The expected incoming and outgoing path trace values are set to a string of 64 bytes of null characters. The DS3x3 or DS3x12e firmware does not report any mismatch between the actual incoming and the expected path trace values. No alarms are raised if any mismatch occurs. ***Note 2:*** In 1+1 mode, you can only edit the expected and the outgoing path trace messages on the working optical interface or DSM DS1x84 termination module mapper. You cannot edit the messages on the protection optical interface or DSM DS1x84 termination module mapper. Path trace on the protection facility automatically sets to the same as on the working optical interface or DSM DS1x84 termination module mapper. ***Note 3:*** To provision path trace, ensure that the cross-connect is already provisioned. See 323-1059-320, Retrieving end-to-end connections on page 1-2. **—end—**

Procedure 5-88
STS Rx RFI, or STS3C Rx RFI, STS12C Rx RFI, STS24C Rx RFI, or STS48C Rx RFI

Probable cause

This alarm is raised when the optical interface circuit pack, EC-1x3, or EC-1x12 circuit pack receives a signal with a remote fault indicator (RFI) sent in the SONET overhead. This alarm is raised when an alarm of higher order is raised on the remote network element.

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 occurs that causes the remote terminal to send this signal out.

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)
- clear any critical or major alarms prior to clearing the STS Rx, STS-3c Rx, STS-12c Rx, STS-24c Rx, or STS-48c Rx RFI alarms
- use an account with level 1 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	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.
4	Retrieve all active and disabled alarms from the remote network element. See Retrieving active alarms for a network element on page 2-3.
5	Look for an alarm message on the remote network element circuit pack that connects to the original shelf. Clear the alarm according to the alarm clearing procedure.

—continued—

Procedure 5-88 (continued)
STS Rx RFI, or STS3C Rx RFI, STS12C Rx RFI, STS24C Rx RFI, or STS48C Rx RFI

Step	Action
6	Verify the fiber connection for the optical interface circuit pack that connects to the original shelf. Repair, clean, and reconnect the fiber as required. ***Note:*** While this alarm is active you may also receive an SDCC Link Failure alarm. The SDCC Link Failure alarm clears automatically after the Rx RFI alarm is cleared.
7	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
8	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-89
STS Rx Signal Degrade, STS3C Rx Signal Degrade, STS12C Rx Signal Degrade, STS24C Rx Signal Degrade, or STS48C Rx Signal Degrade

Probable cause

This alarm is raised when the optical interface circuit pack detects that a respective STS-1, STS-3c, STS-12c, STS-24c, or STS-48c in the payload is significantly degraded.

One of the following conditions causes this alarm:

- excessive attenuation
- dirty optical fibers
- dirty connectors
- improper connector seating
- transmit laser degrade
- threshold set too high
- incorrect or faulty cabling at source end

Note: OPTera Metro 3500 continues to support the OC-12 IR (NTN404BA), IC (NTN404DA), LR (NTN404AA), and ER (NTN404CA) optical interface circuit packs, which support the VT1.5, STS-1, and STS-3c signal rates and associated performance monitoring.

Impact

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

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)
- have an optical power meter with the same optical connectors as the OPTera Metro 3500 network element
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

—continued—

Procedure 5-89 (continued)
STS Rx Signal Degrade, STS3C Rx Signal Degrade, STS12C Rx Signal Degrade, STS24C Rx Signal Degrade, or STS48C Rx Signal Degrade

Step	Action
1	Confirm which rate the alarm is raised against as either STS-1, STS-3c, STS-12c, STS-24c, or STS-48c.
2	Perform one of the following procedures for the rate required: • STS Rx Excessive BIP Error Rate on page 5-188. • STS3C Rx Excessive BIP Error Rate on page 5-210 • STS12C Rx Excessive BIP Error Rate on page 5-220 • STS24C Rx Excessive BIP Error Rate on page 5-229 • STS48C Rx Excessive BIP Error Rate on page 5-236 **—end—**

Procedure 5-90
STS Rx Signal Label Mismatch, STS3C Rx Signal Label Mismatch, STS12C Rx Signal Label Mismatch, STS24C Rx Signal Label Mismatch, or STS48C Rx Signal Label Mismatch

Probable cause

This alarm is raised when one of the following conditions occurs:

- the signal label of a received STS-1 or STS-3c or STS-12c, STS-24c or STS-48c does not match the expected signal label. For example, a DS3x3 mapped STS-1 is expected and a VT mapped STS-1 is received.
- the 2xGigE/FC-P2P circuit pack connects to a 2x100BT-P2P circuit pack

Impact

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

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)
- use an account with level 1 or higher user privilege code (UPC)

Step	Action
1	Retrieve all active and disabled 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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the 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 ends of the alarmed signal.If the network element is not connected to an OPTera Metro 3500 network element at the remote end or 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.

—continued—

Procedure 5-90 (continued)
STS Rx Signal Label Mismatch, STS3C Rx Signal Label Mismatch, STS12C Rx Signal Label Mismatch, STS24C Rx Signal Label Mismatch, or STS48C Rx Signal Label Mismatch

Step	Action
6	Log in to each of the network elements on the STS-1 or STS-3c path as required and retrieve the cross-connects. See 323-1059-302, Procedures for logging in to a network element on page 2-1. See 323-1059-320, Retrieving end-to-end connections on page 1-2.
7	Verify the connection information for the entire path to ensure the path is provisioned correctly before replacing the circuit pack. An error could have been made when entering the connections.
8	Retrieve all active and disabled alarms from the remote network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3. ***Note:*** If the alarmed STS is connected to a 2xGigE/FC-P2P circuit pack, check the cross-connect information to ensure that the 2xGigE/FC-P2P circuit pack connects to another 2xGigE/FC-P2P circuit pack at the far end. You cannot edit the WAN mapping protocol of a Fibre Channel facility. The WAN mapping mode for a Fibre Channel facility is always GFP-T.
9	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-91
STS Rx Unequipped

Probable cause

This alarm is raised when one of the following condiditons occurs

- there is an improper connection and a facility at the far-end network element is out of service. For example, no cross-connect is provisioned at the far end.

  Note 1: While provisioning, the likelihood of unequipped alarms being raised is high.

  Note 2: This procedure does not cover in detail the procedure for clearing an alarm caused during provisioning. You can disable alarm messages during provisioning.

  Note 3: This procedure makes the assumption that provisioning is not taking place, the system has been running without STS unequipped errors, and that all fail LEDs are cleared.

  Note 4: In a BLSR configuration, if the state of the network element changes to be a passthrough network element while the STS Rx loss of pointer alarm is active, the alarm will clear and the STS Rx Unequipped alarm will be raised.

Impact

Major, service-affecting (M, SA) alarm, if on active path, or if STS1s are VT managed
Minor, non-service-affecting (m, NSA) alarm, if on inactive path in a UPSR

Note: The payload is not available to be demapped and the STS path is unprotected, so the system cannot determine if path protection will be successful. Path protection occurs where the VT path terminates. If the protection path is available, the path terminating network element switches to that path to protect traffic.

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)
- use an account with level 3 or higher user privilege code (UPC)

—continued—

Procedure 5-91 (continued)
STS Rx Unequipped

Step	Action
1	Retrieve all active and disabled 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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the 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 network connection information to identify the transmit and receive ends for the alarmed signal.
6	If the network element is not connected to an OPTera Metro 3500 network element at the remote end or 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	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
8	Log in to each of the network elements on the required STS path and retrieve the cross-connects. See 323-1059-302, Procedures for logging in to a network element on page 2-1. 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 all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
11	Ensure that the DS3 facility at the far-end network element is in service. See 323-1059-350, Retrieving equipment and facility details on page 2-2.
12	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
13	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-92
STS3C Rx AIS

Probable cause

This alarm is raised when the optical interface circuit pack or Packet Edge circuit pack receives an STS-3c alarm indication signal (AIS) in the SONET overhead of an STS-3c signal.

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

- incoming signal missing or errored at the far end
- circuit pack failed at the far end
- loss of pointer alarm at a pass-through connection to the optical interface
- on a Packet Edge circuit pack if a ring has been created, cross-connects added, but no cards have been attached to the ring
- traffic is destined for an unreachable node in a BLSR configuration
- 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 in a UPSR

Note: The alarm status is minor, because it is a secondary alarm that indicates a problem upstream of this network element.

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)
- use an account with level 1 or higher user privilege code (UPC)

Step	Action
1	Retrieve all active and disabled 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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	If the alarm does not clear, verify if the Traffic squelched alarm was raised. See Traffic Squelched on page 5-254.

—continued—

Procedure 5-92 (continued)
STS3C Rx AIS

Step	Action
4	Retrieve alarms to determine if the 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 transmit and receive ends of the alarmed signal.
7	If the network element is not connected to an OPTera Metro 3500 NE element at the remote end or part of a mid-span meet and the remote NE is from another vendor, use the alarm system of the other vendor to find the problem.
8	If the alarm is against the Packet Edge circuit pack, verify that all connections on that circuit pack for the ring number are properly provisioned. See 323-1059-320, Retrieving end-to-end connections on page 1-2.
9	Obtain the required topology for the network and identify the network elements using that use ring number.
10	If the connections for the ring number are not properly provisioned, delete the cross-connect and add them again. See 323-1059-320, Deleting an end-to-end connection on page 1-23.
11	Verify that all connections for the ring number are properly provisioned. See 323-1059-320, Retrieving end-to-end connections on page 1-2.
12	Retrieve alarms and verify if the alarm cleared. If the alarm does not clear, go to the next step.
13	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.
14	Retrieve all active and disabled alarms from the transmit end. See Retrieving active alarms for a network element on page 2-3.
15	If there is a loss of signal or circuit pack failed alarm on the optical interface circuit pack at the transmit end, refer to the appropriate alarm clearing procedures.
16	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
17	If the alarm does not clear, log in to each of the pass-through network elements and retrieve alarms.
18	Verify if there are alarms of higher order from the alarm hierarchy. See Alarm hierarchies on page 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.

—continued—

Procedure 5-92 (continued)
STS3C Rx AIS

Step	Action
19	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
20	If the alarm does not clear, contact your next level of support.

—end—

Procedure 5-93
STS3C Rx Excessive BIP Error Rate

Probable cause

This alarm is raised when the received STS-3c is degraded to the point where it is unusable.

This alarm is caused by one of the following conditions:

- excessive attenuation
- dirty optical fibers
- dirty connectors
- improper connector seating
- transmit laser degrade
- the network element is provisioned with STS-3c, but receives an STS-1, STS-12c, STS-24c, or STS-48c signal

Impact

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

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)
- have the network connection information (that is, how the optical circuit packs on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201

—continued—

Procedure 5-93 (continued)
STS3C Rx Excessive BIP Error Rate

Step	Action
1	Retrieve all active and disabled 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 5-9. 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 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. Clear any alarms of higher order by following the appropriate procedure. If Rx Excessive BIP Error Rate is the only alarm, go to the next step.
7	Ensure that the cross-connect signal rate on the entire path matches the network connection information.
8	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
9	**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.

—continued—

Procedure 5-93 (continued)
STS3C Rx Excessive BIP Error Rate

Step	Action
10	Measure the receive power using an optical power meter. If the power is below the receiver sensitivity for this circuit pack, perform the following steps for STS3C 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. **e.** If the power is below the launch power (minimum), replace the optical interface 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. **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, clean the receive optical fibers and connections.
13	If the alarm does not clear, replace the circuit pack raising the alarm.
14	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-94
STS3C Rx Loss of Pointer

Probable cause

This alarm is raised when one of the following conditions occurs:

Note: In a BLSR configuration, if the state of the network element changes to be a passthrough network element while this alarm is active, the alarm will clear and the STS3C Rx unequipped alarm will be raised.

- pointer value in the SONET overhead of an STS-3c is out of a valid range
- pointer value in the SONET overhead of an STS-3c is not stable
- improper network synchronization
- squelching in a BLSR
- network element provisioned with STS-3c cross-connect but the incoming signal is an STS-1, STS-12c, STS-24c, or STS-48c
- on a Packet Edge circuit pack if a ring has been created, and cross-connects added at only one NE
- improper or no connection provisioned at the far-end

  Note 1: If the remote end is not provisioned with a corresponding STS-3c cross-connect, the local end raises this alarm when it receives a non-concatenated STS-1 signal. For example, this often occurs while provisioning.

  Note 2: In a BLSR ring, if far end is an OC-12 or OC-12x4 card and the STS3c connection is deleted, on this SONET channel is going to be raised on OC192 card on the near end
- when a circuit pack has been provisioned for concatenated signals but an unequipped signal is sent

  Note: OC-192 circuit packs cause an Unequipped alarm instead of a Loss of Pointer alarm.

Impact

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

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 circuit packs on each network element connect to other network elements)

—continued—

Procedure 5-94 (continued)
STS3C Rx Loss of Pointer

- use an account with level 1 or higher user privilege code (UPC)

Step	Action
1	Retrieve all active and disabled 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 including the Traffic Squelched alarm. See Alarm hierarchies on page 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms and verify if the alarm cleared. 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. If the alarm is against a Packet Edge circuit pack, go to step 4. If the alarm is not against a Packet Edge circuit pack, go to step 10.
4	Verify that all connections on that circuit pack for the ring number are properly provisioned. See 323-1059-320, Retrieving end-to-end connections on page 1-2.
5	Obtain the required topology for the network and identify the network elements using that ring number.
6	If the connections for the ring number are not properly provisioned, delete the cross-connect and add it back. See 323-1059-320, Deleting an end-to-end connection on page 1-23.
7	Verify that all connections for the ring number are properly provisioned. See 323-1059-320, Retrieving end-to-end connections on page 1-2.
8	Retrieve alarms and verify if the alarm cleared.
9	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.
10	Use the optical fiber connection information to identify the receive and transmit ends of the alarmed signal.
11	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.
12	Retrieve all active and disabled alarms from the transmit end. See Retrieving active alarms for a network element on page 2-3.
13	Look for an alarm message for the optical interface circuit pack that connects to the original shelf.
14	Verify and clear any alarms of higher order in the alarm hierarchy. See Alarm hierarchies on page 5-9. Refer to the appropriate alarm clearing procedures.
15	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.

—continued—

Procedure 5-94 (continued)
STS3C Rx Loss of Pointer

Step	Action
16	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
17	If the alarm does not clear, verify the connection rate for the entire STS-3c path to ensure that it is correct. See 323-1059-320, Procedures for end-to-end connection management on page 1-1. If the connection rate is not correct, edit the cross-connects to the correct rates. See 323-1059-320, Editing an end-to-end connection on page 1-20.
18	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
19	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-95
STS3C Rx Unequipped, STS12C Rx Unequipped, STS24C Rx Unequipped, or STS48C Rx Unequipped

Probable cause

This alarm is raised when one of the following conditions occurs

- there is an improper connection and a facility at the far-end network element is out of service. For example, no cross-connect is provisioned at the far end.
- a circuit pack has been provisioned but an unequipped signal is sent.

  Note 1: OCn circuit packs other than OC-192 define unequipped signals differently than OC-192, consequently a Loss of Pointer alarm is raised if the OCn card receiving the unequipped signal is expecting a concatenated signal.

  Note 2: While provisioning, the likelihood of unequipped alarms being raised is high.

  Note 3: This procedure does not cover in detail the procedure for clearing an alarm caused during provisioning. You can disable alarm messages during provisioning.

  Note 4: This procedure makes the assumption that provisioning is not taking place, the system has been running without STS-3c, STS-12c, STS-24c, or STS-48c unequipped errors, and that all fail LEDs are cleared.

  Note 5: In a BLSR configuration, if the state of the network element changes to be a passthrough network element while the STS Rx loss of pointer alarm is active, the STS3C, STS12C, STS24C, or STS48C Rx loss of pointer alarm will clear and the STS3C, STS12C, STS24C, or STS48C Rx unequipped alarm will be raised.

Impact

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

Note: The payload is not available to be demapped and the STS path is unprotected, so the system cannot determine if path protection will be successful. Path protection occurs where the VT path terminates. If the protection path is available, the path terminating network element switches to that path to protect traffic.

—continued—

Procedure 5-95 (continued)
STS3C Rx Unequipped, STS12C Rx Unequipped, STS24C Rx Unequipped, or STS48C Rx Unequipped

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)
- use an account with level 3 or higher user privilege code (UPC)

Step	Action
1	Retrieve all active and disabled 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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms to determine if the 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 network connection information to identify the transmit and receive ends for the alarmed signal.
6	If the network element is not connected to an OPTera Metro 3500 network element at the remote end or 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	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
8	Log in to each of the network elements on the required STS3c, STS12c, STS24c, or STS48c path and retrieve the cross-connects. See 323-1059-302, Procedures for logging in to a network element on page 2-1. 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 all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
11	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-96
STS12C Rx AIS

Probable cause

This alarm is raised when the optical interface circuit pack or Packet Edge circuit pack receives an STS-12c alarm indication signal (AIS) in the SONET overhead of an STS-12c signal.

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

- incoming signal missing or errored at the far end
- circuit pack failed at the far end
- loss of pointer alarm at a pass-through connection to the optical interface
- on a Packet Edge circuit pack if a ring has been created, cross-connects added, but no cards have been attached to the ring
- traffic is destined for an unreachable node in a BLSR configuration

Impact

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

Note: The alarm status is minor, because it is a secondary alarm that indicates a problem upstream of this network element.

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)
- use an account with level 1 or higher user privilege code (UPC)

Step	Action
1	Retrieve all active and disabled 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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	If the alarm does not clear, verify if the Traffic squelched alarm was raised. See Traffic Squelched on page 5-254.
4	Retrieve alarms to determine if the alarm cleared.

—continued—

Procedure 5-96 (continued)
STS12C Rx AIS

Step	Action
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 transmit and receive ends of the alarmed signal.
7	If the network element is not connected to an OPTera Metro 3500 network element at the remote end or 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	If the alarm is against the Packet Edge circuit pack, verify that all connections on that circuit pack for the ring number are properly provisioned. See 323-1059-320, Retrieving end-to-end connections on page 1-2.
9	Obtain the required topology for the network and identify the network elements using that use ring number.
10	If the connections for the ring number are not properly provisioned, delete the cross-connect and add them again. See 323-1059-320, Deleting an end-to-end connection on page 1-23.
11	Verify that all connections for the ring number are properly provisioned. See 323-1059-320, Retrieving end-to-end connections on page 1-2.
12	Retrieve alarms and verify if the alarm cleared. If the alarm does not clear, go to the next step.
13	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.
14	Retrieve all active and disabled alarms from the transmit end. See Retrieving active alarms for a network element on page 2-3.
15	If there is a loss of signal or circuit pack failed alarm on the OC-12, OC-12x4 STS, OC-48, OC-48 STS, or OC-192 circuit pack at the transmit end, refer to the appropriate alarm clearing procedures.
16	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
17	If the alarm does not clear, log in to each of the pass-through network elements and retrieve alarms.
18	Verify if there are alarms of higher order from the alarm hierarchy. See Alarm hierarchies on page 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
19	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
20	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-97
STS12C Rx Excessive BIP Error Rate

Probable cause

This alarm is raised when the received STS-12c signal is degraded to the point where it is unusable.

This alarm is caused by one of the following conditions:

- excessive attenuation
- dirty optical fibers
- dirty connectors
- improper connector seating
- transmit laser degrade
- the network element is provisioned with STS-12c, but receives an STS-1, STS-3c, STS-24c, or STS-48c signal

  Note: OPTera Metro 3500 continues to support the OC-12 IR (NTN404BA), IC (NTN404DA), LR (NTN404AA), and ER (NTN404CA) optical interface circuit packs, which support the VT1.5, STS-1, and STS-3c signal rates and associated performance monitoring.

Impact

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

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)
- have the network connection information (that is, how the optical circuit packs on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201

—continued—

Procedure 5-97 (continued)
STS12C Rx Excessive BIP Error Rate

Step	Action
1	Retrieve all active and disabled 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 5-9. 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 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. Clear any alarms of higher order by following the appropriate procedure. If Rx Excessive BIP Error Rate is the only alarm, go to the next step.
7	Ensure that the cross-connect signal rate on the entire path matches the network connection information.
8	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
9	**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.

—continued—

Procedure 5-97 (continued)
STS12C Rx Excessive BIP Error Rate

Step	Action
10	Measure the receive power using an optical power meter. If the power is below the receiver sensitivity for this circuit pack, perform the following steps for STS12C 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. **e.** If the power is below the launch power (minimum), replace the OC-12, OC-12x4 STS, OC-48, OC-48 STS, or OC-192 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. **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 alarm does not clear, replace the circuit pack raising the alarm.
12	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-98
STS12C Rx Loss of Pointer

Probable cause

This alarm is raised when one of the following conditions occurs:

Note: In a BLSR configuration, if the state of the network element changes to be a passthrough network element while this alarm is active, the alarm will clear and the STS12C Rx unequipped alarm will be raised.

- pointer value in the SONET overhead of an STS-12c is out of a valid range
- pointer value in the SONET overhead of an STS-12c is not stable
- improper network synchronization
- squelching in a BLSR
- network element provisioned with STS-12c cross-connect but the incoming signal is an STS-1, STS-3c, STS-24c, or STS-48c signal
- on a Packet Edge circuit pack if a ring has been created, and cross-connects added at only one NE
- improper or no connection provisioned at the far-end

  Note: If the remote end is not provisioned with a corresponding STS-12c cross-connect, the local end raises this alarm when it receives a non-concatenated STS-1 signal. This often occurs while provisioning.

- when a circuit pack has been provisioned for concatenated signals but an unequipped signal is sent

  Note: OC-192 circuit packs cause an Unequipped alarm instead of a Loss of Pointer alarm.

Impact

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

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 circuit packs on each network element connect to other network elements)
- use an account with level 1 or higher user privilege code (UPC)

—continued—

Procedure 5-98 (continued)
STS12C Rx Loss of Pointer

Step	Action
1	Retrieve all active and disabled 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 including the Traffic Squelched alarm. See Alarm hierarchies on page 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms and verify if the alarm cleared. 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. If the alarm is against a Packet Edge circuit pack go to step 4. If the alarm is not against a Packet Edge circuit pack, go to step 8.
4	Verify that all connections for the ring number are properly provisioned. See 323-1059-320, Retrieving end-to-end connections on page 1-2.
5	Obtain the required topology for the network and identify the network elements using that ring number.
6	If the connections for the ring number are not properly provisioned, delete the cross-connect and add it back. See 323-1059-320, Deleting an end-to-end connection on page 1-23.
7	Verify that all connections for the ring number are properly provisioned. See 323-1059-320, Retrieving end-to-end connections on page 1-2.
8	Use the optical fiber connection information to identify the receive and transmit ends of the alarmed signal.
9	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.
10	Retrieve all active and disabled alarms from the transmit end. See Retrieving active alarms for a network element on page 2-3.
11	Look for an alarm message for the OC-12, OC-12x4 STS, OC-48, OC-48 STS, or OC-192 circuit pack that connects to the original shelf.
12	Verify if there are any alarms of a higher order in the alarm hierarchy. See Alarm hierarchies on page 5-9. Refer to the appropriate alarm clearing procedures for any higher order alarms.
13	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.
14	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.

—continued—

Procedure 5-98 (continued)
STS12C Rx Loss of Pointer

Step	Action
15	If the alarm does not clear, verify the connection rate for the entire STS-12c path to ensure that it is correct. See 323-1059-320, Procedures for end-to-end connection management on page 1-1. If the connection rate is not correct, edit the cross-connects to the correct rates. See 323-1059-320, Editing an end-to-end connection on page 1-20.
16	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
17	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-99
STS12C Unsupported Concatenated Service

Probable cause

This alarm is raised on a Packet Edge circuit pack that does not support STS-12c if you try to provision it with STS-12c service.

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 1 or higher user privilege code (UPC)

Step	Action
1	Wear antistatic wrist and foot straps to protect the shelf from damage. Connect the wrist strap to the ESD jack on the shelf.
2	Replace the circuit pack raising the alarm with a Packet Edge circuit pack that does support STS-12c. See Replacing an OPTera Packet Edge circuit pack on page 3-15.
3	Retrieve all active and disabled alarms and verify the alarm. See Retrieving active alarms for a network element on page 2-3.
4	If the alarm does not clear, contact your next level of support of your Nortel Networks support group.

—end—

Procedure 5-100
STS24C Rx AIS

Probable cause

This alarm is raised when the optical interface circuit pack receives an STS-24c alarm indication signal (AIS) in the SONET overhead of an STS-24c signal.

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

- incoming signal missing or errored at the far end
- circuit pack failed at the far end
- loss of pointer alarm at a pass-through connection to the optical interface
- traffic is destined for an unreachable node in a BLSR configuration

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 it is a secondary alarm that indicates a problem upstream of this network element.

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)
- use an account with level 1 or higher user privilege code (UPC)

Step	Action
1	Retrieve all active and disabled 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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	If the alarm does not clear, verify if the Traffic squelched alarm was raised. See Traffic Squelched on page 5-254.
4	Retrieve alarms to determine if the alarm cleared.

—continued—

Procedure 5-100 (continued)
STS24C Rx AIS

Step	Action
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 transmit and receive ends of the alarmed signal.
7	If the network element is not connected to an OPTera Metro 3500 network element at the remote end or 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 the network element at the transmit end.See 323-1059-302, Procedures for logging in to a network element on page 2-1.
9	Retrieve all active and disabled alarms from the transmit end. See Retrieving active alarms for a network element on page 2-3.
10	If there is a loss of signal or circuit pack failed alarm on the OC-48 STS or OC-192 circuit pack at the transmit end, refer to the appropriate alarm clearing procedures.
11	Retrieve all active and disabled 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, log in to each of the pass-through network elements and retrieve alarms.
13	Verify if there are alarms of higher order from the alarm hierarchy. See Alarm hierarchies on page 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
14	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
15	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-101
STS24C Rx Excessive BIP Error Rate

Probable cause

This alarm is raised when the received STS-24c signal is degraded to the point where it is unusable.

This alarm is caused by one of the following conditions:

- excessive attenuation
- dirty optical fibers
- dirty connectors
- improper connector seating
- transmit laser degrade
- the network element is provisioned with STS-24c, but receives an STS-1 STS-3c, STS-12c, or STS-48c signal

Impact

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

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)
- have the network connection information (that is, how the optical circuit packs on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201

—continued—

Procedure 5-101 (continued)
STS24C Rx Excessive BIP Error Rate

Step	Action
1	Retrieve all active and disabled 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 5-9. 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 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. Clear any alarms of higher order by following the appropriate procedure. If Rx Excessive BIP Error Rate is the only alarm, go to the next step.
7	Ensure that the cross-connect signal rate on the entire path matches the network connection information.
8	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
9	**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.

—continued—

Procedure 5-101 (continued)
STS24C Rx Excessive BIP Error Rate

Step	Action
10	Measure the receive power using an optical power meter. If the power is below the receiver sensitivity for this circuit pack, perform the following steps for STS24C 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. **e.** If the power is below the launch power (minimum), replace the OC-48 STS or OC-192 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. **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 alarm does not clear, replace the circuit pack raising the alarm.
12	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-102
STS24C Rx Loss of Pointer

Probable cause

This alarm is raised when one of the following conditions occurs:

Note: In a BLSR configuration, if the state of the network element changes to be a passthrough network element while this alarm is active, the alarm will clear and the STS24C Rx unequipped alarm will be raised.

- pointer value in the SONET overhead of an STS-24c is out of a valid range
- pointer value in the SONET overhead of an STS-24c is not stable
- improper network synchronization
- squelching in a BLSR
- network element provisioned with STS-24c cross-connect but the incoming signal is an STS-1, STS-3c, STS-12c, or STS-48c
- improper or no connection provisioned at the far-end

  Note: If the remote end is not provisioned with a corresponding STS-24c cross-connect, the local end raises this alarm when it receives a non-concatenated STS-1 signal. This often occurs while provisioning.

- when a circuit pack has been provisioned for concatenated signals but an unequipped signal is sent

  Note: OC-192 circuit packs cause an Unequipped alarm instead of a Loss of Pointer alarm.

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 network connection information (that is, how the optical circuit packs on each network element connect to other network elements)
- use an account with level 1 or higher user privilege code (UPC)

Step	Action
1	Retrieve all active and disabled alarms from the network element. See Retrieving active alarms for a network element on page 2-3.

—continued—

Procedure 5-102 (continued)
STS24C Rx Loss of Pointer

Step	Action
2	Verify if there are alarms of higher order from the alarm hierarchy including the Traffic Squelched alarm. See Alarm hierarchies on page 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms and verify if the alarm cleared. 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.
4	Use the optical fiber connection information to identify the receive and transmit ends of the alarmed signal.
5	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.
6	Retrieve all active and disabled alarms from the transmit end. See Retrieving active alarms for a network element on page 2-3.
7	Look for an alarm message for the OC-48 STS or OC-192 circuit pack that connects to the original shelf.
8	Verify if there are any alarms of a higher order in the alarm hierarchy. See Alarm hierarchies on page 5-9. Refer to the appropriate alarm clearing procedures for any higher order alarms.
9	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.
10	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
11	If the alarm does not clear, verify the connection rate for the entire STS-24c path to ensure that it is correct. See 323-1059-320, Procedures for end-to-end connection management on page 1-1. If the connection rate is not correct, edit the cross-connects to the correct rates. See 323-1059-320, Editing an end-to-end connection on page 1-20.
12	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
13	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-103
STS48C Rx AIS

Probable cause

This alarm is raised when the optical interface circuit pack receives an STS-48c alarm indication signal (AIS) in the SONET overhead of an STS-48c signal.

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

- incoming signal missing or errored at the far end
- circuit pack failed at the far end
- loss of pointer alarm at a pass-through connection to the optical interface
- traffic is destined for an unreachable node in a BLSR configuration

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 it is a secondary alarm that indicates a problem upstream of this network element.

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)
- use an account with level 1 or higher user privilege code (UPC)

Step	Action
1	Retrieve all active and disabled 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 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	If the alarm does not clear, verify if the Traffic squelched alarm was raised. See Traffic Squelched on page 5-254.
4	Retrieve alarms to determine if the alarm cleared.

—continued—

Procedure 5-103 (continued)
STS48C Rx AIS

Step	Action
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 transmit and receive ends of the alarmed signal.
7	If the network element is not connected to an OPTera Metro 3500 network element at the remote end or 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 the network element at the transmit end.See 323-1059-302, Procedures for logging in to a network element on page 2-1.
9	Retrieve all active and disabled alarms from the transmit end. See Retrieving active alarms for a network element on page 2-3.
10	If there is a loss of signal or circuit pack failed alarm on the OC-48 STS or OC-192 circuit pack at the transmit end, refer to the appropriate alarm clearing procedures.
11	Retrieve all active and disabled 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, log in to each of the pass-through network elements and retrieve alarms.
13	Verify if there are alarms of higher order from the alarm hierarchy. See Alarm hierarchies on page 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
14	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
15	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-104
STS48C Rx Excessive BIP Error Rate

Probable cause

This alarm is raised when the received STS-48c signal is degraded to the point where it is unusable.

This alarm is caused by one of the following conditions:

- excessive attenuation
- dirty optical fibers
- dirty connectors
- improper connector seating
- transmit laser degrade
- the network element is provisioned with STS-48c, but receives an STS-1 STS-3c, STS-12c, or STS-24c signal

Impact

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

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)
- have the network connection information (that is, how the optical circuit packs on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element

Step	Action
1	Observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201Retrieve all active and disabled 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 5-9. 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.

—continued—

Procedure 5-104 (continued)
STS48C Rx Excessive BIP Error Rate

Step	Action
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 the receive sites of the alarmed signal.
6	Retrieve all alarms from the transmit end. Clear any alarms of higher order by following the appropriate procedure. If Rx Excessive BIP Error Rate is the only alarm, go to the next step.
7	Ensure that the cross-connect signal rate on the entire path matches the network connection information.
8	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
9	**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.

—continued—

Procedure 5-104 (continued)
STS48C Rx Excessive BIP Error Rate

Step	Action
10	Measure the receive power using an optical power meter. If the power is below the receiver sensitivity for this circuit pack, perform the following steps for STS48C 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. **e.** If the power is below the launch power (minimum), replace the OC-48 STS or OC-192 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. **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 alarm does not clear, replace the circuit pack raising the alarm.
12	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-105
STS48C Rx Loss of Pointer

Probable cause

This alarm is raised when one of the following conditions occurs:

Note: In a BLSR configuration, if the state of the network element changes to be a passthrough network element while this alarm is active, the alarm will clear and the STS48C Rx unequipped alarm will be raised.

- pointer value in the SONET overhead of an STS-48c is out of a valid range
- pointer value in the SONET overhead of an STS-48c is not stable
- improper network synchronization
- squelching in a BLSR
- network element provisioned with STS-48c cross-connect but the incoming signal is an STS-1, STS-3c, STS-12c, or STS-24c
- improper or no connection provisioned at the far-end

  Note: If the remote end is not provisioned with a corresponding STS-48c cross-connect, the local end raises this alarm when it receives a non-concatenated STS-1 signal. This often occurs while provisioning.

- when a circuit pack has been provisioned for concatenated signals but an unequipped signal is sent

  Note: OC-192 circuit packs cause an Unequipped alarm instead of a Loss of Pointer alarm.

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 network connection information (that is, how the optical circuit packs on each network element connect to other network elements)
- use an account with level 1 or higher user privilege code (UPC)

Step	Action
1	Retrieve all active and disabled alarms from the network element. See Retrieving active alarms for a network element on page 2-3.

—continued—

Procedure 5-105 (continued)
STS48C Rx Loss of Pointer

Step	Action
2	Verify if there are alarms of higher order from the alarm hierarchy including the Traffic Squelched alarm. See Alarm hierarchies on page 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
3	Retrieve alarms and verify if the alarm cleared. 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.
4	Use the optical fiber connection information to identify the receive and transmit ends of the alarmed signal.
5	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.
6	Retrieve all active and disabled alarms from the transmit end. See Retrieving active alarms for a network element on page 2-3.
7	Look for an alarm message for the OC-48 STS or OC-192 circuit pack that connects to the original shelf.
8	Verify if there are any alarms of a higher order in the alarm hierarchy. See Alarm hierarchies on page 5-9. Refer to the appropriate alarm clearing procedures for any higher order alarms.
9	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.
10	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
11	If the alarm does not clear, verify the connection rate for the entire STS-48c path to ensure that it is correct. See 323-1059-320, Procedures for end-to-end connection management on page 1-1. If the connection rate is not correct, edit the cross-connects to the correct rates. See 323-1059-320, Editing an end-to-end connection on page 1-20.
12	Retrieve all active and disabled alarms from the original network element to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
13	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-106
Switch mode mismatch

Probable cause

This alarm is raised when the near-end and far-end network elements are not operating in the same mode - unidirectional or bidirectional. For every pair of optical interfaces in linear 1+1 mode, you can configure unidirectional or bidirectional line switching.

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 5-11, and in *Installation,* 323-1059-201
- have an account with a level 3 or higher UPC

Step	Action
1	Retrieve the switch mode for the linear optical interface at the near-end and far-end network elements. See Retrieving protection scheme and protection switch mode for a pair of optical facilities on page 1-3.
2	Change the switch mode of the appropriate optical interface to ensure that the near-end and far-end network elements are both unidirectional or bidirectional. See Changing the linear protection switch mode for a pair of optical facilities on page 1-4. ***Note:*** Changing the protection swtich mode for one of the optical interface circuit packs in a pair automatically changes the protection switch mode for the other circuit pack.
3	Change the switch mode for every set of linear optical interfaces in the configuration until the alarm clears. See Changing the linear protection switch mode for a pair of optical facilities on page 1-4. ***Note:*** Changing the protection swtich mode for one of the optical interface circuit packs in a pair automatically changes the protection switch mode for the other circuit pack.

—end—

Procedure 5-107
TBOS Connection Failure

Probable cause

This alarm is raised when the network element detects that the network elements mapped into the TBOS array have stopped reporting.

Note 1: This procedure assumes that the system is not being provisioned and all nodes are in contact before the fault occurred.

Note 2: Clear this alarm only after you clear all SDCC link failure alarms and conditions.

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)
- have the network connection information (that is, how the optical modules on each network element connect to other network elements)
- ensure that there are no active SDCC link failure alarms or conditions in the network

Step	Action
1	Retrieve all active and disabled alarms. See Retrieving active alarms for a network element on page 2-3.
2	Record the TID of the network element that does not respond.Wear an antistatic wrist strap to protect the shelf from static damage.
3	Connect the wrist strap to the ESD jack on the shelf.

—continued—

Procedure 5-107 (continued)
TBOS Connection Failure

Step	Action
4	Try to log in to the remote network element you identified. If you cannot log in remotely, perform the following steps for TBOS connection failure (unable to log in to remote network element): **a.** Replace the shelf processor at the site where the remote shelf is located. See Replacing the shelf processor on page 3-7. **b.** Wait 5 minutes for the shelf processor to restart. **c.** Log in to the network element and retrieve all active and disabled alarms to determine if the alarm cleared. See 323-1059-302, Procedures for logging in to a network element on page 2-1. **d.** If the alarm does not clear, perform a WARM restart the shelf processor at the network element that raised the alarm. See Restarting the shelf processor on page 2-47. **e.** When you work in a remote session, a loss of connection occurs when you restart the shelf processor. Log in again after the restart. **f.** Wait 5 minutes for the shelf processor to restart. **g.** Retrieve all active and disabled alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3. **h.** If the alarm does not clear, contact your next level of support or your Nortel Networks support group. If the remote login is successful, go to the next step.
5	Perform a WARM restart on the remote shelf processor. See Restarting the shelf processor on page 2-47. ***Note:*** When you work in a remote session, a loss of connection occurs when you restart the shelf processor. Log in again after the restart.
6	Wait 5 minutes for the shelf processor to restart.
7	Retrieve all active and disabled alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.If the alarm does not clear, perform a WARM restart on the shelf processor at the network element that originally raised the alarm. See Restarting the shelf processor on page 2-47. ***Note:*** When you work in a remote session, a loss of connection occurs when you restart the shelf processor. Log in again after the restart.
8	Wait 5 minutes for the shelf processor to restart.
9	Retrieve all active and disabled alarms to determine if the alarm cleared. See Retrieving active alarms for a network element on page 2-3.
10	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-108
Threshold AIS on BITSout-A or Threshold AIS on BITSout-B

Probable cause

If the signal quality of the BITS out source (determined by the synchronization status message (SSM) in the OC-n signal) is at or below the user provisioned threshold level, the BITS out timing reference sends an alarm indication signal (AIS) and the alarm is raised.

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	Ensure that the user-provisioned threshold value is correct. See 323-1051-310, Provisioning BITS Out on page 1-13.
2	Verify if the active alarms include Loss of BITSout-A Pri. Timing Ref. or Loss of BITSout-B Pri. Timing Ref. or Loss of BITSout-A Sec. Timing Ref. or Loss of BITSout-B Sec. Timing Ref. on page 5-38. Clear the alarms according to the alarm clearing procedure.
3	If the alarm does not clear, check if there is a provisioned quality level for the active BITS Out reference. **If** the quality level for the active BITS Out reference is — **Then** go to provisioned — step 4 not provisioned — step 5
4	Verify that the provisioned quality level for the active synchronization reference is correct. See 323-1051-310, Setting the synchronization-status message quality value on page 1-7. If the provisioned value is supposed to be at or below the threshold value, then this synchronization reference signal quality is too low to be used as a BITS out reference. Select a different BITS out reference. See 323-1051-310, Provisioning BITS Out on page 1-13. If the provisioned value is above the threshold value, contact your next level of support or your Nortel Networks support group. You have completed this procedure.

—continued—

Procedure 5-108 (continued)
Threshold AIS on BITSout-A or Threshold AIS on BITSout-B

Step	Action
5	On the network element that raised the alarm, verify the synchronization quality level for the active reference signal for the BITS out signal. See 323-1051-310, Retrieving synchronization data for a network element on page 1-2.

If the synchronization quality level is	**Then**
equal or below the provisioned threshold value	go to step 6
above the provisioned threshold value	contact your next level of support or your Nortel Networks support group

6	Working from the network element that raised the alarm, verify the source of the active timing reference (The alarm is raised on Network element D in Synchronization on page 5-246.)
7	Clear all synchronization alarms.
8	If the alarm does not clear, check if there is a provisioned quality level for the active synchronization reference.

If the quality level for the active synchronization reference is	**Then** go to
provisioned	step 9
not provisioned	step 10

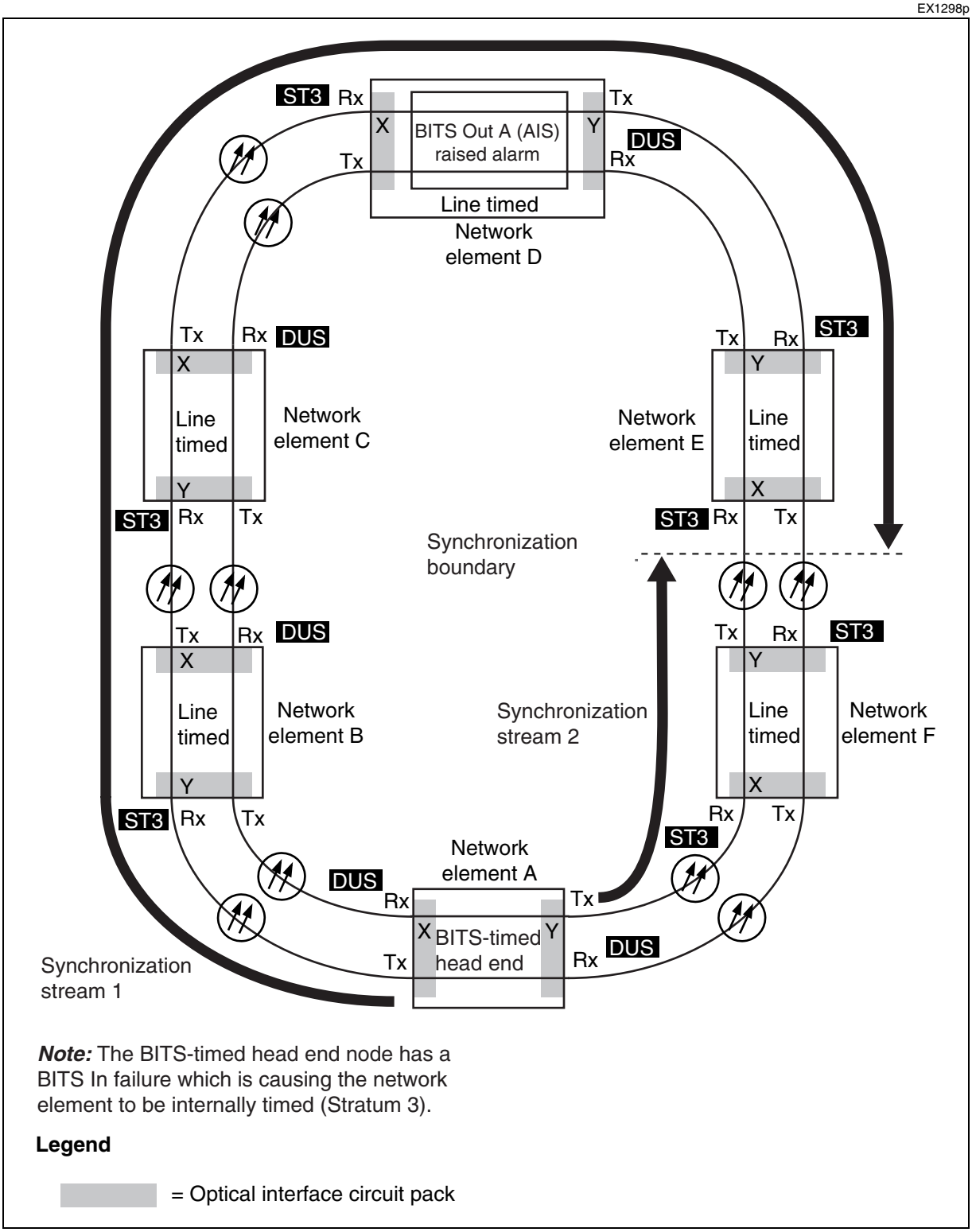
9	Verify that the provisioned quality level for the active synchronization reference is correct. See 323-1051-310, Setting the synchronization-status message quality value on page 1-7. If the provisioned value is supposed to be at or below the threshold value, then this synchronization reference signal quality is too low to be used as a BITS out reference. Select a different BITS out reference. See 323-1051-310, Provisioning BITS Out on page 1-13. If the provisioned value is above the threshold value, contact your next level of support or your Nortel Networks support group.
10	If the alarm does not clear, verify the quality level of the active synchronization reference.

If the synchronization level is	**Then**
above the provisioned threshold value	contact your next level of support or your Nortel Networks support group
equal or below the provisioned threshold value	verify the source of the active timing reference, repeat from step 7

—end—

Synchronization

EX1298p



Note: The BITS-timed head end node has a BITS In failure which is causing the network element to be internally timed (Stratum 3).

Legend

= Optical interface circuit pack

Procedure 5-109
TL1 Script file Failed

Probable cause

The network processor raises this alarm when loading of a TL1 script file or the committing of a TL1 script file 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
- use an account with level 3 or higher user privilege code (UPC)

Step	Action
1	Ensure you are logged in to the network processor. 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Ensure that the target network element is selected in the Navigation Tree.
3	Start a TL1 Command Builder session. 323-1059-302, Procedures for using the TL1 Command Builder on page 7-1.
4	Cancel the loading of the TL1 script file by entering `CMMT-TL1SCRPT-NE:[TID]::CTAG;`
5	Click Run Command.
6	Wait until a completed message is displayed in the Status area. You have completed this procedure.

—end—

Procedure 5-110
TL1 Script file Load in Progress

Probable cause

The network processor raises this standing condition alarm when it is in the process of loading a TL1 script file from a remote source. You can clear this alarm by committing the TL1 script file to a target network element, or cancel the loading command.

Impact

Minor, non-service-affecting (m, 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 the loading of the TL1 script file to the network processor.

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	Ensure you are logged in to the network processor. 323-1059-302, Procedures for logging in to a network processor on page 2-1.
2	Ensure that the target network element is selected in the Navigation Tree.
3	Start a TL1 Command Builder session. 323-1059-302, Procedures for using the TL1 Command Builder on page 7-1.
4	**If** you want to / **Then** go to commit the TL1 script file to a target network element — step 5 cancel the loading command — step 9
5	Wait until a completed message is displayed in the Status area for the LOAD-TL1SCRPT-NE command.
6	Commit the TL1 script file to the target network element by entering `CMMT-TL1SCRPT-NE:[TID]::CTAG;`
7	Click Run Command.
8	Wait until a completed message is displayed in the Status area. You have completed this procedure.

—continued—

Procedure 5-110 (continued)
TL1 Script file Load in Progress

Step	Action
9	Cancel the loading of the TL1 script file by entering `CMMT-TL1SCRPT-NE:[TID]::CTAG;`
10	Click Run Command.
11	Wait until a completed message is displayed in the Status area. You have completed this procedure.

—end—

Procedure 5-111
TOD Server has not responded to a request

Probable cause

The network processor and shelf processor raises this standing condition alarm whenever it cannot receive a response from one or more time of day (TOD) servers. This alarm is raised even if only one provisioned server is in an out of synchronization state or Unknown state. This alarm occurs on shelf processors or network processors.

This alarm is masked by the Unable to Synchronize TOD on page 5-257.

Impact

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

Note: This alarm is minor when time of day synchronization is active but one of the provisioned timing servers is invalid. This alarm is major when all of the timing servers are invalid.

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** this alarm occurs on	**Then** ensure that a
	a shelf processor	timing server is configured and valid on both the shelf processor and network processor. See 323-1059-302, Setting time of day servers on the network processors or network element on page 8-4. ***Note:*** Theprovisioned timing source of a shelf processor is normally obtained from the network processor. Therefore, the shelf processor must be within the span of control of the selected network processor.
	a network processor	timing server is configured and valid on the network processor. See 323-1059-302, Setting time of day servers on the network processors or network element on page 8-4.

—continued—

Procedure 5-111 (continued)
TOD Server has not responded to a request

Step	Action
2	Check connectivity to the NTP server.
3	Ensure that the time of day synchronization status is active (on) on both the network processor and shelf processor. 323-1059-302, Editing time of day synchronization parameters on the network processor or network element on page 8-2.
4	If the time on the NTP server has been recently adjusted, operate a time of day synchronization on both the network processor and shelf processor. See, 323-1059-302, Operating a time of day synchronization on the network processors or network element on page 8-6.
5	If any of the time of day parameters such as the offset threshold or polling periods have been adjusted, this alarm may clear by itself over time. If it does not clear, readjust the parameters. See 323-1059-302, Editing time of day synchronization parameters on the network processor or network element on page 8-2.
6	If the alarm does not clear, contact your next level of support or your Nortel Networks support group. You have completed this procedure. **—end—**

Procedure 5-112
TOD Threshold Exceeded

Probable cause

The network processor and shelf processor raises this event when the timing offset exceeds the value of the user provisionable offset threshold parameter. This event is an early warning and it is masked by the Unable to Synchronize TOD alarm or if the time-of-day feature is inactive.

Note: This alarm can also be raised during upgrades, backups and restores, and while the active synchronization is in progress. The lower the provisioned offset threshold parameter, the greater probability this alarm is raised for these reasons.

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	Ensure that the user-provisioned offset threshold value is correct. See 323-1059-302, Displaying time of day server details and parameters on page 8-7. ***Note:*** If any of the time of day parameters, were recently adjusted, this event will likely clear by itself over time, unless the maximum provisoned offset is exceeded.
2	Verify if the active alarms include TOD Threshold Exceeded on page 5-252 and Unable to Synchronize TOD on page 5-257. Clear the alarms according to the alarm clearing procedure.
3	If the time on the NTP server has been recently adjusted, operate a time of day synchronization on both the network processor and shelf processor. See 323-1059-302, Operating a time of day synchronization on the network processors or network element on page 8-6.

—continued—

Procedure 5-112 (continued)
TOD Threshold Exceeded

Step	Action
4	If the alarm does not clear, increase the offset threshold value and wait and see if this alarm clears. See 323-1059-302, Editing time of day synchronization parameters on the network processor or network element on page 8-2.
5	If the alarm does not clear, contact your next level of support or your Nortel Networks support group. You have completed this procedure. **—end—**

Procedure 5-113
Traffic Squelched

Probable cause

This alarm is raised when the network element has squelched traffic on one or more:

- STS or VT paths on an OC-48 facility
- STS paths on an OC-192 facility

The path alarm indication signal (AIS) is inserted into the affected incoming and outgoing STS or incoming VT paths.

One of the following conditions causes this alarm:

- node failure or node isolation
- ring segmentation

Node failure, node isolation or ring segmentation can be caused by two or more of the following conditions:

- fiber cut
- fiber pulled from the circuit pack
- circuit pack failure
- circuit pack pulled from the shelf
- any protection switch

When there is a node failure, node isolation, or ring segmentation, the ring attempts to restore as much traffic as possible through automatic protection switches.

Impact

Critical, service-affecting (C, SA) alarm

Requirements

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

—continued—

Procedure 5-113 (continued)
Traffic Squelched

Step	Action
1	Identify the circuit pack or circuit packs raising the alarm. See Identifying the circuit pack or facility that has raised an alarm on page 2-52. The circuit pack performing the traffic squelching is located adjacent to the failed span or node.
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	Once you have identified which node has failed or where the ring is segmented, you need to retrieve alarms from that node and look for: • an OCn Rx Loss of Signal alarm. The presence of this alarm can indicate a fiber cut. If the fibers have been cut, replace the fibers. If the fibers are not linked, connect them as required. • a Circuit pack failed alarm. See Circuit Pack Failed on page 4-57. • a Circuit pack missing alarm. See Circuit Pack Missing on page 4-74.
4	The nodes adjacent to the failed span or node are the switching nodes. Retrieve alarms for those nodes and look for: • automatic protection switch alarm. Verify the cause of the automatic protection switch. • Clear the alarms according to the applicable alarm clearing procedures in this document.

—end—

Procedure 5-114
Transport Data Recovery Failed

Probable cause

This alarm is raised when data is not recovered after a shelf processor replacement or removal. Data cannot be recovered properly if at least one of the transport circuit packs are running a higher software release than the shelf processor.

Impact

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

Note 1: Transport circuit packs are not visible during this alarm, but neighboring network elements can be seen. You may need to perform the upgrade from another network element that is running the correct release.

Note 2: SDCC is only available in slots 11 and 12 when the SPx is running a release lower than that of the cards in the shelf. If there are subtending network elements they are only seen after the SPx is upgraded to the correct release.

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)

Step	Action
1	Log in to the network element in the navigation tree. See 323-1059-302, Other login and logout related procedures on page 2-1.
2	Select Inventory List from the Configuration menu and verify the software releases on all the circuit packs on the shelf including the shelf processor.
3	Retrieve all active and disabled alarms and verify the alarm. See Retrieving active alarms for a network element on page 2-3.
4	Upgrade the shelf processor to match the release on the network element. See 323-1059-302, Procedures for provisioning data and software management on page 6-1. ***Note:*** Local transport circuit packs are not visible, but neighboring network elements are visible. Perform the upgrade from another network element that is running the correct load.
5	Ensure that the system is restored to its original state by retrieving all conditions and alarms. Clear all alarms using the appropriate alarm clearing procedure.

—end—

Procedure 5-115
Unable to Synchronize TOD

Probable cause

Time of day synchronization has two thresholds; a maximum threshold and an offset threshold. The maximum threshold is set by the system and its value is greater than the user provisionable offset threshold. The network processor and shelf processor raise the Unable to Synchronize TOD alarm when the maximum threshold is exceeded. For example, the maximum threshold could be exceeded if the NP is removed from the shelf and then reinserted after several minutes have passed. The maximum threshold for the shelf processor is 8 seconds. The maximum threshold for the network processor is 30 minutes.

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
- use an account with level 3 or higher user privilege code (UPC)

Step	Action
1	If the time on the NTP server has been recently adjusted, operate a time of day synchronization on both the network processor and shelf processor. See, 323-1059-302, Operating a time of day synchronization on the network processors or network element on page 8-6.
2	If the alarm does not clear, contact your next level of support or your Nortel Networks support group. You have completed this procedure. **—end—**

Procedure 5-116
Unsupported Service - Path Trace

Probable cause

This alarm is raised during a reconfiguration from DS3x3 or DS3x12e to DS3x12 if path trace is provisioned on the DS3x3 or DS3x12e mapper.

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	Disable the path trace monitoring for all ports. See 323-1059-520, Enabling or disabling path trace messages on page 2-7.
2	Select Active Alarms from the Faults list.
3	Ensure that the Unsupported Service - Path Trace alarm has cleared.
4	If the alarm does not clear, contact your next level of support of your Nortel Networks support group.

—end—

Procedure 5-117
Upgrade Failed

Probable cause

This alarm is raised when a failure occurs during a manual or automatic upgrade of circuit packs.

Impact

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

Step	Action
1	Contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-118
Upgrade Failed Slot n

Probable cause

This alarm is raised when the upgrade process of a circuit pack fails.

The upgrade process can fail for the following reasons:

- when unsupported equipment is inserted into the shelf

  Note: For example, a single port DS3 or EC-1 circuit pack that is specific to an OPTera Metro 3300/3400 shelf is inserted into an OPTera Metro 3500 shelf.

- a faulty circuit pack
- interruption of the upgrade process
- the circuit pack is not properly seated in the shelf

  Note: Follow this procedure to clear any Upgrade Failed Slot n alarms, where $2 \leq n \leq 14$ or $19 \leq n \leq 56$ for OPTera Metro 3500.

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 5-11, and in *Installation,* 323-1059-201

—continued—

Procedure 5-118 (continued)
Upgrade Failed Slot n

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	Verify the PEC of the alarmed circuit pack to make sure it is a circuit pack that is supported on an OPTera Metro 3500 shelf. See 323-1059-302, Displaying shelf inventory information on page 5-8 and *OPTera Metro 3500 Multiservice Platform, Rel. 12.0 Planning and Ordering Guide*, NTRN10AM. If it is an unsupported circuit pack, replace it with a circuit pack of the correct PEC for the shelf. See Procedures for equipment replacement on page 3-1. If it is a supported circuit pack go to the next step.
3	Perform a WARM restart of the circuit pack. See Restarting a circuit pack on page 2-45.
4	Verify if the circuit pack upgrade was successful. If the circuit pack upgrade was successful, you have completed this procedure. If the circuit pack upgrade was not successful, go to the next step.
5	Reseat the circuit pack in the correct slot. See Reseating a circuit pack on page 3-4.
6	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-119
Upgrade in Progress

Probable cause

This alarm is raised while a system upgrade is in progress after the initialization of the load upgrade. 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 5-120
Virtual Circuit Failure

Probable cause

This alarm is raised in the following two circumstances:

- on the network processor while waiting for X.25-associated TL1 resources to be recovered

  Note: The alarm clears when the resources are recovered.

- on one or more circuits when you edit the virtual circuit, delete a PVC, or edit the upper layer X.25

Impact

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

Note: The affected circuit is not available for an X.25 call while the Virtual Circuit Failure alarm is raised.

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 5-11, and in *Installation,* 323-1059-201

Step	Action
1	Log into the network processor. See 323-1059-302, Procedures for logging in to a network processor on page 2-1. ***Note:*** If an network processor restart occurred, you cannot access the network processor until the network processor database is released.
2	If you log in to a network processor using an account with a level 5 UPC, you automatically log into all the network elements in the network processor span of control.Reset the appropriate circuit(s): • To reset a switched virtual circuit (SVC), go to step 3. • To reset a permanent virtual circuit (PVC), go to step 4.

—continued—

Procedure 5-120 (continued)
Virtual Circuit Failure

Step	Action
3	To reset a switched virtual circuit (SVC), modify the upper layer X.25 parameters. See 323-1059-520, Editing X.25 parameters on page 3-6 or Editing the SVC parameter values on page 3-14.
4	To reset a permanent virtual circuit (PVC), modify the PVC parameters. See 323-1059-520, Editing the PVC parameter values on page 3-12.
5	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-121
VT Rx AIS

Probable cause

This alarm is raised when the network element detects a VT AIS (alarm indication signal) in the SONET overhead. The VT 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) if the VT mapping is byte synchronous for this DS1
- circuit pack failed (tributary) at the far end
- STS-1 faults at a pass-through network element
- 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 in a UPSR

Note: The alarm status is minor because it is a secondary alarm. Another fault caused the remote terminal to send this signal. The problem that prevents the transmission of the signal raised a separate 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
- ensure that no EC1 Rx AIS, 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 5-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

—continued—

Procedure 5-121 (continued)
VT 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 16
3	Verify if there are alarms of higher order from the alarm hierarchy. See Alarm hierarchies on page 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
4	Retrieve alarms to determine if the VT 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 network connection information to identify the receive and transmit sites of the alarmed signal: **If** the network element you identified / **Then** at the remote end is not an OPTera Metro 3500 network element — refer to the appropriate procedure in the Nortel Networks technical publications (NTPs) for that product, then You have completed this procedure. at the remote end is an OPTera Metro 3500 network element — step 7 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, then You have completed this procedure.
7	Log in to the alarmed remote network element. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
8	Retrieve all alarms from the transmit end.
9	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.

—continued—

Procedure 5-121 (continued)
VT Rx AIS

Step	Action
10	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.
11	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.
12	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.
13	If the alarm does not clear, verify the facility state at the transmit end, if applicable. If the 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.
14	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.
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	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
17	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 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 5-122
VT Rx Excessive BIP Error Rate

Probable cause

This alarm is raised when the received VT1.5 is degraded to the point where it is unusable.

One of the following conditions causes this alarm:

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

Impact

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

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 5-11, and in *Installation,* 323-1059-201

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

—continued—

Procedure 5-122 (continued)
VT Rx Excessive BIP Error Rate

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 5-9. 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.
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.

—continued—

Procedure 5-122 (continued)
VT Rx Excessive BIP Error Rate

Step	Action
9	Measure the receive power using an optical power meter. If the power is below the receiver sensitivity for this circuit pack, perform the following steps for VT 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. **e.** If the power is below the launch power (minimum), replace the optical interface 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. **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.
10	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.
11	If the alarm does not clear, replace the optical interface circuit pack raising the alarm.
12	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-123
VT Rx Loss of Pointer

Probable cause

This alarm is raised when the network element detects an invalid pointer sequence in the VT line overhead.

One of the following conditions causes this alarm:

- improper network synchronization
- connection rate mismatch (for example, VT1.5 connects to STS-1)

Impact

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

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 5-11, and in *Installation,* 323-1059-201
- use an account with level 1 or higher user privilege code (UPC)

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. See Alarm hierarchies on page 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
4	Retrieve alarms to determine if the VT 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.

—continued—

Procedure 5-123 (continued)
VT Rx Loss of Pointer

Step	Action
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.
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. See Alarm hierarchies on page 5-9. • If there is VT RX LOP, 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 whole 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 cross-connect for that facility. • If the signal contains VT loss of 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 no VT loss of pointer, go to the next step.
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.

—continued—

Procedure 5-123 (continued)
VT Rx Loss of Pointer

Step	Action
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 AIS. See Replacing the EC-1x3 or EC-1x12 circuit pack on page 3-32.
20	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-124
VT Rx RFI

Probable cause

This alarm is raised when an optical interface circuit pack, DSM DS1x84 TM mapper, or DS3VTx12 circuit pack receives a signal with a remote fault indicator (RFI) sent in the SONET overhead. This alarm is raised when an alarm of higher order is raised on the remote network element or the far end detects a VT signal failure condition.

On the OPTera Metro 3500 shelf, this alarm is raised against the DS1 or DS3VTx12 circuit pack (source of the VT signal), and not on the corresponding optical interface circuit pack.

On the DSM, this alarm is raised against the optical interface circuit pack (and not against the corresponding DS1 facility on the DSM).

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 network 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 5-11, and in *Installation,* 323-1059-201

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.

—continued—

Procedure 5-124 (continued)
VT Rx RFI

Step	Action
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.
4	Retrieve alarms from the transmit end.
5	Look for an alarm message for the 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 5-125
VT Rx Signal Degrade

Probable cause

This alarm is raised when the received signal is degraded significantly.

One of the following conditions causes this alarm:

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

Impact

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

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 signal degrade alarms, signal failure or excessive BIP error rate alarms on the system
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201

CAUTION
Risk of outage
This procedure assumes that no signal degrade alarms are active, and only a few VTs are degraded. Performing this procedure before clearing any signal degrade or signal failure alarms or excessive BIP error rate alarms is not effective and can cause an outage.

—continued—

Procedure 5-125 (continued)
VT Rx Signal Degrade

Step	Action
1	Retrieve alarms from the network element. See Retrieving active alarms for a network element on page 2-3.
2	Retrieve the line signal degrade threshold (SDTH) and compare the SDTH with the network diagram. See 323-1059-311, Retrieving the line SDTH of an optical facility on page 1-36. Edit the SDTH, as required. See 323-1059-311, Editing the line SDTH of an optical facility on page 1-37.
3	Verify if there are alarms of higher order from the alarm hierarchy. See Alarm hierarchies on page 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
4	Retrieve alarms to determine if the Rx excessive BIP error rate 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 the receive sites of the alarmed signal.
7	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.
8	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
9	**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.

—continued—

Procedure 5-125 (continued)
VT Rx Signal Degrade

Step	Action
10	Measure the receive power using an optical power meter. If the power is below the receiver sensitivity for this circuit pack, perform the following steps for VT 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 optical interface 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. **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, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-126
VT Rx Signal Label Mismatch

Probable cause

This alarm is raised when the network element detects that the signal label in the VT overhead does not match the expected signal label. The received VT signal label is not equal to Async VT or VT Unequipped.

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

On the OPTera Metro 3500 shelf, this alarm is raised against the DS1 or DS3VTx12 circuit pack (source of the VT signal), and not on the corresponding optical interface circuit pack.

On the DSM, this alarm is raised against the optical interface circuit pack (and not against the corresponding DS1 facility on the DSM).

Impact

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

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

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 5-11, and in *Installation,* 323-1059-201

—continued—

Procedure 5-126 (continued)
VT 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 5-9. 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 network connection information to identify the receive and transmit sites of the alarmed signal:

If the network element you identified	**Then**
at the remote end is not an OPTera Metro 3500 network element	refer to the appropriate procedure in the Nortel Networks technical publications (NTPs) for that product You have completed this procedure.
at the remote end is an OPTera Metro 3500 network element	step 6
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 You have completed this procedure.

6	Log in to each of the network elements on the VT1.5 path. See 323-1059-302, Procedures for logging in to a network element on page 2-1.
7	Retrieve all cross-connects from the remote network element. See 323-1059-320, Retrieving end-to-end connections on page 1-2.
8	Verify the VT1.5 connection information for the entire path to ensure that it is provisioned correctly. An error could have been made when entering the connections.
9	Retrieve the alarms from the remote network element to determine if the alarm cleared.
10	Verify that the DS1 provisioning at the far-end network element is correct and it matches the near-end network element. See 323-1059-350, Retrieving equipment and facility details on page 2-2 and Editing DS1, DS3, EC-1, 2x100BT-P2P or GE/FC SFP facility signal attributes on page 2-28.
11	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-127
VT Rx Unequipped

Probable cause

This alarm is raised when the network element detects an unequipped signal label in the VT path overhead.

One of the following conditions causes this alarm:

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

Impact

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

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)
- use an account with level 1 or higher user privilege code (UPC)
- observe all safety requirements described in Safety requirements on page 5-11, and in *Installation,* 323-1059-201

Note: 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.

—continued—

Procedure 5-127 (continued)
VT 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 DS3VTx12 — step 3 OCn — step 5 EC-1x3 or EC-1x12 — step 17
3	Verify if the alarm has been raised because of a software loopback.
4	**If** the alarm is … **Then** caused by a software loopback — this alarm clears automatically once the software loopback is released and the facility is placed back in-service. You have completed this procedure. not caused by a software loopback — If the alarm does not clear, contact your next level of support or your Nortel Networks support group.
5	Verify if there are alarms of higher order from the alarm hierarchy. See Alarm hierarchies on page 5-9. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
6	Retrieve alarms to determine if the Rx Unequipped alarm cleared.
7	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.
8	Use the optical fiber connection information to identify the transmit and receive ends for the alarmed signal:

—continued—

Procedure 5-127 (continued)
VT Rx Unequipped

Step	Action	
9	**If** the network element you identified	**Then**
	at the remote end is not an OPTera Metro 3500 network element	refer to the appropriate procedure in the Nortel Networks technical publications (NTPs) for that product You have completed this procedure.
	at the remote end is an OPTera Metro 3500 network element	go to step 10
	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 You have completed this procedure.
10	Log in to each of the network elements on the VT1.5 path. See 323-1059-302, Procedures for logging in to a network element on page 2-1.	
11	Retrieve all cross-connects from the remote network element. See 323-1059-320, Retrieving end-to-end connections on page 1-2.	
12	Verify cross-connects for the entire path to ensure that 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.	
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 to ensure that the DS1 facility is in service. 323-1059-350, Changing a facility state to In Service (IS) on page 2-26.	
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	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 5-127 (continued)
VT Rx Unequipped

Step	Action
18	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 unequipped, 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 unequipped, go to the next step.
19	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.
20	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
21	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.
22	If the alarm does not clear, contact your next level of support or your Nortel Networks support group.

—end—

Procedure 5-128
VTX Shelf ID Mismatch Detected

Probable cause

This alarm is raised following a shelf processor replacement when it is not clear whether the transport cards or shelf processor have shelf mastership. This mastership will indicate whether the shelf processor should retrieve the shelf provisioning data from the transport cards or deliver the provisioning data to the transport cards.

Note: No circuit packs should be reseated or replaced.

Impact

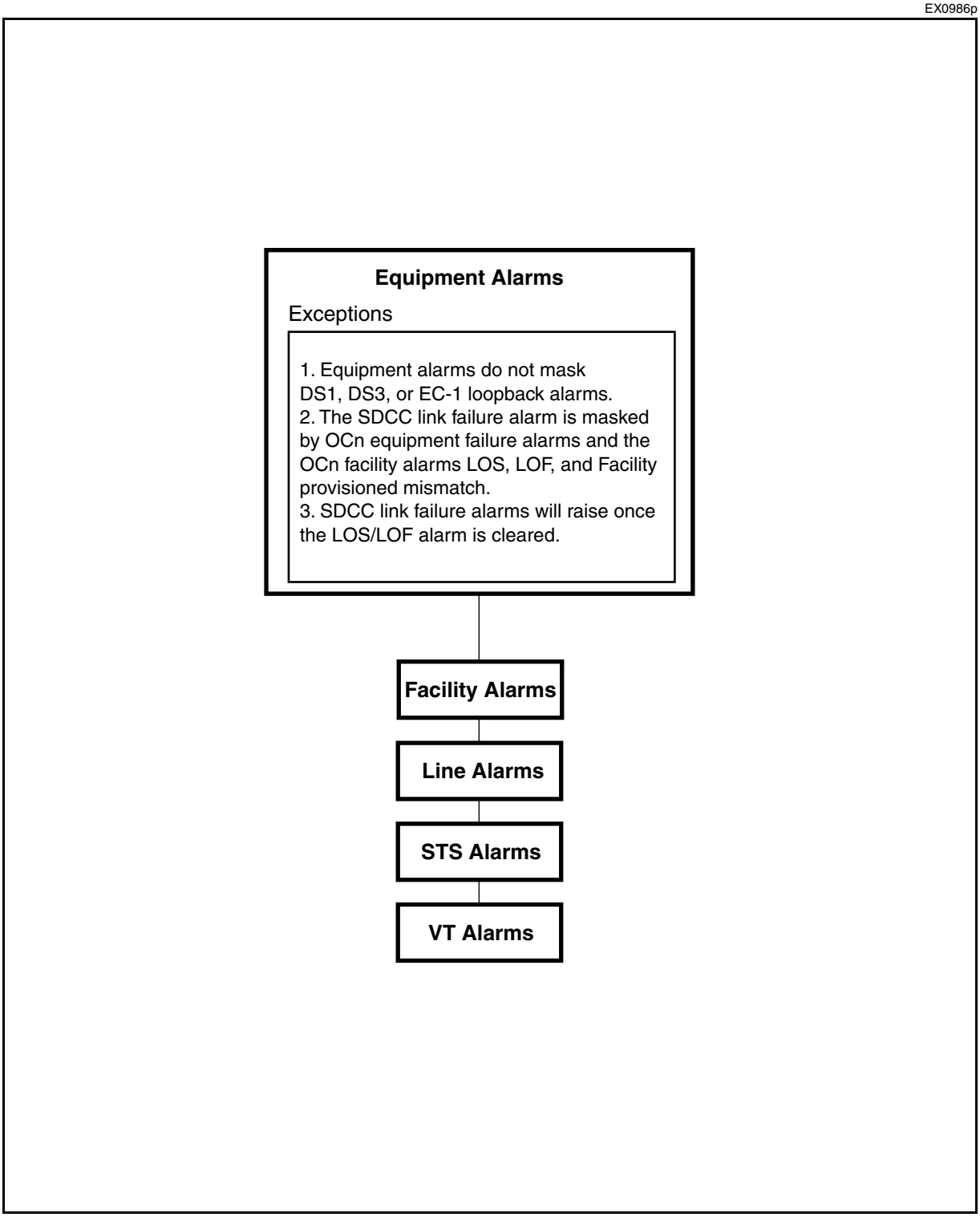
Major, non-service-affecting (M, NSA) alarm

Step	Action
1	Contact your next level of support or your Nortel Networks support group.

—end—

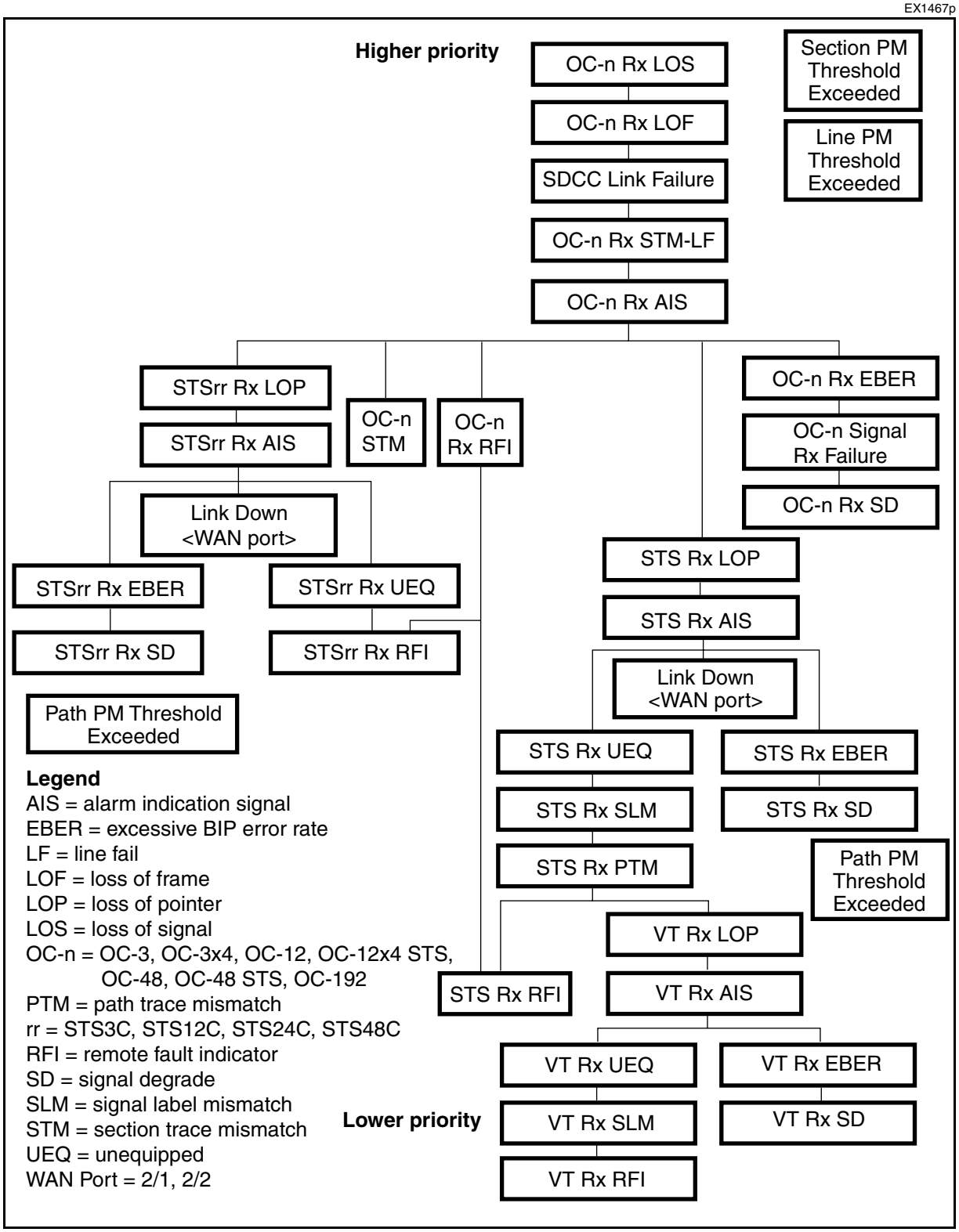
Overall alarm hierarchy

EX0986p



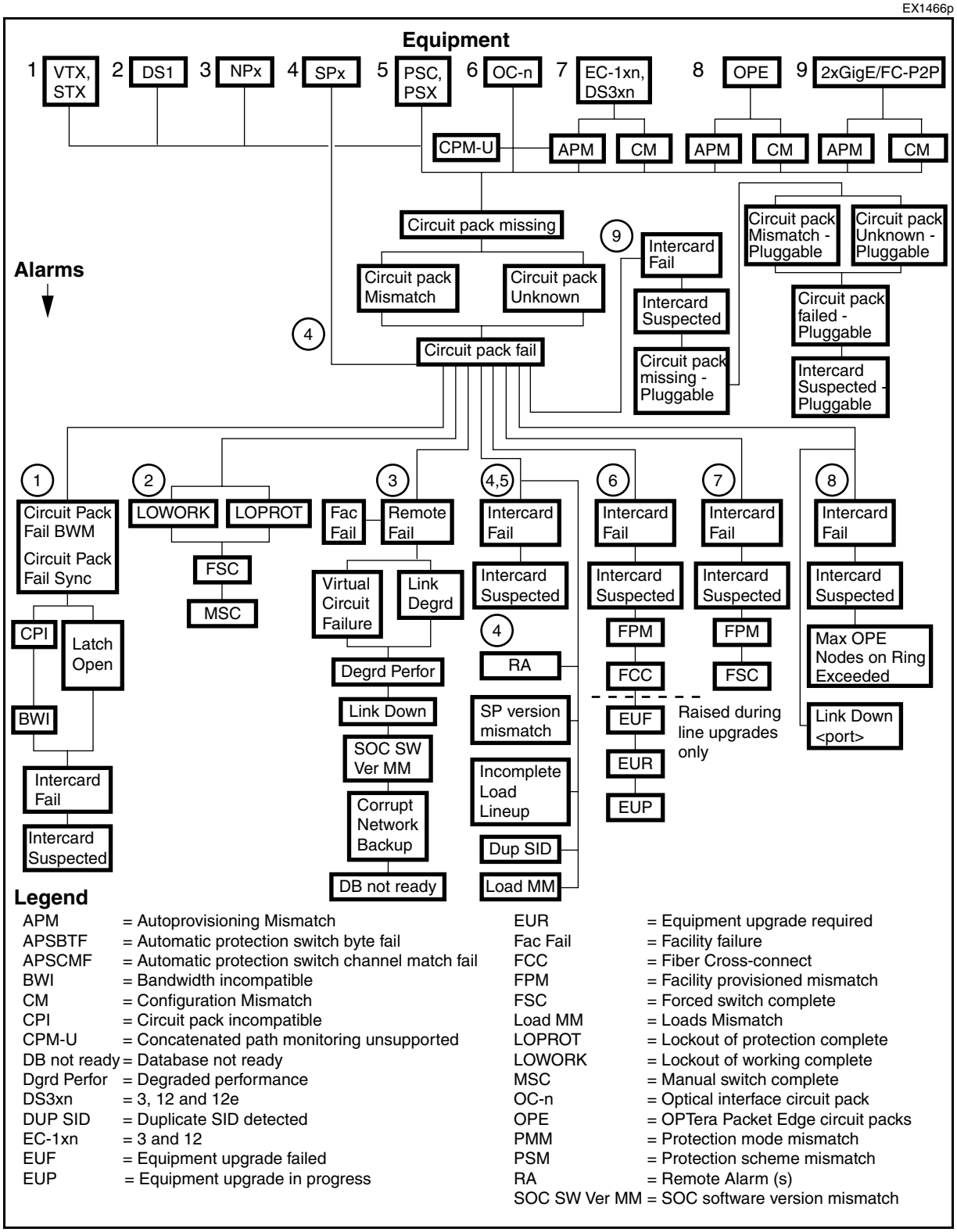
OC-n facility alarm hierarchy

EX1467p



Equipment alarm hierarchy

EX1466p

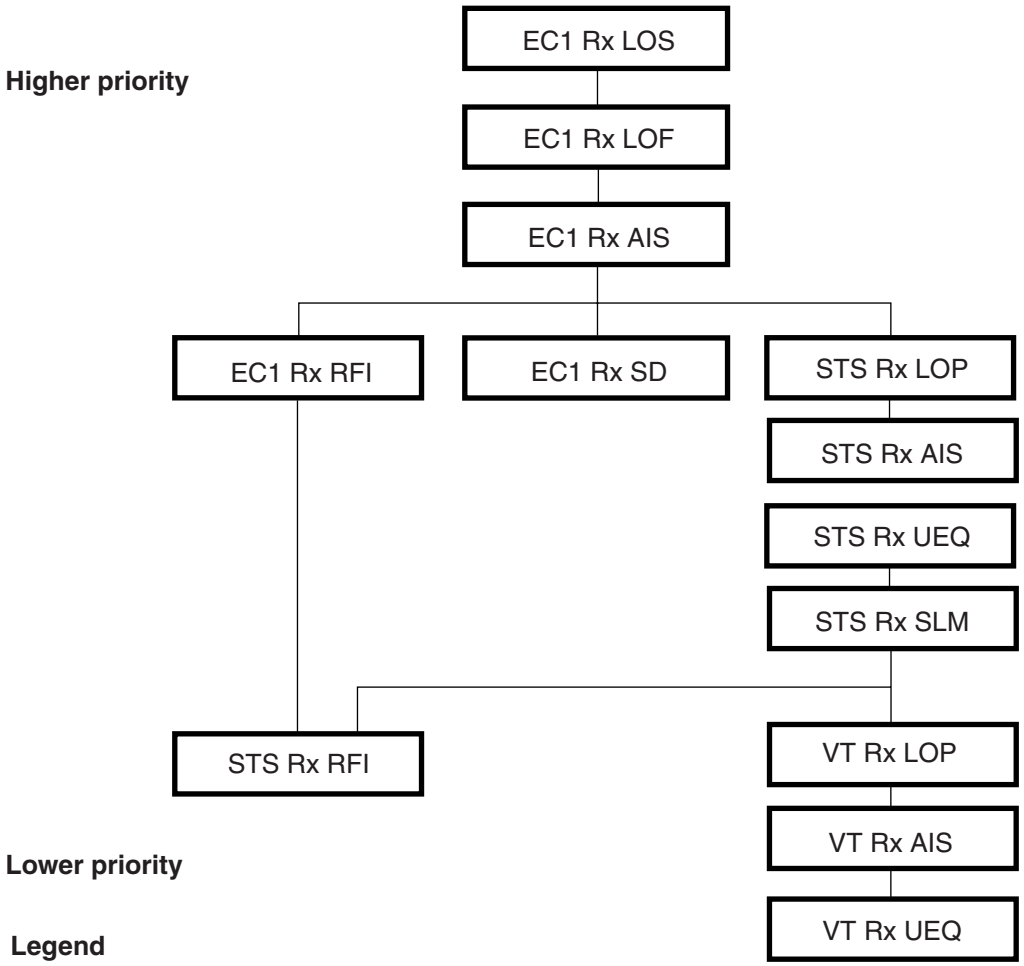


Legend

APM	= Autoprovisioning Mismatch
APSBTF	= Automatic protection switch byte fail
APSCMF	= Automatic protection switch channel match fail
BWI	= Bandwidth incompatible
CM	= Configuration Mismatch
CPI	= Circuit pack incompatible
CPM-U	= Concatenated path monitoring unsupported
DB not ready	= Database not ready
Dgrd Perfor	= Degraded performance
DS3xn	= 3, 12 and 12e
DUP SID	= Duplicate SID detected
EC-1xn	= 3 and 12
EUF	= Equipment upgrade failed
EUP	= Equipment upgrade in progress
EUR	= Equipment upgrade required
Fac Fail	= Facility failure
FCC	= Fiber Cross-connect
FPM	= Facility provisioned mismatch
FSC	= Forced switch complete
Load MM	= Loads Mismatch
LOPROT	= Lockout of protection complete
LOWORK	= Lockout of working complete
MSC	= Manual switch complete
OC-n	= Optical interface circuit pack
OPE	= OPTera Packet Edge circuit packs
PMM	= Protection mode mismatch
PSM	= Protection scheme mismatch
RA	= Remote Alarm (s)
SOC SW Ver MM	= SOC software version mismatch

EC-1 facility alarm hierarchy

EX1215p

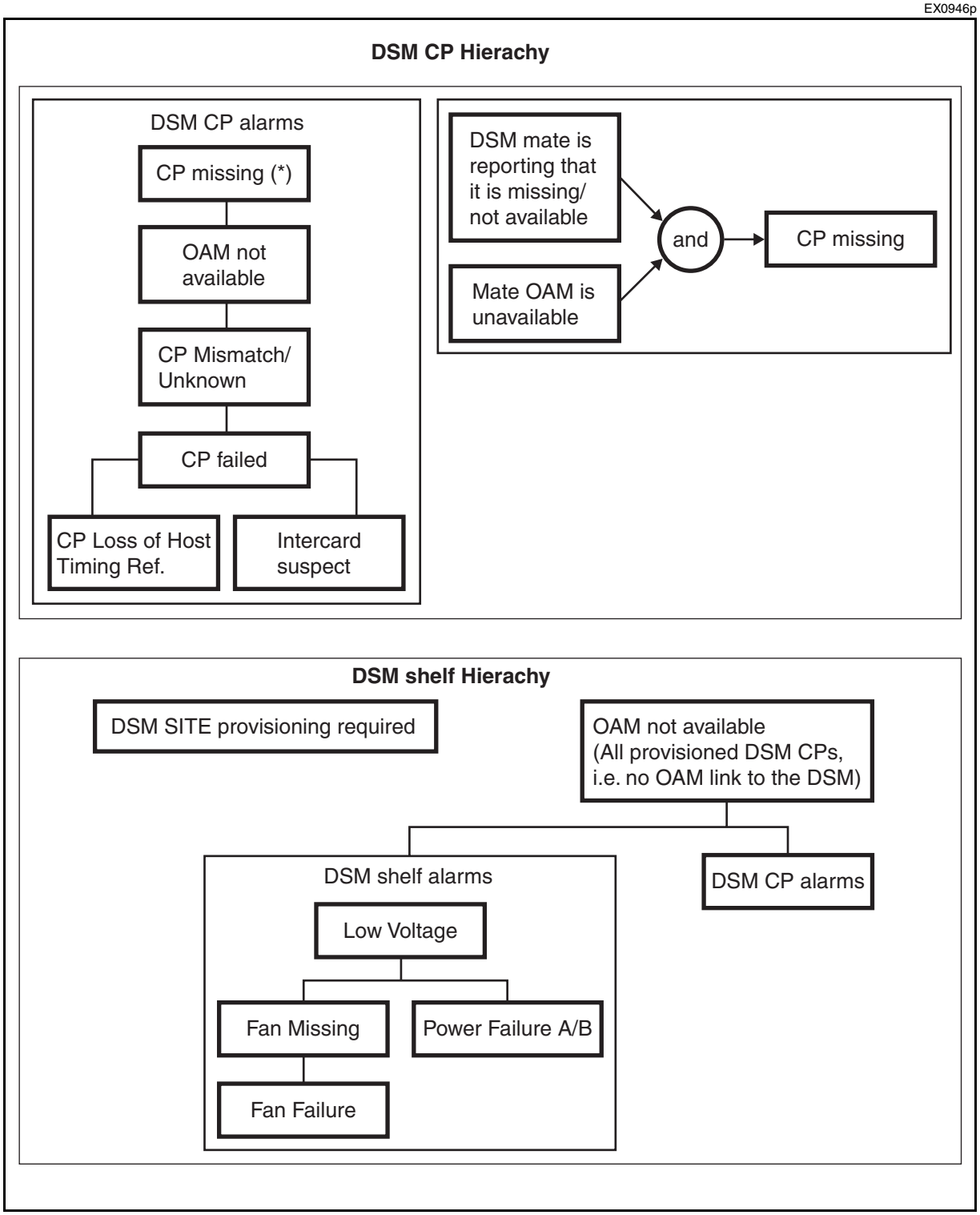


Legend

AIS	= alarm indication signal
LOF	= loss of frame
LOP	= loss of pointer
LOS	= loss of signal
RFI	= remote fault indicator
SD	= signal degrade
SLM	= signal label mismatch
UEQ	= unequipped

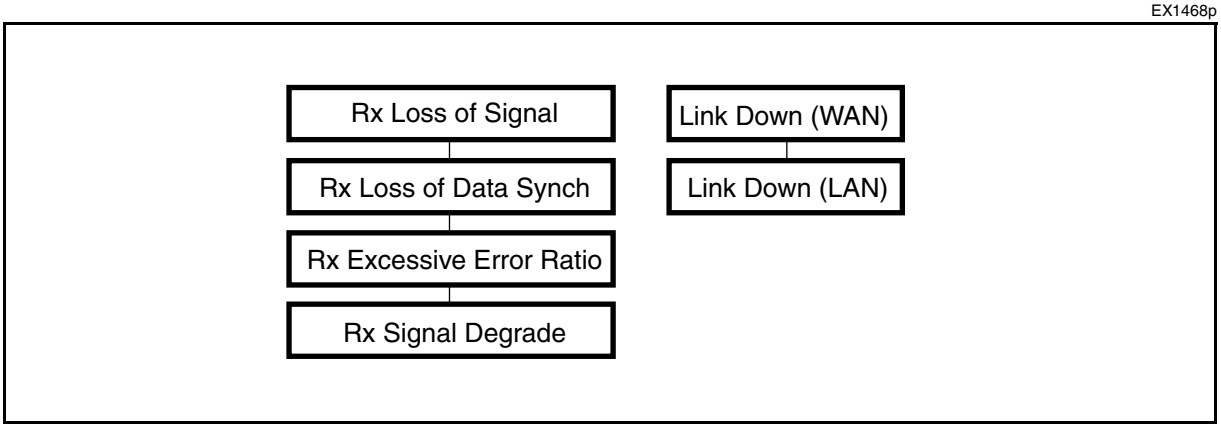
DS1 service module alarm hierarchy

EX0946p



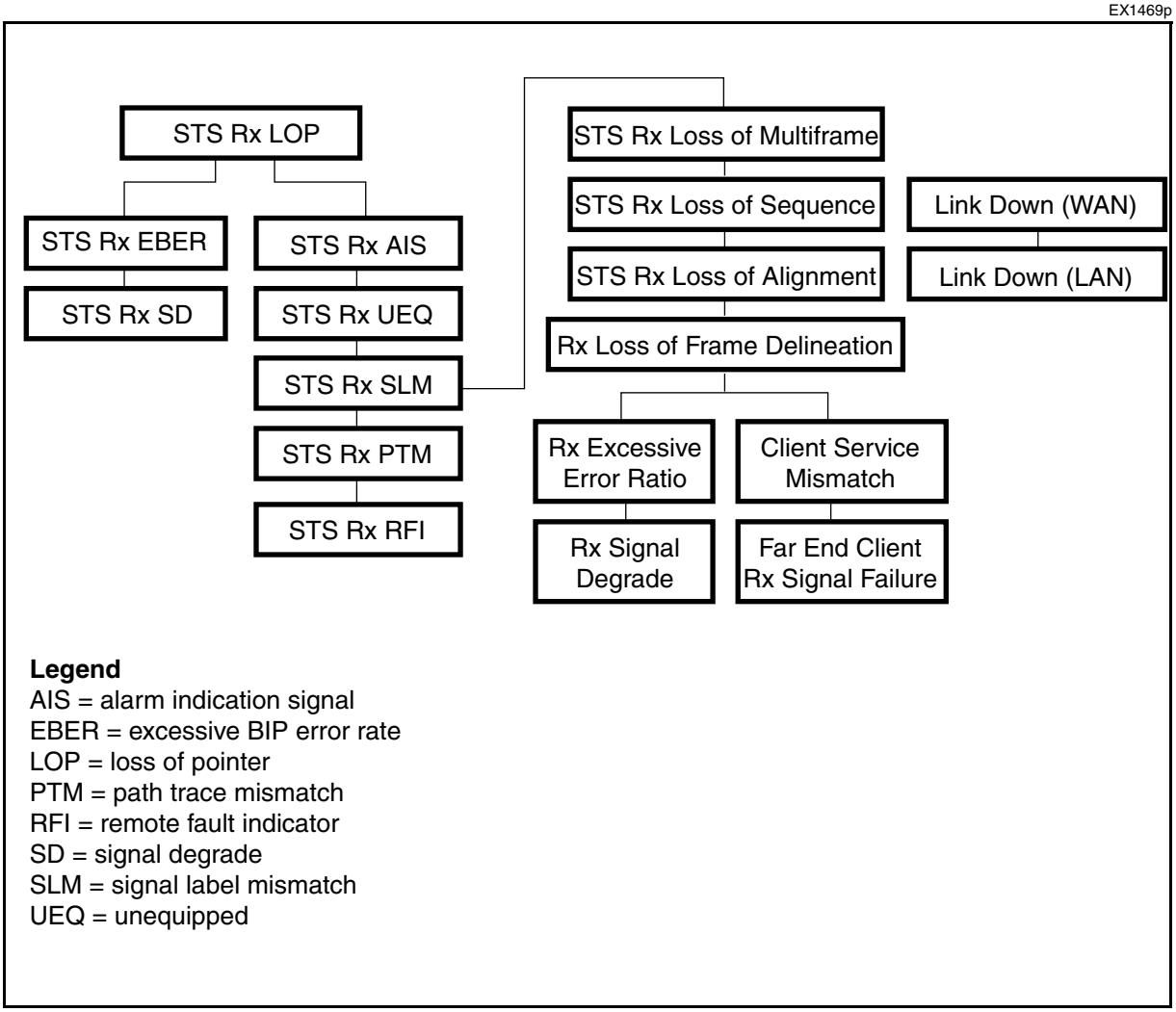
2xGigE/FC-P2P circuit pack ingress LAN port alarm hierarchy

EX1468p



2xGigE/FC-P2P circuit pack egress WAN port alarm hierarchy

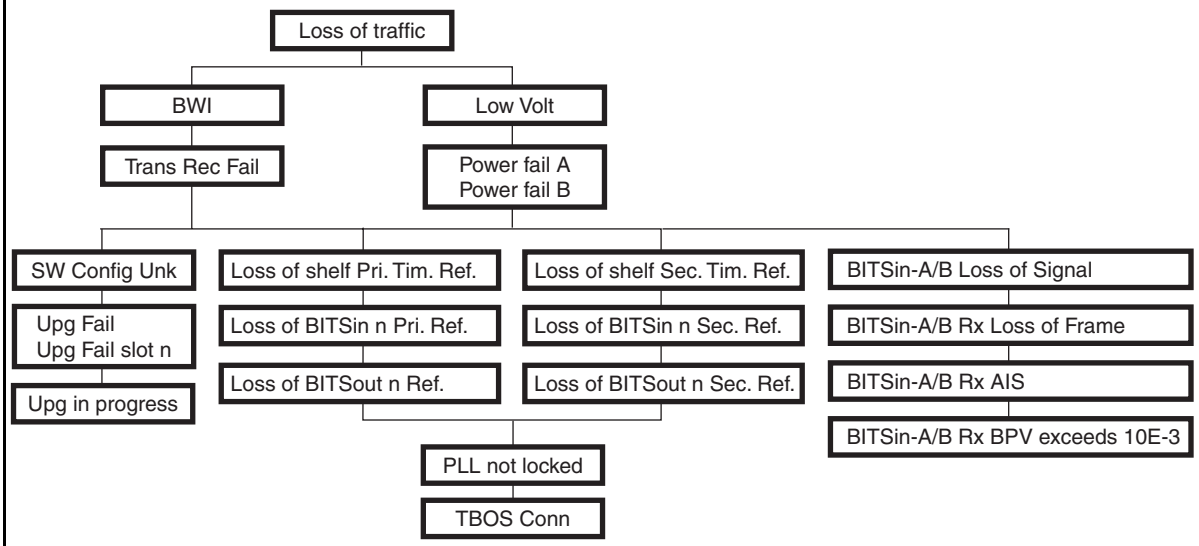
EX1469p



Legend
AIS = alarm indication signal
EBER = excessive BIP error rate
LOP = loss of pointer
PTM = path trace mismatch
RFI = remote fault indicator
SD = signal degrade
SLM = signal label mismatch
UEQ = unequipped

Shelf equipment alarm hierarchy

EX0947p



Legend

BITSin-A/B Rx AIS	= BITSin-A Rx AIS or BITSin-B Rx AIS
BITSin-A/B Rx BPV exceeds 10E-3	= BITSin-A Rx BPV exceeds 10E-3 or BITSin-B Rx BPV exceeds 10E-3
BITSin-A/B Rx Loss of Frame	= BITSin-A Rx loss of frame or BITSin-B Rx loss of frame
BITSin-A/B Rx Loss of Signal	= BITSin-A Rx loss of signal or BITSin-B Rx loss of signal
BWI	= Bandwidth incompatible
Loss of BITS in n Pri. Ref.	= Loss of BITS in n primary reference
Loss of BITS in n Sec. Ref.	= Loss of BITS in n Secondary reference
Loss of BITSout n Pri. Ref.	= Loss of BITSout n primary reference
Loss of BITSout n Sec. Ref.	= Loss of BITSout n Secondary reference
Loss of shelf Pri. Tim. Ref.	= Loss of shelf primary timing reference
Loss of shelf Sec. Tim. Ref.	= Loss of shelf Secondary timing reference
Low Volt	= Low Voltage
PLL not locked	= PLL not locked to timing reference
Power fail A	= Power failure A
Power fail B	= Power failure B
SW Config Unk	= Software Configuration Unknown
TBOS Conn	= TBOS Connection failure
Trans Rec Fail	= Transport Recovery Fail
Upg Fail	= Upgrade Failed
Upg Fail slot n	= Upgrade Failed slot n

Terms and conditions

Completion of a purchase agreement is required prior to purchasing OPTera Metro 3500 products and/or services. Contact one of the following:

- your Nortel Networks sales person
- telephone: Suzanne Calton (972) 685-2888
- email CONTMGNT@nortelnetworks.com

Statement of Conditions

Portions of the code in this software may be Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994 The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3 All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4 Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,

PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of the code in this software may be Copyright © 1988 Juniper Networks, Inc. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of the code in this software may be Copyright © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the “RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as “derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided “as is” without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software. $FreeBSD: src/lib/libmd/md5c.c,v 1.11 1999/12/29 05:04:20 peter Exp $This code is the same as the code published by RSA Inc. It has been edited for clarity and style only.

Nortel Networks

OPTera Metro 3500 Multiservice Platform

Alarm and Trouble Clearing—Part 2 of 2

Copyright © 2000–2003 Nortel Networks, All Rights Reserved

The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose the information only to its employees with a need to know, and shall protect the information, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

Nortel Networks, the Nortel Networks logo, the Globemark, OPTera, and Preside are trademarks of Nortel Networks.

323-1059-543
Standard Release 12.0 Issue 1
November 2003
Printed in Canada