

Preside Multiservice Data Manager

# Proxy Alarms

Reference Guide

241-6001-501



---

Preside Multiservice Data Manager

# **Proxy Alarms**

## Reference Guide

---

Publication: 241-6001-501

Document status: Standard

Document version: 14.3RSUP

Document date: December 2003

---

Copyright © 2003 Nortel Networks.

All Rights Reserved.

Printed in Canada

NORTEL, NORTEL NETWORKS, the globemark design, the NORTEL NETWORKS corporate logo, PRESIDE, DPN, and PASSPORT are trademarks of Nortel Networks. OPENVIEW is a trademark of Hewlett-Packard Company.

---



## Publication history

---

### December 2003

14.3RSUP Standard  
Commercial availability



---

# Contents

---

## **About this document** **9**

Who should read this document and why 9

What you need to know 9

How this document is organized 10

Text conventions 10

Related documents 11

---

## **Chapter 1**

### **Introducing proxy alarms** **13**

MDM proxy alarms 13

Turning off proxy alarms 13

---

## **Chapter 2**

### **Preside Multiservice Data Manager (MDM) alarms** **15**



## About this document

---

The following topics are discussed in this section:

- “Who should read this document and why” (page 9)
- “What you need to know” (page 9)
- “How this document is organized” (page 10)
- “Text conventions” (page 10)
- “Related documents” (page 11)

### Who should read this document and why

This guide is for systems administrators and network operators who are responsible for Preside Multiservice Data Manager (MDM) fault management. This guide describes the alarm codes coming from various MDM servers and proxy agents.

### What you need to know

This document assumes that you have a knowledge of

- the elements in your network, for example, DPN and Passport devices
- the diagnostics of the switches being managed by the Preside Multiservice Data Manager (MDM)
- network fault management

## How this document is organized

241-6001-501 *Preside MDM Proxy Alarms Reference Guide* contains the following sections:

- “Introducing proxy alarms” (page 13) describes the alarms and their alarm codes.
- “Preside Multiservice Data Manager (MDM) alarms” (page 15) contains a sequential listing of all Preside Multiservice Data Manager (MDM) proxy alarms.

## Text conventions

This document uses the following text conventions:

- `nonproportional spaced plain type`  
Nonproportional spaced plain type represents system generated text or text that appears on your screen.
- **`nonproportional spaced bold type`**  
Nonproportional spaced bold type represents words that you should type or that you should select on the screen.
- *italics*  
Statements that appear in italics in a procedure explain the results of a particular step and appear immediately following the step.  
  
Words that appear in italics in text are for naming.
- `[optional_parameter]`  
Words in square brackets represent optional parameters. The command can be entered with or without the words in the square brackets.
- `<general_term>`  
Words in angle brackets represent variables which are to be replaced with specific values.

- UPPERCASE,lowercase

In the Preside Multiservice Data Manager (MDM), uppercase and lowercase letters that appear in UNIX commands and parameters must be matched exactly. The system matches upper and lowercase characters differently.

- |

This symbol separates items from which you may select one; for example, ON|OFF indicates that you may specify ON or OFF. If you do not make a choice, a default ON is assumed.

- ...

Three dots in a command indicate that the parameter may be repeated more than once in succession.

The term absolute pathname refers to the full specification of a path starting from the root directory. Absolute pathnames always begin with the slash (/) symbol. A relative pathname takes the current directory as its starting point, and starts with any alphanumeric character (other than /).

## Related documents

See the following documents for related information:

- 241-6001-303 *Preside MDM Administrator Guide*



# Chapter 1

## Introducing proxy alarms

---

This chapter describes the Preside Multiservice Data Manager (MDM) proxy alarms: where they are generated from and how to turn off the alarm stream.

### MDM proxy alarms

The Preside Multiservice Data Manager (MDM) proxy alarms come from various MDM servers and proxy agents. A proxy alarm is an alarm that is generated by MDM in place of an alarm or an event from a switch, such as a trap.

MDM generates these proxy alarms and injects them into the main alarm stream along with switch-generated alarms. The MDM alarms come from the following:

- FMIP Management Data Router (FMDR)
- Inbound Management Data Router (IMDR)
- Inbound Application Programming Interface (IAPI)
- SNMP Management Data Router (SMDR)
- DPN Management Data Router (DMDR)
- MDM Server Manager (SVM)

### Turning off proxy alarms

To turn off the proxy alarm stream, refer to the sections on configuring the file `/op/MagellanNMS/cfg/DMDRAAlarmExcep.cfg` and an additional configuration for alarm exception handling in 241-6001-310 *Preside MDM Server Reference Guide*.



---

## Chapter 2

# Preside Multiservice Data Manager (MDM) alarms

---

### 3010 0000

Component	Severity	Status
MDM/<w/s name> APP <application name>	major/cleared	set/clear

#### Legend

<w/s name> is the name of the workstation generating the error

<application name> is the MDM server on the MDM workstation that has stopped or restarted

#### Details

This alarm is generated by the MDM Server Manager (SVM). It is issued when the key MDM server application is stopped and restarted.

This alarm contains COMMENT text information that describes the name of the server application. In the SET alarm, the COMMENT text contains the signal # that caused the MDM application to stop. In the CLEAR alarm, the COMMENT text contains the current number of restart times, out of the total restarted times allowed for this application.

#### Remedial action

Verify that no one on the workstation terminated the application. If the application restarts on its own (as it is supposed to do) there is no problem. However, if the application cannot restart, review the failure code and refer to the MDM documentation for more information.

## 3010 0700

<b>Component</b>	<b>Severity</b>	<b>Status</b>
NMS/<w/s name> GROUP <Passport group name>	warning	msg

### Legend

<w/s name> is the name of the workstation generating the error

<Passport group name> is the name of the unreachable Passport group

### Details

This alarm is issued when the MDM host cannot reach the indicated Passport group to perform a TODchangeover command.

### Remedial action

Verify that the Passport group is included in the HGDS.cfg file and that this Passport group name was specified using capital letters. Verify that the userID and password for this Passport group are valid. Execute the command again using the correct parameters.

## 3010 0701

<b>Component</b>	<b>Severity</b>	<b>Status</b>
NMS/<w/s name> PP <Passport nodeID/nodename>	warning	msg

### Legend

<w/s name> is the name of the workstation generating the error

<Passport nodeID/nodename> is the nodeID or nodename of the unreachable Passport

### Details

This alarm is issued when the MDM host cannot reach the indicated Passport to query the current time offset.

### Remedial action

Verify that the specified Passport is active and accessible. Verify that the Passport userID and password for this Passport are valid. If the userID or password for the indicated Passport are different than those used by the other Passports in the Passport group, have the userID and password added or changed on the affected Passport. If the Passport was unavailable during the execution of the TODchangeover, execute the command again after the Passport has returned to service.

## 3010 0702

<b>Component</b>	<b>Severity</b>	<b>Status</b>
NMS/<w/s name> PP <Passport nodeID/nodename>	warning	msg

### **Legend**

<w/s name> is the name of the workstation generating the error

<Passport nodeID/nodename> is the nodeID or nodename of the unreachable Passport

### **Details**

This alarm is issued when the MDM host cannot reach the indicated Passport to set the current time offset.

### **Remedial action**

Verify that the specified Passport is active and accessible. Verify that the Passport userID and password for this Passport are valid. If the userID or password for the indicated Passport are different than those used by the other Passports in the Passport group, have the userID and password added or changed on the affected Passport. If the Passport was unavailable during the execution of the TODchangeover, execute the command again after the Passport has returned to service.

## 3010 0703

<b>Component</b>	<b>Severity</b>	<b>Status</b>
NMS/<w/s name> APPL TODCHANGEOVER	warning	msg

### **Legend**

<w/s name> is the name of the workstation generating the error

### **Details**

This alarm is issued when the TODchangeover command failed due to incorrectly specified parameters.

### **Remedial action**

Check the log file associated with this application to determine which parameter was incorrectly specified. Execute the command again with the correct parameters.

## 3011 0001

<b>Component</b>	<b>Severity</b>	<b>Status</b>
NMS/<w/s name> APP <application_name>	critical/cleared	set/clear

### **Legend**

<w/s name> is the name of the workstation generating the error

<application\_name> is the application name.

### **Details**

This alarm is generated by MDM workstation surveillance. It is issued when the application is stopped by signal 15. This alarm contains COMMENT text information that identifies the application. When the alarm clears, the COMMENT text information indicates that the application is restarted.

### **Remedial action**

Contact the MDM administrator and the workstation administrator and apprise them of the resource alarm.

## 3011 0100

<b>Component</b>	<b>Severity</b>	<b>Status</b>
NMS/<w/s name> DISK <id>	critical/major/ minor/cleared	set/clear

### **Legend**

<w/s name> is the name of the workstation generating the error

<id> is disk volume identifier

### **Details**

This alarm is generated by MDM workstation surveillance. It is issued when disk resource usage exceeds pre-defined thresholds. This alarm contains COMMENT text information that identifies the percentage of resources used. When the alarm clears, the COMMENT text information indicates that resource usage is normal.

The default threshold values are:

- 70% of resource used: MINOR
- 80% of resource used: MAJOR
- 90% of resource used: CRITICAL

Threshold values can be redefined through the `sfm_config` script.

**Remedial action**

Contact the MDM administrator and the workstation administrator and apprise them of the resource alarm.

**3011 0200**

<b>Component</b>	<b>Severity</b>	<b>Status</b>
NMS/<w/s name> CPU <id>	critical/major/ minor/cleared	set/clear

**Legend**

<w/s name> is the name of the workstation generating the error

<id> is CPU identifier

**Details**

This alarm is generated by MDM workstation surveillance. It is issued when CPU resource usage exceeds pre-defined thresholds. This alarm contains COMMENT text information that identifies the percentage of resources used. When the alarm clears, the COMMENT text information indicates that resource usage is normal.

The default threshold values are:

- 70% of resource used: MINOR
- 80% of resource used: MAJOR
- 90% of resource used: CRITICAL

Threshold values can be redefined through the `sfm_config` script.

**Remedial action**

Contact the MDM administrator and the workstation administrator and apprise them of the resource alarm.

**3011 0300**

<b>Component</b>	<b>Severity</b>	<b>Status</b>
NMS/<w/s name> MEMORY	critical/major/ minor/cleared	set/clear

**Legend**

<w/s name> is the name of the workstation generating the error

### Details

This alarm is generated by MDM workstation surveillance. It is issued when memory resource usage exceeds pre-defined thresholds. This alarm contains COMMENT text information that identifies the percentage of resources used. When the alarm clears, the COMMENT text information indicates that resource usage is normal.

The default threshold values are:

- 70% of resource used: MINOR
- 80% of resource used: MAJOR
- 90% of resource used: CRITICAL

Threshold values can be redefined through the sfm\_config script.

### Remedial action

Contact the MDM administrator and the workstation administrator and apprise them of the resource alarm.

## 3011 0401

Component	Severity	Status
NMS/<w/s name> PORT <ip_addr>	major/cleared	set/clear

### Legend

<w/s name> is the name of the workstation generating the error

<ip\_addr> is the IP address assigned to the Ethernet port.

### Details

This alarm is generated by MDM workstation surveillance. It is issued when the port at the indicated IP address is out of service. This alarm contains COMMENT text information that identifies the component. When the alarm clears, the COMMENT text information indicates that the component is back in service.

There are no threshold values that trigger this alarm.

### Remedial action

Contact the MDM administrator and the workstation administrator and apprise them of the resource alarm.

## 3011 0501

<b>Component</b>	<b>Severity</b>	<b>Status</b>
NMS/<w/s name> CONNECTION <ip_addr>	critical/cleared	set/clear

### Legend

<w/s name> is the name of the workstation generating the error

<ip\_addr> is the IP address of the remote workstation.

### Details

This alarm is generated by MDM workstation surveillance. It is issued when the connection to either a remote peer MDM workstation or a common device is lost. This alarm contains COMMENT text information that identifies the remote peer MDM workstation or the device. When the alarm clears, the COMMENT text indicates that the connection to the peer MDM workstation or the device has been re-established and redundancy is restored.

There are no threshold values that trigger this alarm.

### Remedial action

Contact the MDM administrator and the workstation administrator and apprise them of the resource alarm.

## 3011 0600

<b>Component</b>	<b>Severity</b>	<b>Status</b>
NMS/<w/s name> SDS <logical disk name>	critical/cleared	set/clear

### Legend

<w/s name> is the name of the workstation generating the error

<logical disk name> is the logical disk name used by SDS.

### Details

This alarm is generated by MDM workstation surveillance. It is issued when the redundancy of the Solstice Disk Suite (SDS) disk mirroring system fails. This alarm contains comment text that identifies the file system that is jeopardized. When the alarm clears, the comment text indicates that the redundancy of the file system is restored.

There are no threshold values that trigger this alarm. This alarm is generated only by the machine that has SDS installed.

### Remedial action

Contact the MDM administrator and the workstation administrator and apprise them of the resource alarm.

## 3011 0700

<b>Component</b>	<b>Severity</b>	<b>Status</b>
NMS/<hostname>	critical/major/ cleared	set/clear

### Legend

<hostname> is the name of the MDM host generating the error.

### Details

This alarm occurs during the 30-day temporary license period after MDM is installed. The alarm indicates that the temporary license is about to expire. A major alarm occurs when 6 to 10 days remain on the temporary license period. A critical alarm occurs when 5 days or less remain. You cannot regenerate another temporary license key.

### Remedial action

Contact the Nortel Networks account representative for your MDM permanent license key. Install the permanent license key.

## 50xx 00xx

<b>Component</b>	<b>Severity</b>	<b>Status</b>
<xx> /<component id>	major/cleared	set/clear

### Legend

<xx> is the device class that you are managing

<component id> is the name of the component

### Details

For customers who decide to use the SNMP integrator, they are recommended to use a range of alarms to indicate an alarm arriving from their system.

This range is from 50xx 0000 to 50xx 0200. Since we have no control over what the customers use therefore we suggest that customer build their own alarms document and include it into the document so that their alarms can be found. We suggest that customers choose a different value for each type of device.

### Remedial action

Not applicable

## 50xx 01xx

<b>Component</b>	<b>Severity</b>	<b>Status</b>
<xx> /<component id>	major/cleared	set/clear

### **Legend**

<xx> is the device class that you are managing

<component id> is the name of the component

### **Details**

For customers who decide to use the SNMP integrator, they are recommended to use a range of alarms to indicate an alarm arriving from their system.

This range is from 50xx 0000 to 50xx 0200. Since we have no control over what the customers use therefore we suggest that customer build their own alarms document and include it into the document so that their alarms can be found. We suggest that customers choose a different value for each type of device.

### **Remedial action**

Not applicable

## 50xx 02xx

<b>Component</b>	<b>Severity</b>	<b>Status</b>
<xx> /<component id>	major/cleared	set/clear

### **Legend**

<xx> is the device class that you are managing

<component id> is the name of the component

### **Details**

For customers who decide to use the SNMP integrator, they are recommended to use a range of alarms to indicate an alarm arriving from their system.

This range is from 50xx 0000 to 50xx 0200. Since we have no control over what the customers use therefore we suggest that customer build their own alarms document and include it into the document so that their alarms can be found. We suggest that customers choose a different value for each type of device.

### **Remedial action**

Not applicable

## 5004 0001

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Network	major	set

### **Legend**

none

### **Details**

The SNMP Integrator has received an invalid SNMP poll response. Operator data contains in the first 4-bytes, the source code location, and in the next 4-bytes, further information to be used for debugging.

Comment text contains the IP address of where the poll response is originated.

### **Remedial action**

none

## 5004 0002

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Network	major	set

### **Legend**

none

### **Details**

The SNMP Integrator has received an invalid SNMP trap message.

Operator data contains in the first 4-bytes, the source code location, and in the next 4-bytes, further information to be used for debugging.

Comment text contains the Internet address of where the poll response is originated.

### **Remedial action**

none

## 5004 0003

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

A software error has occurred.

Operator data contains in the first 4-bytes, the source code location, and in the next 4-bytes, further information to be used for debugging.

### **Remedial action**

none

## 5004 0004

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Engineering	major	set

### **Legend**

none

### **Details**

An overrun condition is encountered during polling. It occurs when the actual poll interval device exceeds the poll interval defined in the Network Element configuration file. The probable cause is due to improper engineering of the polling parameters: time-out, number of retry, and poll interval.

Operator data contains in the first 4-bytes, the source code location, and in the next 4-bytes, the actual poll interval.

Comment text contains: Polling frequency overrun.

### **Remedial action**

none

## 5004 0005

Component	Severity	Status
Engineering	major	set

### Legend

none

### Details

The SNMP GET response message indicates that there is an error for the requested MIB variable.

Operator data contains in the first 4-bytes, the source code location, and in the next 4-bytes, the error code as follows:

1. tooBig
2. noSuchName
3. badValue
4. readOnly
5. genErr

Consult Internet Standard RFC 1157, *Simple Network Management Protocol (SNMP)* for more meanings of this error status.

Comment text contains the Internet address of where the poll response message is originated and the symbolic name of the MIB variable.

### Remedial action

none

## 5004 0006

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Engineering	major	set

### **Legend**

none

### **Details**

An overrun condition is encountered during PING polling. It occurs when the actual poll interval device exceeds the poll interval defined in the Network Element configuration file. The probable cause is due to improper engineering of the polling parameters: timeout, number of retry, and poll interval.

Operator data contains in the first 4-bytes, the source code location, and in the next 4-bytes, the actual poll interval.

Comment text contains: Polling frequency overrun.

### **Remedial action**

none

## 5004 0007

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Network	major	set

### **Legend**

none

### **Details**

The SNMP trap message received contains a MIB variable that the SNMP Integrator cannot translate into a symbolic form.

Operator data contains the MIB variable in a numeric format. For example, the MIB variable 1.2.3.4 will be shown as 01020304.

### **Remedial action**

none

## 5004 0100

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The RTR X25 link named in this alarm has gone down. Check whether the device has been shut down on purpose. If not, check the physical connection first, then the network path to this device.

### **Remedial action**

none

## 5004 0101

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The RTR X25 link named in this alarm has gone into testing mode. The interface should be considered unavailable for operational data.

### **Remedial action**

none

## 5004 0102

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The RTR FR link named in this alarm has gone down. Check whether the device has been shut down on purpose. If not, check the physical connection first, then the network path to this device.

### **Remedial action**

none

## 5004 0103

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The RTR FR link named in this alarm has gone into testing mode. The interface should be considered unavailable for operational data.

### **Remedial action**

none

## 5004 0104

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The RTR EPO link named in this alarm has gone down. Check whether the device has been shut down on purpose. If not, check the physical connection first, then the network path to this device.

### **Remedial action**

none

## 5004 0105

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The RTR EPO link named in this alarm has gone into testing mode. The interface should be considered unavailable for operational data.

### **Remedial action**

none

## 5004 0106

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The HUB EPO link named in this alarm has gone down. Check whether the device has been shut down on purpose. If not, check the physical connection first, then the network path to this device.

### **Remedial action**

none

## 5004 0107

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The HUB EPO link named in this alarm has gone into testing mode. The interface should be considered unavailable for operational data.

### **Remedial action**

none

## 5004 0108

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The BR EPO link named in this alarm has gone down. Check whether the device has been shut down on purpose. If not, check the physical connection first, then the network path to this device.

### **Remedial action**

none

## 5004 0109

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The BR EPO link named in this alarm has gone into testing mode. The interface should be considered unavailable for operational data.

### **Remedial action**

none

## 5004 0110

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The SLAN SBR B\_EPO link named in this alarm has gone down. Check whether the device has been shut down on purpose. If not, check the physical connection first, then the network path to this device.

### **Remedial action**

none

## 5004 0111

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The SLAN SBR B\_EPO link named in this alarm has gone into testing mode. The interface should be considered unavailable for operational data.

### **Remedial action**

none

## 5004 0112

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The SLAN SHUB H\_EPO link named in this alarm has gone down. Check whether the device has been shut down on purpose. If not, check the physical connection first, then the network path to this device.

### **Remedial action**

none

## 5004 0113

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The SLAN SHUB H\_EPO link named in this alarm has gone into testing mode. The interface should be considered unavailable for operational data.

### **Remedial action**

none

## 5004 0114

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The SLAN PRT P\_EPO link named in this alarm has gone down. Check whether the device has been shut down on purpose. If not, check the physical connection first, then the network path to this device.

### **Remedial action**

none

## 5004 0115

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The SLAN PRT P\_EPO link named in this alarm has gone into testing mode. The interface should be considered unavailable for operational data.

### **Remedial action**

none

## 5004 0116

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The SLAN FS F\_EPO link named in this alarm has gone down. Check whether the device has been shut down on purpose. If not, check the physical connection first, then the network path to this device.

### **Remedial action**

none

## 5004 0117

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The SLAN FS F\_EPO link named in this alarm has gone into testing mode. The interface should be considered unavailable for operational data.

### **Remedial action**

none

## 5004 0118

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The SLAN WS W\_EPO link named in this alarm has gone down. Check whether the device has been shut down on purpose. If not, check the physical connection first, then the network path to this device.

### **Remedial action**

none

## 5004 0119

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The SLAN WS W\_EPO link named in this alarm has gone into testing mode. The interface should be considered unavailable for operational data.

### **Remedial action**

none

## 5004 0120

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The SLAN SRTR R\_X25 link named in this alarm has gone down. Check whether the device has been shut down on purpose. If not, check the physical connection first, then the network path to this device.

### **Remedial action**

none

## 5004 0121

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The SLAN SRTR R\_X25 link named in this alarm has gone into testing mode. The interface should be considered unavailable for operational data.

### **Remedial action**

none

## 5004 0122

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The SLAN SRTR R\_EPO link named in this alarm has gone down. Check whether the device has been shut down on purpose. If not, check the physical connection first, then the network path to this device.

### **Remedial action**

none

## 5004 0123

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The SLAN SRTR R\_EPO link named in this alarm has gone into testing mode. The interface should be considered unavailable for operational data.

### **Remedial action**

none

## 5004 0124

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The SLAN SRTR R\_FR link named in this alarm has gone down. Check whether the device has been shut down on purpose. If not, check the physical connection first, then the network path to this device.

### **Remedial action**

none

## 5004 0125

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The SLAN SRTR R\_FR link named in this alarm has gone into testing mode. The interface should be considered unavailable for operational data.

### **Remedial action**

none

## 5004 0126

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The ERTR S\_X25 link named in this alarm has gone down. Check whether the device has been shut down on purpose. If not, check the physical connection first, then the network path to this device.

### **Remedial action**

none

## 5004 0127

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The ERTR S\_X25 link named in this alarm has gone into testing mode. The interface should be considered unavailable for operational data.

### **Remedial action**

none

## 5004 0128

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The ERTR S\_FR link named in this alarm has gone down. Check whether the device has been shut down on purpose. If not, check the physical connection first, then the network path to this device.

### **Remedial action**

none

## 5004 0129

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The ERTR S\_FR link named in this alarm has gone into testing mode. The interface should be considered unavailable for operational data.

### **Remedial action**

none

## 5004 0130

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The ERTR EPO link named in this alarm has gone down. Check whether the device has been shut down on purpose. If not, check the physical connection first, then the network path to this device.

### **Remedial action**

none

## 5004 0131

<b>Component</b>	<b>Severity</b>	<b>Status</b>
Software	major	set

### **Legend**

none

### **Details**

The ERTR EPO link named in this alarm has gone into testing mode. The interface should be considered unavailable for operational data.

### **Remedial action**

none

## 50048888

<b>Component</b>	<b>Severity</b>	<b>Status</b>
<deviceType>/<deviceName>	major	set

### Legend

<deviceType> is the device type in ASCII (e.g. RTR)

<deviceName> is the device name in ASCII

### Details

The device is not responding to a PING command by the SNMP Integrator within the specified time period.

### Remedial action

Verify that the device is UP and/or reachable from the MDM workstation that is running the SNMP Integrator. If the device is UP and reachable, verify that the TIMEOUT value for this device, as defined in the Network Element file, is large enough to allow the device to respond..

## 5004FFFF

<b>Component</b>	<b>Severity</b>	<b>Status</b>
<deviceType>/<deviceName>	cleared	clear

### Legend

<deviceType> is the device type in ASCII (e.g. RTR)

<deviceName> is the device name in ASCII

### Details

The device has responded to an initial PING command by the SNMP Integrator, or a sysReset trap has been received by the SNMP Integrator.

### Remedial action

none

## 600X XXXX

<b>Component</b>	<b>Severity</b>	<b>Status</b>
NMS/<host> MDP/<application>	critical/major/ warning	message

### Legend

<host> is the name of the Management Data Provider (MDP) host  
 <application> is the name of the MDP process that generated the alarm

### Details

The indicated MDP process has encountered an error. The COMMENT text information indicates the alarm cause.

### Remedial action

The last 5-digits of the alarm fault code refers to a specific log message. Refer to the Log Messages section of 241-6001-309 *Preside MDM Management Data Provider User Guide* for an explanation of the message.

## A0XX XXXX

<b>Component</b>	<b>Severity</b>	<b>Status</b>
<xx> /<component id>	major/cleared	set/clear

### Legend

<xx> is the device class that you are managing  
 <component id> is the name of the component

### Details

For customers who decide to use the Inbound alarm and status Application Programming Interface (I-API) or Injected Management Data Router (IMDR) to inject alarms into MDM, they are recommended to use this range of alarms to indicate an alarm arriving from their system.

This range is from A000 0000 to A0FF FFFF. Customers can build their own alarms document and include it into this document so that their alarms can be found.

We recommend that the xx of A0xx 0000 be used to signify the device type to which the alarm refers. This will allow for better identification of the device type that failed.

In addition the xxxx of A000 xxxx be used to signify the specific failure.

Please refer to the specific documentation for details on the alarm.

### Remedial action

Refer to the product-specific documentation for fault correction steps.

## B000 BXXX

Component	Severity	Status
<xx> /<component id>	major/cleared	set/clear

### Legend

<xx> is the device class that you are managing

<component id> is the name of the component

### Details

For custom development, for example, for Meridian view.

Please refer to the specific documentation for details on the alarm.

### Remedial action

Refer to the product-specific documentation for fault correction steps.

## CDXX XXXX

### Legend

CD means customer-defined

XX XXXX is the value that you assign to an alarm fault code

**Note:** The first two numbers (<xx>) should match the device type value for the device being managed.

### Details

This alarm code is a template for the customer to use to define alarms. The SNMP Surveillance Adapter allows you to create alarm codes and descriptions in the MDM tool. See the section on adding a description for a new alarm code in the 241-6001-011 *Preside MDM Fault Management User Guide*.

## 0999 0001

<b>Component</b>	<b>Severity</b>	<b>Status</b>
<deviceType>/<deviceName>	critical/cleared	set/clear

### **Alarm type**

equipment

### **Probable cause**

equipment failure

### **Legend**

<deviceType> is the network device

<deviceName> is the name assigned to this device in your network

### **Details**

When status is set, the MDM network management workstation has lost its IP connection to the indicated network device. The cause of the failure is a problem with the communications links connecting the MDM network management workstation and the network device or device failure on the remote end.

When the status is clear, connectivity has been restored.

### **Remedial action**

Check the communication link connecting the MDM network management workstation and the network device. Also ensure that the network device has not failed. If you cannot detect a problem in the communication link, the physical link, or the remote-end device, and the problem persists, contact your Nortel Networks representative.

**0999 0002**

<b>Component</b>	<b>Severity</b>	<b>Status</b>
<deviceType>/<deviceName>	critical/cleared	set/clear

**Alarm type**

operator

**Probable cause**

unexpected information

**Legend**

<deviceType> is the network device

<deviceName> is the name assigned to this device in your network

**Details**

When status is set, the system object ID (sysOID) polled from the network device does not have the value expected. This situation can be caused by IP address duplication or incorrect information given to IP discovery.

When status is clear, the expected device type (or sysOID) has been found when polled from the device.

**Remedial action**

Determine if the IP address specified in the alarm comment text is duplicated in the network and verify the information given to IP discovery.

## 0999 0003

<b>Component</b>	<b>Severity</b>	<b>Status</b>
<deviceType>/<deviceName>	critical/warning/ cleared	set/clear

### **Alarm type**

operator

### **Probable cause**

unexpected information

### **Legend**

<deviceType> is the network device

<deviceName> is the name assigned to this device in your network

### **Details**

When status is set, the polled hardware identification <hardware ID> has changed. IP address duplication or a device replacement can cause this state. If the device name has not changed, it is assumed that a faulty device has been replaced by a new one. The new hardware identification is accepted, and the Warning severity is used. If the device name has also changed, it is assumed that is it due to IP address duplication. The Critical severity is used and subsequent polling results are ignored until the problem is resolved.

When status is clear, the expected hardware identification <hardware ID> has been found when polled from the device.

### **Remedial action**

For the CRITICAL SET alarm, determine if the IP address specified in the alarm comment text is duplicated in the network. For the WARNING SET alarm, no action is required.

**0999 0004**

<b>Component</b>	<b>Severity</b>	<b>Status</b>
<deviceType>/<deviceName>	major/cleared	set/clear

**Alarm type**

operator

**Probable cause**

duplicate information

**Legend**

<deviceType> is the network device

<deviceName> is the name assigned to this device in your network

**Details**

When the status is set, a new name assigned to a device duplicates a name already assigned to another device of the same type; the name change is rejected and the alarm is raised against the old name.

When the status is clear, the problem has been resolved.

**Remedial action**

Change the name of the device so that it does not duplicate the name of any other device of the same type.

## 0999 0010

<b>Component</b>	<b>Severity</b>	<b>Status</b>
PM/<component id>	major/cleared	set/clear

### **Legend**

<component id> is the name of any DPN component that generates status records

### **Details**

The state of the component has been changed due to a status record received from the network. When the status of the alarm is a set, it means that the status record indicated that the component is down, and there are no corresponding active alarms (generated by the switch) on that component to indicate that it is down. Therefore MDM created a proxy alarm to replace the missing alarm. MDM will mark the component Out of service.

When the status of the alarm is a clear, it means that the status record indicated that the component is up, and there were active alarms on that component to indicate that it is down. Therefore MDM generates a proxy alarm to replace the missing clear. MDM will mark the component Inservice.

The comment text of this alarm contains information on the status record that was received that triggered MDM to create the proxy alarm.

### **Remedial action**

This alarm is issued either because the status record was received before the alarm issued by the switch, which would put the component in the proper state (and the proxy alarm would be cleared when the real alarm is received) or because the alarm issued by the switch has been lost.

Treat proxy alarms as you would treat regular alarms and use them in debugging network problems.

## 0999 0011

<b>Component</b>	<b>Severity</b>	<b>Status</b>
xx/<component id>	major/cleared	set/clear

### **Legend**

xx is the device type managed by IMDR

<component id> is the name of a component managed by IMDR

### **Details**

The alarm generated by IMDR for an SNMP component is inconsistent with traps received from the network. This can happen, for example, if an SNMP poll produces a state change notification without receiving a corresponding trap from the network.

When the status of the alarm produced by IMDR is a set, it means that the Poll response indicates that the component is down, but there are no corresponding active alarms (generated by the switch) on that component to indicate that it is down. Therefore MDM creates a proxy alarm to replace the missing alarm. MDM marks the component Out of service.

When the status of the alarm is a clear, it means that the Poll response indicates that the component is up, but there are active alarms on that component to indicate that it is down. Therefore MDM generates a proxy alarm to replace the missing clear. MDM marks the component Inservice.

The comment text of this alarm contains information on the state notification that was received and triggered MDM to create the proxy alarm.

### **Remedial action**

This alarm is issued either because the state notification was received before the trap was issued by the switch, which would put the component in the proper state (and the proxy alarm would be cleared when the real trap is received) or because the trap issued by the switch has been lost or the switch never generated a trap.

Treat proxy alarms as you would treat regular alarms and use them in debugging network problems.

## 0999 0012

<b>Component</b>	<b>Severity</b>	<b>Status</b>
EM/<component id>	major/cleared	set/clear

### **Legend**

<component id> is the name of any PP component generating SCNs

### **Details**

The state of the component has been changed due to a state change notification (SCN) received from the network. When the status of the alarm is a set, it means that the SCN indicated that the component is down, and there are no corresponding active alarms (generated by the switch) on that component to indicate that it is down. Therefore MDM created a proxy alarm to replace the missing alarm. MDM will mark the component Out of service.

When the status of the alarm is a clear, it means that the SCN indicated that the component is up, and there were active alarms on that component to indicate that it is down. Therefore MDM generates a proxy alarm to replace the missing clear. MDM will mark the component Inservice.

The comment text of this alarm contains information on the SCN that was received that triggered MDM to create the proxy alarm.

### **Remedial action**

This alarm is issued either because the SCN was received before the alarm issued by the switch, which would put the component in the proper state (and the proxy alarm will be cleared when the real alarm is received) or because the alarm issued by the switch has been lost.

Treat proxy alarms as you would treat regular alarms and use them in debugging network problems.

## 0999 0013

<b>Component</b>	<b>Severity</b>	<b>Status</b>
<device>/<device name> [<component type>/<component instance>]	major/cleared	set/clear

### **Alarm type**

unknown

### **Probable cause**

unknown

### **Legend**

<device> is the network device

<device name> is the name assigned to this device in your network

### **Details**

The alarm generated by the MDM SNMP Management Data Router (SMDR) for an SNMP component is inconsistent with traps received from the network.

When the status of the alarm produced by SMDR is a set, it means that the Poll response indicates that the network device is down, but there are no corresponding active alarms on that network device to indicate that it is down. Therefore, the MDM creates a proxy alarm to replace the missing alarm. The MDM marks the network device Out of Service (OOS).

When the status of the alarm is a clear, it means that the Poll response indicates that the network device is up, but there are active alarms on that network device to indicate that it is down. Therefore, the MDM generates a proxy alarm to replace the missing clear. The MDM marks the network device Inservice.

### **Remedial action**

This alarm is issued either because the Poll responses was received before the trap was issued by the network device, which would put the network device in the proper state (and the proxy alarm would be cleared when the trap is received) or because the trap issued by the network device has been lost or the network device never generated a trap.

Treat proxy alarms as you would treat regular alarms. Use them to debug network problems.



---

# Index

---

09990001	42	50040102	28
09990002	43	50040103	29
09990003	44	50040104	29
09990004	45	50040105	29
09990010	46	50040106	30
09990011	47	50040107	30
09990012	48	50040108	30
09990013	49	50040109	31
30100000	15	50040110	31
30100700	16	50040111	31
30100701	16	50040112	32
30100702	17	50040113	32
30100703	17	50040114	32
30110001	18	50040115	33
30110100	18	50040116	33
30110200	19	50040117	33
30110300	19	50040118	34
30110401	20	50040119	34
30110501	21	50040120	34
30110600	21	50040121	35
30110700	22	50040122	35
50040001	24	50040123	35
50040002	24	50040124	36
50040003	25	50040125	36
50040004	25	50040126	36
50040005	26	50040127	37
50040006	27	50040128	37
50040007	27	50040129	37
50040100	28	50040130	38
50040101	28	50040131	38

50048888 39  
5004FFFF 39  
50xx00xx 22  
50xx01xx 23  
50xx02xx 23  
600XXXXX 40

**A**

A0XXXXXX 40

**B**

B000BXXX 41

**C**

CDXXXXXX 41

**M**

MDM proxy alarms 13

**T**

turn off proxy alarm 13



Preside Multiservice Data Manager  
**Proxy Alarms**  
Reference Guide

Release: R14.3

Copyright © 2003 Nortel Networks.  
All Rights Reserved.

NORTEL, NORTEL NETWORKS, the globemark design, the NORTEL NETWORKS corporate logo, PRESIDE, DPN, and PASSPORT are trademarks of Nortel Networks. OPENVIEW is a trademark of Hewlett-Packard Company.

Publication: 241-6001-501  
Document status: Standard  
Document version: 14.3RSUP  
Document date: December 2003  
Printed in Canada

