Lucent Technologies
Bell Labs Innovations

Navis™ Optical Provisioning Manager (PM) - Network Provisioning (NP)

Release 1.0

Maintenance Guide

365-314-101R1.0
Issue 1
April 2002

Copyright © 2002 Lucent Technologies. All Rights Reserved.

This material is protected by the copyright laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Lucent Technologies), except in accordance with applicable agreements, contracts or licensing, without the express written consent of Lucent Technologies and the business management owner of the material.

Lucent Technologies at: 800 645-6759 (continental U.S.) or +1 317 322 6847

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Mandatory customer information

Warranty

Lucent Technologies provides a limited warranty for this product. For more information, consult your Lucent Technologies customer team representative.

Trademarks

TrueWave is a registered trademark of Lucent Technologies.

WaveStar is a registered trademark of Lucent Technologies.

Navis is a trademark of Lucent Technologies.

Hewlett-Packard is a registered trademark of Hewlett-Packard.

HP-UX is a registered trademark of Hewlett-Packard.

UNIX is a registered trademark of X/Open Company Limited. In the United States and other countries, it is licensed exclusively through X/Open Company Limited.

Windows NT is a registered trademark of Microsoft.

Orbix is a registered trademark of Iona Technologies

Windows is a registered trademark of Microsoft.

VUE is a registered trademark of Hewlett-Packard Co.

Ordering information

The ordering number for this document is 365-314-101. To order WaveStar NMS information products, do one of the following:

- Contact your Lucent Technologies customer team representative.
- Contact the Lucent Technologies at:

- From the United States, call 888-LUCENT8, prompt 1.

- From Canada, call 317-322-6619.

- From Europe, the Middle East, and Africa, call 317-322-6416.

- From Asia, the Pacific Region, China, the Caribbean, and Latin America, call 317-322-6411.

Support

Information product support

Lucent Technologies provides a referral telephone number for support. Use this number to report errors or to ask questions about the information in the information product. This is a non-technical number. The referral number is 800-645-6759.

Technical support

In the continental United States, when you need additional technical assistance, the Lucent Technologies Global TSS Contact Center is your first point of contact. Technical assistance is available 24 hours a day, 7 days a week. Contact the Global TSS Contact Center at 866-LUCENT8 (866 852-3688).

Outside the continental United States, contact your Local Customer Support (LCS) or the support organization designated by your Lucent customer team representative. If you are unsure of who to call, contact the Global TSS Contact Center at 630-224-4672.

Contents

About this information product

Purpose xi

Reason for reissue xi

Safety labels xi

Intended audience xi

How to use this information product xi

Conventions used xii

Related documentation xii

How to comment xiv

How to order xiv

1 Maintenance Overview

Overview 1-1

Section I: Fault management

Overview 1-3

Fault management overview 1-4

Fault management operational mode 1-7

Fault management forms 1-8

Accessing fault management information from the Network Map 1-9

Color-coded alarm notification on Network Map 1-10

Color-coded alarm notification on fault management forms 1-13

User settings 1-15

Installation options 1-16

Optical Network Navigator 1-18

Section II: Performance monitoring

Overview 1-20

Performance monitoring overview 1-21

Performance monitoring data 1-23

Performance monitoring user interface 1-25

PM Port List 1-27

Performance monitoring path list 1-29

Default filter thresholds on the PM Data Reporting form 1-30

2 Fault management tasks

Overview 2-1

Acknowledge an alarm 2-3

Change the fault management operational mode 2-4

Filter secondary alarms 2-5

Create a trouble ticket 2-7

Add alarms or alarmed objects to trouble tickets 2-9

Delete a trouble ticket 2-10

Delete an alarm from the Alarm List 2-11

Archive, export, and delete alarm log records 2-12

Perform a manual alarm synchronization 2-14

View alarms on a link between two network elements 2-15

View alarms on a bridge 2-16

View alarms for a network element 2-17

View alarms for an EMS 2-18

Filter non-alarm events from the Network Event Summary form 2-19

View alarm counts from the Network Event Summary 2-20

Filter/sort alarms 2-21

Display Optical Network Navigator ports with failed and unknown status 2-23

3 Performance monitoring tasks

Overview 3-1

Performance monitoring tasks

Overview 3-2

Display the installed date format 3-3

Set up a monitoring point 3-4

Set a threshold value for a performance parameter 3-6

Create a data report 3-8

Delete a monitoring point 3-11

Execute the performance monitoring export tool 3-12

Change the scheduled run time of the performance monitoring file transfer 3-13

Add special archiving features for performance monitoring 3-14

4 Alarm management concepts

Overview 4-1

Alarm collection 4-2

Alarm classification 4-4

Alarm correlation 4-7

Fault state determination 4-12

Alarm and alarmed object suppression 4-19

Service impact assessment 4-21

Alarm deletion 4-23

Alarm acknowledgement 4-24

Domain partitioning 4-26

Trouble ticketing 4-27

5 Fault management fault lists

Overview 5-1

Section I: Navis™ Optical EMS fault lists

Overview 5-2

Navis™ Optical EMS management alarms 5-3

Navis™ Optical EMS: WaveStar® BandWidth Manager and OC192 network elements fault list 5-4

Navis™ Optical EMS: WaveStar® OLS 1.6T Family fault list 5-6

Navis™ Optical EMS: LambdaRouter™ AOS fault list 5-7

Section II: Navis™ Optical PM - NP fault lists

Overview 5-8

Navis™ Optical PM - NP fault list 5-9

6 Performance monitoring parameters

Overview 6-1

Section I: Performance monitoring parameters

Overview 6-3

Performance monitoring parameters 6-4

Termination point performance parameters 6-6

Monitoring points 6-10

Metropolis™ EON performance monitoring parameters 6-12

Ethernet performance monitoring data 6-13

Optical network termination point performance parameters 6-14

Section II: Threshold setting parameters

Overview 6-16

Threshold setting 6-17

Optical threshold crossing alert parameters 6-18

Threshold crossing alert parameters 6-19

Section III: Trail Types

Overview 6-23

Connection level and trail types: WaveStar® BandWidth Manager, WaveStar® TDM 2.5/10G, and WaveStar® OLS 1.6T 6-24

7 Reports Management

Overview 7-1

About reports 7-2

IN Index IN-1

List of Tables

4 Alarm management concepts

4-1 Alarm categories 4-5

4-2 Severity mapping 4-6

6 Performance monitoring parameters

6-1 Performance monitoring parameters 6-4

6-2 Termination point performance parameters per supported network element 6-6

6-3 Supported performance monitoring points per supported network element 6-10

6-4 Metropolis™ EON monitoring points 6-12

6-5 Ethernet performance monitoring data 6-13

6-6 Optical network termination point performance parameters for WaveStar® OLS 1.6T 6-14

6-7 Optical threshold crossing alert parameter settings 6-18

6-8 Threshold crossing alert parameters per supported network element 6-19

6-9 Connection level and trail types supported by the WaveStar® BandWidth Manager, TDM 2.5G/10G, and WaveStar® OLS 1.6T network elements. 6-24

About this information product

Purpose

This preface provides an overview of this information product, which is the Navis™ Optical Provisioning Manager (PM) - Network Provisioning (NP) Maintenance Guide, Release 1.0.

The purpose of this Maintenance Guide is to instruct users how to maintain the Navis™ Optical PM - NP Release 1.0 and the network.

Reason for reissue

Issue 1 of this Maintenance Guide is a new document that supports Navis™ Optical PM - NP Release 1.0.

Safety labels

This document does not use safety labels.

Intended audience

This document is written for operations personnel who will be maintaining Navis™ Optical PM - NP.

How to use this information product

This document contains:

- ***task*** information, which includes maintenance tasks (that is, step-by-step instructions).
- ***conceptual*** information, which is specific data related to tasks.

Both types of information is presented within the chapters of this Maintenance Guide.

Chapter descriptions

The following table describes the information in each chapter of this Maintenance Guide.

Section	Title	Description
Preface	About this information product	Explains this document’s purpose and intended audience, and how to use the information product.
Chapter 1	Chapter 1, “Maintenance Overview”	Describes how maintenance is performed for Navis™ Optical PM - NP.
Chapter 2	Chapter 2, “Fault management tasks”	Explains how to set up and use fault management.
Chapter 3	Chapter 3, “Performance monitoring tasks”	Explains how to set up and use performance monitoring.
Chapter 4	Chapter 4, “Alarm management concepts”	Explains how alarms are collected and managed.
Chapter 5	Chapter 5, “Fault management fault lists”	Lists the supported alarms.
Chapter 6	Chapter 6, “Performance monitoring parameters”	Describes the performance monitoring parameters.
Chapter 7	Chapter 7, “Reports Management”	Describes reports that can be run.
Index	Index	Enables the user to quickly find information on specific topics.

Conventions used

This Maintenance Guide uses the following typographical conventions to distinguish between computer input and output.

- When describing the Navis™ Optical PM - NP software, fields in windows and field entries are identified with **this font**.
- When describing the *UNIX*® environment, text and numbers that the user inputs to the computer are identified with **`boldface type`**.
- In the UNIX environment, text and numbers that the computer outputs to the user are identified with `monospace type`.

Related documentation

This Maintenance Guide is part of a set of documents that supports Navis™ Optical PM - NP.

List of documents

The document set that supports Navis™ Optical PM - NP comprises:

1. *Navis™ Optical PM - NP Provisioning Guide*, (365-314-100) instructs users how to use Navis™ Optical PM - NP to provision network equipment. This document includes tasks and conceptual information.
2. *Navis™ Optical PM - NP Maintenance Guide,* (365-314-101) instructs users on how to maintain Navis™ Optical PM - NP and the network.
3. *Navis™ Optical PM - NP Administration Guide*, (365-314-102) instructs users on how to administer Navis™ Optical PM - NP and the network.
   This document includes tasks and conceptual information.
4. *Navis™ Optical PM - NP Getting Started Guide,* (365-314-104): provides information useful to first-time users of the Navis™ Optical PM - NP software. It describes how to start and stop Navis™ Optical PM - NP, how to use the software, and how to interpret the graphical user interface.
   This document includes tasks and conceptual information.

Glossary

The *Navis™ Optical PM - NP Administration Guide* contains a glossary that will be helpful to users of Navis™ Optical PM - NP.

On-line documentation

On-line documentation for Navis™ Optical PM - NP is provided in two formats:

1. An on-line version, in HTML format, of this document set is provided as part of theNavis™ Optical PM - NP software.
2. An on-line version, in HTML format, of this document set is available on CD-ROM.
   Navis™ Optical PM - NP User Documentation CD-ROM, (365-314-103) - includes the full set of documents listed above.

Screen help

The Navis™ Optical PM - NP software includes screen help for each form, which describes the purpose of the form, each field, and each button.

How to comment

To comment on this information product online, go to *http://www.lucent-info.com/comments* or email your comments to ctiphotline@lucent.com (mailto:ctiphotline@lucent.com).

How to order

To order Navis™ Optical PM - NP information products, contact your Lucent Technologies customer team representative or contact Lucent Technologies at:

- From the United States, call 888-LUCENT8, prompt 1.
- From Canada, call 317-322-6619.
- From Europe, the Middle East, and Africa, call 317-322-6416.
- From Asia, the Pacific Region, China, the Caribbean, and Latin America, call 317-322-6411.

1 Maintenance Overview

Overview

Purpose

This Maintenance Guide describes the fault management and performance monitoring components of Navis™ Optical PM - NP. This chapter provides an overview of the Navis™ Optical PM - NP fault management and performance monitoring processes.

Contents

Section I: Fault management	1-3
Fault management overview	1-4
Fault management operational mode	1-7
Fault management forms	1-8
Accessing fault management information from the Network Map	1-9
Color-coded alarm notification on Network Map	1-10
Color-coded alarm notification on fault management forms	1-13
User settings	1-15
Installation options	1-16
Optical Network Navigator	1-18
Section II: Performance monitoring	1-20
Performance monitoring overview	1-21

Performance monitoring data	1-23
Performance monitoring user interface	1-25
PM Port List	1-27
Performance monitoring path list	1-29
Default filter thresholds on the PM Data Reporting form	1-30

□

Section I: Fault management

Overview

Purpose

Contents

Fault management overview	1-4
Fault management operational mode	1-7
Fault management forms	1-8
Accessing fault management information from the Network Map	1-9
Color-coded alarm notification on Network Map	1-10
Color-coded alarm notification on fault management forms	1-13
User settings	1-15
Installation options	1-16
Optical Network Navigator	1-18

☐

Fault management overview

Introduction

The fault management subsystem of the Navis™ Optical PM - NP receives and processes the alarms on the network in real time. It supports a network operator in achieving the following high level goals:

- Locating and repairing faults in the network
- Identifying the impact of failures in the network on services
- Initiating service restoration, if appropriate

Process overview

Fault management combines the functionality of multiple Navis™ Optical PM - NP modules to process and analyze alarms generated from the managed network elements.

1. Alarm events are first filtered by the EMS.
2. Filtered events are passed to Navis™ Optical PM - NP for analysis.
3. The analysis determines whether there is a problem within a network element or a problem on the connection between network elements.
4. Connection problems are sectionalized down to the link level. Network element alarms are pinpointed down to the slot or port level.
5. To alert the user to the alarm condition:
    - A Network Event Summary form appears and is dynamically updated.
    - Network Map links and nodes change color.
    - Various forms are populated with alarm information.

Element management systems

Navis™ Optical PM - NP provides fault management through the following element management systems (EMSs):

- Navis™ Optical Element Management System (EMS)

Network elements

Fault management is a powerful tool that utilizes the forwarded alarms from the EMSs that have received and processed the alarms from the following network elements:

- Lambda UNITE MultiService Switch Release 2.0
- Metropolis™ EON Release 8.0 and 8.1
- Metropolis™ DMXpress Release 1.0
- Metropolis™ DMXpress Access Multiplexer Release 2.0 and 2.1
- WaveStar® BandWidth Manager Release 4.1
- WaveStar® OLS1.6T Release 6.1
- WaveStar® TDM 2.5G/10G Release 6.0

Functionality

The fault management functionality consists of the following:

- Alarm collection
- Alarm classification
- Alarm correlation
- Fault state determination
- Alarm and alarm trail suppression
- Service impact assessment
- Identification of problem location internal and external to the network
- Processing of TCAs (Threshold Crossing Alerts)
- Alarm deletion
- Network Map and screen display colors for alarm notification

Alarm setting recommendations

To prevent a flood of alarms, the following overall settings must be set as “not reported” for each network element.

- AIS (Alarm Indication Signal)
- TTP (Trail Termination Point)
- SSF (Server Signal Fail).

For existing protected connections terminating on network elements that support per-instance reporting, the alarms must be turned on at the trail termination points. If the user also has connections where the end points are not visible, the user can set AIS to be reported on the domain boundary termination points. These alarms should not be turned on for unprotected connections.

☐

Fault management operational mode

Introduction

Two distinct modes of operation are available for the operation of fault management:

- Service Approach
- Alarm Approach

The approach selected determines the forms that fault management presents to the user, and the filtering and sorting options within these forms. For more information, refer to "Fault management forms" (1-8) in this information product.

Service approach

The Service Mode of operation focuses on the maintenance of services provided over the network. Alarms are correlated to an alarmed object, which in turn enables the services that are affected to be identified. This allows prioritization to be applied to the maintenance of the network.

The Service Approach focuses on alarm management from the Traffic Correlated Alarm List form.

Alarm approach

The Alarm Mode of operation focuses on the maintenance of the network itself. This approach allows the user to look through all of the alarms on the system, identify where the problems are and what is causing the alarm.

The Alarm Approach focuses on management of alarms from the Alarm List form.

Changing modes

The default operational mode for all users is set on installation. After installation, the mode can be set on a per user basis, by setting the Fault Management Operational Mode option on the Preferences form. The setting selected affects the next and subsequent user sessions. For more information refer to "Change the fault management operational mode" (2-4).

□

Fault management forms

Overview This section describes the supported fault management forms.

GUI forms The following forms are a functional part of fault management:

- Network Event Summary - Alarm View. This form displays all of the alarms on the system. The form is used to view alarm summary information when the Alarm Approach is selected.
- Network Event Summary - Service View. This form focuses on the maintenance of services provided over the network. Alarms are correlated to a trail, circuit, or equipment, which allows identification of the services that are affected. The form is used to view correlated alarm summary information when the Service Approach is selected.
- Traffic Correlated Alarm List. This form indicates alarms that affect trails. These are alarms which have been correlated to an object, because they affect traffic.
- Alarm List. This form displays a list of all Navis™ Optical PM - NP, EMS and network element alarms.
- Affected Trail List. This form allows the user to view a list of trails associated with a selected alarm or alarmed object.
- Trouble Ticket forms. These forms allow a user to create or delete a Trouble Ticket, add alarms to a trouble ticket, and assign an owner to be responsible for resolution of the problem.
- Alarm Log - Service View. This form allows users to view details about all alarmed objects that are historic, and to archive and export this information.
- Network Navigator Failed Link List. This form allows the user to display Optical Network Navigator ports with a status of “failed” and “unknown”.
- Alarm Log - Alarm View. This form allows users to view details about all alarms, and to archive and export this information.
- Log Administration - Service View. This form allows the user to perform archive, export and delete functions for records from the Alarm Log - Service View.
- Log Administration - Alarm View. This form allows the user to perform archive, export and delete functions for records from the Alarm Log - Alarm View.

☐

Accessing fault management information from the Network Map

Overview The user can access and display fault management forms from the Network Map.

Regenerator alarms By selecting the regenerator symbol on a digital link, the user displays a list of the regenerators on that link. This list indicates which regenerator has alarms. By selecting a regenerator, the user then cuts through to the Navis™ Optical PM - NP Alarm List for that network element.

Nodes The user selects a node on the Network Map to cut through to the SNMS Alarm List for the corresponding network element. The Alarm List is filtered to show only records which have the network element ID of the selected node. It is not possible to cut through from an aggregate node.

Links By selecting a link on the Network Map, the user accesses a filtered view of the Traffic Correlated Alarm List for that link. The link must be between two network elements, and not between two aggregates and not between a network element and an aggregate. The Traffic Correlated Alarm List is filtered to show only those trail alarmed objects that are connections represented by that link.

□

Color-coded alarm notification on Network Map

Overview The icons on the Network Map are color-coded to show the alarm status of the node or link they represent. The link color, the node color, or the port color is dynamically updated to indicate the current status of the network.

Nodes and node borders are color-coded to represent the most severe alarm condition of all alarms reported against that node.

Links are color-coded to represent the service state of that link.

A color-coding scheme for alarms is also used on the fault management forms.

Links The link on the Network Map indicates one or more physical connections between two nodes.

The digital link color on the Network Map is dynamically updated.

The link color displayed is based on the worst case existing on the link.

- Green: Indicates that all in-effect trails represented by the link have no alarms.
- Yellow: Non-Service Affecting. Indicates that at least one channelized facility, without provisioned circuits, is alarmed. Also indicates line degradation alarm, specifically for a digital link that is in alarm.
  Also applies to a channel with a provisioned protected circuit which has lost its protection path.
  A non-assignable circuit does not exist using this digital link.
- Red: Service Affecting. Indicates that at least one non-channelized facility is alarmed or that at least one channelized facility with provisioned circuits is alarmed.
- Blue: Identifies the service path of a trail. This color does not indicate whether a fault is present.
- Purple: Identifies the protection path of a trail. This color does not indicate whether a fault is present.

Nodes The node color on the Network Map is dynamically updated.

EMS nodes

The node representing an EMS (including Navis™ Optical PM - NP) change color from green to either red or yellow. Changing color to red or yellow represents platform alarms on that EMS alone, and do not show any effect on transmission through the network. In most cases, there is no impact on services.

Navis™ Optical PM - NP uses the following colors for EMS nodes, listed in descending order of priority.

- Magenta - Loss of communication with the EMS, shown on the EMS only.
- Red - Critical or major alarm. These are EMS platform alarms only, and do not represent alarms on controlled network elements.
- Yellow - Other alarm severities. These are EMS platform alarms only, and do not represent alarms on controlled network elements.
- Green - No alarm.

Navis™ Optical PM - NP uses the following colors for Navis™ Optical PM - NP platform alarms.

- Red - Critical or major alarm.
- Yellow - Other alarm severities.
- Green - No alarm.

DXC and regenerators

> **Important!** When a node is first added into the Navis™ Optical PM - NP, it is always displayed as green, independent of whether equipment or environment alarms exist. Always perform a manual database synchronization after adding a node to display the true state of the new node.

Node colors are based on the worst case existing on the node.

- Green: The communication link between Navis™ Optical PM - NP and the node is UP. Equipment alarms do not exist.
- Gray: The node has been deleted, but digital links and circuits are still present. The node cannot be used in further provisioning.
- Magenta: The communication link between Navis™ Optical PM - NP and node is down.

- Red: One or more service affecting equipment alarm condition(s) are on the network element.
- Yellow: One or more non-service affecting equipment or environment alarms are on the network element. Service affecting equipment alarms do not exist on the network element.

Network elements (except regenerators)

Navis™ Optical PM - NP uses the following colors for all network elements (excluding regenerators), listed in descending order of priority.

- Green: The communication link between the controlling EMS and the node is up. No equipment alarms exist.
- Gray: The node has been deleted, but digital links and circuits are still present. The node cannot be used in further provisioning.
- Magenta: The communication link between Navis™ Optical PM - NP and the node is down.
- Red: One or more major (service-affecting) equipment alarm condition(s) are on the network element.
- Yellow: One or more minor (non-service-affecting) equipment or environment alarms are on the network element. Service-affecting equipment alarms do not exist on the network element.
- Orange colored box around the node: One or more uncorrelated alarms are on the network element.

Black boxes

Black boxes are always white/black since communication links are not connected to them from the Navis™ Optical PM - NP, Navis™ Optical EMS.

Aggregates

Color is based on the worst alarm condition of the nodes, links, or regenerators associated with this aggregate. The severity of the alarm condition is from highest to lowest the following:

- Magenta
- Red
- Yellow
- Green

□

Color-coded alarm notification on fault management forms

Visual alarm display in user interface forms

In addition to the dynamic node and link color changes caused by alarms in the Network Map, Navis™ Optical PM - NP provides static visual display of alarms by using color schemes and/or lists in the following user interface forms:

- Graphical Layout
- Network Event Summary
- Traffic Correlated Alarm List
- Affected Trail List
- Alarm List

Graphical Layout form

The port in the alarmed trail shown in the graphical layout will show the alarm as cleared for the correlated port. The Graphical Layout form display shows the alarm on the port. If a PDH alarm is received in Navis™ Optical PM - NP, the VC-12 graphical layout shows the alarm on the 2-Mb/s port. The alarm colors are:

- Red: indicates that an alarm condition exists
- Green: indicates that alarm condition is not present.

The colors in the graphical layout form are not updated dynamically.

Network Event Summary form

The severity values displayed on the Network Event Summary form are colored as follows:

- Critical - red
- Major - red
- Minor - yellow
- Warning - yellow
- Indeterminate - yellow.

Traffic Correlated Alarm List form

The fault state values displayed on the Traffic Correlated Alarm List form are as follows:

- Failed - red
- Degraded - yellow
- Working - green.

The service impact values displayed on the Traffic Correlated Alarm List are as follows:

- Failed - red
- Degraded - yellow
- Working - green
- No services - green
- Calculating - green.

Affected Trail List form

The fault state values displayed on the Affected Trail List form are as follows:

- Failed - red
- Degraded - yellow
- Working - green.

Alarm List form

The severity values displayed on the Alarm List form are as follows:

- Critical - red
- Major - red
- Minor - yellow
- Warning - yellow
- Indeterminate - yellow.

□

User settings

Introduction

The user setting feature is designed to allow the user to set up individual user settings in order to organize and customize some of the fault management forms, which enables the user to display data in a way that is tailored to their needs.

The User Settings feature allows the user to organize and display data in the following ways:

- Customize the form display on certain forms
- Change user preferences, including Operational Mode

Customize form display

The user is able to determine how many columns are visible and in which order. Additionally, the user can alter the width of each column.

The user can save and retrieve the user-defined form settings, and also display default forms at any time.

This feature is available to any form with five or more columns.

Preferences

At installation, options that relate to fault management are set. The user can change the following options for their individual login ID:

- Event Indications
- Map display
- Alarm Color of Forms
- Fault Management Operational Mode

These options can be changed through the Preferences form, which is accessed by selecting the following from the Network Map:

Administration > Preferences

☐

Installation options

Introduction

Several installation options that relate to fault management should be considered when Navis™ Optical PM - NP is installed. They are:

- FM operational mode
- Interval time
- Number of events
- Alarm storage limits
- Alarm deletion options
- Read-only viewing for GD users
- Aging period for restoration notification
- Port aliasing

FM operational mode

Navis™ Optical PM - NP is set to run in the default Service Mode or Alarm Mode. This setting can later be changed by the user for individual login IDs.

Interval time

The default interval time for polling to update the counters on the Network Event Summary forms varies between 30 and 60 seconds.

Number of events

The default number of events displayed on the Network Event Summary forms.

Alarm storage limits

The default alarm record limit for current alarms and historic alarms.

Alarm deletion options

The following are options for the deletion of persistent alarms. Persistent alarms are those which have a raise and a clear.

- Delete automatically for both unacknowledged and acknowledged alarms on receipt of a clear.
- Delete automatically for acknowledged alarm on clear.
- Delete automatically for unacknowledged alarms on clear.
- Delete automatically with enforced clear acknowledgement.

Aging period for restoration notification

The user can set the time, in seconds, that a service trail must be failed before the restoration component is notified about the failure.

Port Aliasing

If enabled, the user can toggle between the Lucent Technologies port name and their own customer port name on the following screens:

- Network Event Summary - (Events List section) Alarm and Service view
- Alarm List
- Traffic Correlated Alarm List
- Affected Trail List
- Alarm List - Alarm and Service view

□

Optical Network Navigator

Overview

This section discusses the Optical Network Navigator (ONN).

Definition

The ONN is software and hardware present in the LambdaRouter network elements which performs management functions, i.e. configuration management and fault management, on optical connections across a network of LambdaRouters.

Navis™ Optical PM - NP and Optical Network Navigator interaction

The Optical Network Navigator system essentially acts as the network manager for the domain of optical connections it controls. The Navis™ Optical PM - NP domain provides capacity to the Optical Network Navigator domain, which provides capacity back to the Navis™ Optical PM - NP. Each management system tracks the fault state of it's connectivity, then uses Navis™ Optical PM - NP to display combined fault state information to the user.

For the current release of Navis™ Optical PM - NP, the Optical Network Navigator feature is available only on a limited basis.

Fault management

Fault management performs the following for Optical Network Navigator:

- Identification of connections which are currently failed. Fault management identifies which mesh Optical Network Navigator connections cannot be re-routed and have therefore failed, and which 1+1 or unprotected connections are failed.
- Identification of infrastructure (fiber/ducts) which need repair. Fault management identifies the root cause failure in the network to allow them to be repaired.

Fault state

Fault management uses a combination of information to find the fault state of the connection.

The following are points to note:

- Optical Network Navigator mesh connections do not have a defined route. For these connections, Navis™ Optical PM - NP considers that the Optical Network Navigator is responsible for management of the connections and will inform fault management of the fault state. Fault management will not attempt to propagate server alarms to these connections and will not know the route these connection take in the network.
- Optical Network Navigator 1+1 protected connections are identified as “working” or “failed” by Optical Network Navigator. Fault management will use it’s normal protected mechanism to mark the connection as degraded.

Alarm synchronization

Optical Network Navigator does not store autonomous notifications which it sends northbound. As a result, if Navis™ Optical PM - NP or Optical Network Navigator, or the links between them go down, the autonomous notifications are lost. Therefore Navis™ Optical PM - NP does not support alarm re-synchronization for Optical Network Navigator.

□

Section II: Performance monitoring

Overview

Purpose

Performance monitoring allows the system administrator to precisely monitor the quality of the end-to-end paths, be notified of performance degradation, and initiate corrective action, if necessary.

This section describes the Navis™ Optical PM - NP performance monitoring system.

Contents

Performance monitoring overview	1-21
Performance monitoring data	1-23
Performance monitoring user interface	1-25
PM Port List	1-27
Performance monitoring path list	1-29
Default filter thresholds on the PM Data Reporting form	1-30

☐

Performance monitoring overview

Purpose

The purpose of Navis™ Optical PM - NP performance monitoring is to enable the user to:

- Define the paths (via ports) in the network to monitor for performance monitoring
- Start or stop the collection of performance monitoring data for the paths
- Set parameter thresholds for Threshold Crossing Alert (TCA) reporting
- Request display of data with filtering capabilities by path, date range, and threshold

The “dacscan” login has to be present on the workstation from where performance monitoring reports are requested. See ***Navis™ Optical PM - NP Administration Tasks*** for details on adding the “dacscan” login.

Benefits

Performance monitoring facilitates the planning and implementation of proactive, forward-looking network maintenance strategies by providing a centralized facility to monitor network performance systemically. This is accomplished by non-intrusively gathering in-service information about the state of the network. The gathered information can be effectively used to maintain existing uninterrupted delivery of services.

Effects of rearrange and merge on performance monitoring

Because a digital link or facility/circuit requires two nodes, two ports are always associated with a path. However, performance monitoring data may not be collectible from both ports.

When circuits with existing monitoring points are to be merged and if the total number of monitoring points for the merged circuit does not exceed four, performance monitoring points as they exist prior to the merging are retained. However, if the number of monitoring points exceed four after merging, the Navis™ Optical PM - NP displays a notification that includes the number of ports where performance monitoring collection has to be stopped for the merge to succeed.

Performance monitoring data collection will not be stopped if a circuit is rearranged, as long as the ports where performance monitoring data collection is occurring are part of the new (rearranged) path. If performance monitoring data collection occurs on ports that are no longer part of the new path, performance monitoring on these ports is stopped and deleted. The performance monitoring stopping and deletion are done automatically as part of the rearrange process. performance monitoring cannot be reinstated if a rearrange fails after performance monitoring has been stopped to support the rearrange process. It is the user’s responsibility to restart performance monitoring on those ports.

Supported network elements

Navis™ Optical PM - NP supports performance monitoring for the following network elements:

- Lambda UNITE™ MultiService Switch Release 2.0
- Metropolis® EON Release 8.0 and 8.1
- Metropolis® DMXpress Release 1.0
- Metropolis® DMXpress Access Multiplexer Release 2.0 and 2.1
- WaveStar® BandWidth Manager Release 4.1
- WaveStar® OLS1.6T Release 6.1
- WaveStar® TDM 2.5G/10G Release 6.0

□

Performance monitoring data

Overview

The performance of a transport connection is monitored by an EMS at termination points located at its extremities, or at termination points located along its route. This monitoring can occur as long as the network elements at these termination points each have the capability to monitor performance parameters.

Performance monitoring data

In the case of the SONET network, performance parameters are determined from anomalies and defects detected at termination points.

The following are examples of performance parameters:

- errored seconds (ESs)
- severely errored seconds (SESs)
- background block errors (BBEs)
- unavailable seconds (UAS)

Those network elements with the capability to count the number of these performance parameters detected over a specific period of time, transfer the values of its counters to the EMS. Navis™ Optical PM - NP collects the counter data from selected termination points through services provided by the EMSs. The counter values are know collectively as performance monitoring data.

Types of performance monitoring data

In the case of certain network elements, the performance monitoring data available at a termination point represents errors detected in the signal received at the termination point. This is known as near-end data.

For other network elements, the performance monitoring data represents both near-end and far-end data. Far end data represents error measurements taken at the upstream extremity of the transport connection, of which the termination point is part.

Time periods

All network elements managed by Navis™ Optical PM - NP use two time periods to accumulate unidirectional performance parameters.

They are:

- 15 minutes
- 24 hours

PM Data Export/file transfer

Navis™ Optical PM - NP automatically requests each EMS to recover all performance monitoring data collected during the previous 24 hours, from midnight to midnight. Navis™ Optical PM - NP stores the recovered 24-hour data on a single designated UNIX workstation. One week of data is stored.

For Navis™ Optical EMS managed network elements, the file format used for the file transfer is per the TMF G72.0 interface definition.

□

Performance monitoring user interface

Introduction

The performance monitoring feature is accessible from Performance menu on the Network Map and from the Graphical Layout form.

Performance menu

The performance monitoring feature is accessible from the Network Map and from the Graphical Layout form.

From the Performance menu on the Network Map, the following performance monitoring capabilities can be accessed:

- ***PM Path List***: Allows the user to perform performance monitoring on monitored paths.
- ***PM Port List***: Allows the user to perform performance monitoring data collection.

Subfunctions

The following are subfunctions that allow the user to access performance monitoring capabilities.

- ***Ckt/DTS:*** allows the user to enter the circuit ID or order number for a port or trail to be monitored. The minimum entry is the Order number.
- ***Data Collection:*** allows the user to start, stop, or schedule collection of performance monitoring data from the network for the path.
- ***Threshold Setting:*** allows the user to set thresholds on the monitored ports of the path that the network elements use to report TCAs.
- ***Path List Query:*** (Optional) allows the user to enter the CKT/Trail ID, Location, circuit type, and from/to date to display and modify the monitored trail/port. Selecting **OK** displays all monitored trails in the path list.
- ***Port List:***displays a list of monitorable ports.
- ***Data Reporting:***allows the user to view performance monitoring data that was collected from the network for the path.

Message log

The DXC Administration Node Menu provides the following form:

- ***Performance Monitoring Message Log:***contains DXC performance monitoring output messages.

Threshold crossing alerts

The Alarm List displays:

- ***Threshold Crossing Alerts:*** allows the user to be alerted of threshold levels that crossed the set thresholds.

☐

PM Port List

Overview

The PM Port List form allows the user to perform the following functions related to the collection of performance monitoring data.

- displaying all monitorable ports for a path
- selecting terminations points for data collection
- start and stop data selection
- schedule data collection
- delete performance monitoring

Select termination points for data collection

The PM Port List provides the user with a means to identify a single trail for which performance monitoring data is to be collected. The user may collect performance monitoring data from in-effect transport connections only.

The user selects up to four ports to be monitored, and selects whether 15-minute or 24-hour performance monitoring data is collected. In the case of WaveStar® DACS, the user select one hour performance monitoring data.

About data collection

Performance monitoring data collection allows the user to start performance monitoring for a trail that has not yet been set up (on the Navis™ Optical PM - NP) or to add more ports to be monitored on the trail. performance monitoring data collection also allows the user to modify the monitored trail/port in terms of trail type (network-element-dependent), start/stop time, location/port, and measurement period.

When performance monitoring is requested by the user, default ports that would result in Trail Termination Point (TTP) monitoring points are identified by the Navis™ Optical PM - NP and their port addresses are automatically populated on the PM Port List form for a particular path. If the user accepts these two default trail termination ports and does not add any more ports and proceeds, the procedure amounts to a TTP performance monitoring. When the user navigates from the Graphical Layout, the A and Z location/Ports are pre-populated but the intermediate monitors (if trail has more than two monitors) are not displayed in the selection list until the user specifies the trail type and measurement period.

When one or both trail termination points are not appropriate for performance monitoring (for example, the termination points are outside the managed domain), the Navis™ Optical PM - NP identifies other monitoring ports. These ports are then used as default ports to automatically populate the Port List Data form. The user can accept, modify, or add to these ports. A trail is defined by the CKT/Trail ID, Circuit Type, Trail Type and Measurement Period.

> **Important!** The user should use caution when entering port data, as the Navis™ Optical PM - NP system does not check for duplicate port entries. An error or warning message is not presented if the user enters the same port data.

Start and stop data collection

Using the PM Port List, the user starts and stops data collections on a selected port. Additionally, the user may delete a port from the list of monitored ports, however the user must stop the collection of performance monitoring data first.

The user may select up to four sets of data per trail, per granularity associated with the transport connection selection.

□

Performance monitoring path list

Overview

The PM Path List allows the user to perform performance monitoring functions on monitored paths.

These functions include:

- view a list of ports for which performance monitoring data is being monitored
- Performance monitoring data reporting
- set up and view thresholds

View a list of ports

The PM Path List provides the user with a list of ports for which performance monitoring data is being monitored.

Monitored ports are depicted as follows:

- Started: performance monitoring data is currently being collected
- Stopped: performance monitoring data has been collected and collection is no longer taking place
- Scheduled: performance monitoring data is scheduled to be collected in the future

Data reporting

From the PM Path List, the user accesses the PM Data Reporting form, which allows the user to request a report of performance monitoring parameter values for selected ports in either tabular or graphical format. The user may filter the report by parameter type.

Threshold crossing alerts

From the PM Path List the user access the Threshold Setting form which allows the user to set each of the TCA parameters for one or two ports associated with a selected transport connection, on a per granularity basis.

□

Default filter thresholds on the PM Data Reporting form

Overview

The following are three independent filters that may be applied to the tabular or graphical display of performance monitoring data.

- Standard Level 1
- Standard Level 2
- User Defined

The user selects one of these filters, displayed as tabs on the PM Data Reporting form, as the one filter that applies to the desired display of performance monitoring data.

Filters

The Standard Level 1 and the Standard Level 2 filters are derived from the ITU-T recommendation M.2101's "Default Unacceptable Thresholding" for independent monitoring. The Level 2 filter is set at the Unacceptable Threshold while the Level 1 filter is derived as 0.5 times the Level 2 filter to provide a useful range. The thresholds depend only on the measured parameter, 15-minute or 24-hour granularity, and the rate of the measured circuit/trail or link.

The User Defined filter allows user data entry of a setting that makes sense for the data at hand. The user-defined threshold entries are all initialized to "0" at the start of the first user session. Once entered, these values are available for the current and subsequent user sessions, but do not persist after a workstation reboot.

Effect of filters

When any one of the three filter tab choices (Level 1, Level 2, or User Defined) are applied to the PM Data Reporting form, the filtered performance monitoring parameter is displayed with the following modification:

```
Displayed Value for X = {Stored value of X | given that
     it is above the filter threshold}
```

No parameter displays when it is at or below its threshold, and no negative values display. The absence of a parameter (when not greater than its threshold) displays with a dash.

Keep in mind

Keep in mind the following when using default filter thresholds.

1. Where the standards do not cover a parameter explicitly, the network-element-specific guidelines are consulted to fill in the uncovered thresholds as official Navis™ Optical PM - NP default values. Some parameters may be left without default values. Where a parameter is unspecified, the value “0” displays.
2. The feature is installed on the Navis™ Optical PM - NP host, as a performance monitoring Option, with special off-line adjustments:
   - The filter table can be reinitialized anytime the Navis™ Optical PM - NP is off line.
   - The filter tables are editable with a UNIX editor.
   - The next initialization of the Navis™ Optical PM - NP GUI carries the edited filter settings, which persist from session to session, until the next edit.
3. User Defined setting are available for the current and subsequent user sessions, but they do not persist after a workstation reboot.

□

2 Fault management tasks

Overview

Purpose

This chapter describes fault management tasks that can be performed for Navis™ Optical PM - NP.

Related topics

The following topics are related to fault management.

Database synchronization

Database synchronization is done to manually repopulate the Navis™ Optical PM - NP database with network element and alarm information from an EMS. For information, refer to *Navis™ Optical PM - NP Administration Guide*.

Contents

Acknowledge an alarm	2-3
Change the fault management operational mode	2-4
Filter secondary alarms	2-5
Create a trouble ticket	2-7
Add alarms or alarmed objects to trouble tickets	2-9
Delete a trouble ticket	2-10
Delete an alarm from the Alarm List	2-11
Archive, export, and delete alarm log records	2-12
Perform a manual alarm synchronization	2-14

View alarms on a link between two network elements	2-15
View alarms on a bridge	2-16
View alarms for a network element	2-17
View alarms for an EMS	2-18
Filter non-alarm events from the Network Event Summary form	2-19
View alarm counts from the Network Event Summary	2-20
Filter/sort alarms	2-21
Display Optical Network Navigator ports with failed and unknown status	2-23

□

Acknowledge an alarm

Purpose Use this task to acknowledge an alarm. The user can acknowledge alarms from these forms:

- Traffic Correlated Alarm List
- Alarm List

Before you begin For more information on acknowledging alarms, refer to Chapter 4, "Alarm management concepts" in this information product.

Task Perform the following steps to acknowledge alarms from the Traffic Correlated Alarm List and the Alarm List.

1 From either the Traffic Correlated Alarm List or the Alarm List, select the desired alarm or alarms to be acknowledged.

Result:

The selected alarm(s) is/are highlighted.

2 Select **Actions > Acknowledge**, or click the **Acknowledge** button on the toolbar.

Result:

The selected alarms are acknowledged. Additionally, associated alarms are automatically acknowledged.

In order to see the changes displayed on the form, select **Query Again**.

END OF STEPS

☐

Change the fault management operational mode

Purpose The fault management operational mode is set at installation, however, the user has the option of changing the operational mode for their individual user ID.

Before you begin For more information about the fault management operational modes, refer to Chapter 4, "Alarm management concepts".

Task Perform the following steps to change the fault management operational mode for an individual user login ID.

1 From the Network Map, access **Administration > Preferences**.

Result:

The Preferences form displays.

2 Select the **FM Operational Mode** tab.

Result:

The FM Operational Mode tab displays.

3 Select the desired operational mode by clicking the appropriate radio button.

Result:

A dialog box advises the user that the change will only take effect for their next and subsequent sessions.

4 Click **OK**.

5 Click **OK**.

Result:

The user is returned to the Network Map.

The operational mode change will take effect for the user's next and subsequent sessions. In order to use the new operational mode, the user must log off and log on again.

END OF STEPS

Filter secondary alarms

Purpose

If the option to filter secondary alarms is not chosen at the time of installation, the user may use fault management forms to filter secondary alarms.

The user may filter secondary alarms from the following forms:

- Alarm List
- Traffic Correlated Alarm List

Before you begin

For more information about filtering secondary alarms, refer to Chapter 4, "Alarm management concepts".

Filter secondary alarms from the Alarm List

Perform the following steps to filter secondary alarms from the Alarm List.

1 Access the Alarm List by doing one of the following:

- From the Network Map select, **Fault > Alarm List**
- From the Alarm List, select **File > New Query**, or select the **New Query** button.

Result:

The **Filter** tab of the Filter/Sort for Alarm List form displays.

2 Select **Alarm Group** from the drop down list.

Result:

A list of alarm groups displays.

3 Select one or more of the filter options.

Important! By selecting all of the alarm groups except Signal Failed - Secondary, all alarms are filtered into the Alarm List except the secondary alarms.

4 Click **OK**.

Result:

The user is returned to the Alarm List, which displays the appropriately filtered alarms.

END OF STEPS

Filter secondary alarms from the Traffic Correlated Alarm List

Perform the following steps to filter secondary alarms from the Traffic Correlated Alarm List.

1 Access the Traffic Correlated Alarm List by doing one of the following:

- From the Network Map select, **Fault > Traffic Correlated Alarm**.
- From the Traffic Correlated Alarm List, select **File > New Query**, or select the **New Query** button.

Result:

The **Filter** tab of the Filter/Sort for Traffic Correlated Alarm List form displays.

2 Select `Priority` > `Primary` from the displayed drop down lists.

3 Click **OK**.

Result:

The user is returned to the Traffic Correlated Alarm List, which displays the appropriately filtered alarms.

END OF STEPS

☐

Create a trouble ticket

Purpose Use this task to create a trouble ticket. The user accesses the Trouble Ticket Details form from either the Traffic Correlated Alarm List or the Alarm List.

Before you begin For more information refer to Chapter 4, “Alarm management concepts” in this information product.

Task Perform the following steps to create a trouble ticket from either the Traffic Correlated Alarm List or the Alarm List.

1 From either the Traffic Correlated Alarm List or the Alarm List, select the alarm or alarmed objects for which a trouble ticket will be created.

> **Important!** The user may select multiple alarms or alarmed objects at once.

2 Select **Actions > Trouble Ticket > Create**.

Result:

The Trouble Ticket Details form displays.

3 In the **Trouble Ticket ID** field, type the user-defined identifier of the trouble ticket

4 ***Optional:*** In the **Owner** field, type the login ID of the user who owns the trouble ticket.

5 ***Optional:*** In the **Remarks** field, type in descriptive text associated with the trouble ticket.

6 Click the **OK** button.

Result:

The trouble ticket is created, and the user is returned to the original form.

END OF STEPS

☐

Add alarms or alarmed objects to trouble tickets

Purpose Use this task to add additional alarms or alarmed objects to an existing trouble ticket. The user accesses the Trouble Ticket Details form from either the Traffic Correlated Alarm List or the Alarm List.

Before you begin For more information on trouble tickets, refer to Chapter 4, "Alarm management concepts" in this information product.

Task Perform the following steps to add alarms or alarmed objects to a trouble ticket.

1 From the Traffic Correlated Alarm List or the Alarm List, select the alarm or alarmed object to be added to a trouble ticket.

> **Important!** The user may select multiple alarms or alarmed objects to be added at once.

2 Select **Actions > Trouble Ticket > Add selected Alarms to Trouble Ticket**.

Result:

The Trouble Ticket Details form displays.

3 In the **Trouble Ticket ID** field, type the identifier of the trouble ticket to which the selected alarms or alarmed objects will be added.

4 Click **OK**.

Result:

The selected alarm or alarm object is added to the trouble ticket, and user is returned to the original form.

END OF STEPS

☐

Delete a trouble ticket

Purpose

Trouble tickets are automatically deleted by Navis™ Optical PM - NP when all the associated alarms or the associated alarmed objects are deleted. In addition, the user may manually delete a trouble ticket from the Trouble Ticket form. In both cases, the user can view the alarm and trouble ticket information, less the remarks, from the Alarm Log.

Use this task to manually delete trouble tickets.

Before you begin

For more information on trouble tickets, refer to Chapter 4, "Alarm management concepts".

Task

Perform the following steps to delete trouble tickets. To delete trouble tickets containing alarmed objects, the user should begin this task from the Traffic Correlated Alarm List form. To delete trouble tickets containing alarms, the user should begin this task from the Alarm List form.

1 Select the alarm or alarmed object containing the trouble ticket to be deleted.

2 Select **Actions > Trouble Ticket > Delete**.

Result:

A confirmation dialog box displays.

3 Click **OK**.

Result:

The trouble ticket is deleted and the user is returned to the original form.

END OF STEPS

☐

Delete an alarm from the Alarm List

Purpose Navis™ Optical PM - NP automatically deletes persistent alarms based on a deletion option set at the time of installation. Use this task to manually delete alarms.

Deleted alarms are not removed from the system, but are moved to the Alarm Log.

Task Perform the following steps to manually delete alarms.

1 From the Alarm List, select the alarm(s) to be deleted.

2 Select **Actions > Delete**.

Result:

A confirmation dialog box displays.

3 Click **OK**.

Result:

The alarm is deleted and the user is returned to the Alarm List.

END OF STEPS

☐

Archive, export, and delete alarm log records

Purpose

Alarm log administration functions (archive, export, and delete) are performed from the Log Administration form. This form supports both the service and alarm modes. In service mode, it is used to archive, export, and delete alarm log records from the Alarmed Object Log. In both modes of operation, alarm log records in the Alarm Log can be archived, exported, and filtered.

Filtering the alarm or alarmed object records

The user must filter the alarm or alarmed object records to be archived, exported or deleted. Otherwise, all records will be archived, exported, or deleted.

Before you begin

For more information on alarm log records, refer to Chapter 4, “Alarm management concepts”.

Task

Perform the following steps to archive, export, or delete alarm log records.

1 From the Network Map, select **Fault > Alarm Log Alarm View** or **Fault > Alarm Log Service View**

Result:

The filter/sort window for the selected form displays.

2 Select the desired filter criteria and click **OK**.

Result:

The filtered Alarm Log Alarm View or Alarm Log Service View form displays.

3 Select **Actions > Log Administration**.

Result:

The Log Administration Alarm View or Log Administration Service View form displays.

4 ***Optional:*** Select **File > New Query**, and apply additional filtering criteria to the displayed alarms or alarmed objects.

5

IF	**THEN**
You want to archive alarm log records.	Enter the destination of the archive alarm log records in the **Archive To:** field.
You want to export alarm log records.	Enter the destination of the export alarm log records in the **Export To:** field. **Important!** Always enter the complete path, for example: `/usr/dacscan/my_export`.
You want to delete alarm log records.	Enter the destination of the delete alarm log records in the **Archive To:** field.

6

IF	**THEN**
You want to archive alarm log records.	Select **Actions > Archive**. **Result:** A confirmation dialog box displays.
You want to export alarm log records.	Select **Actions > Export**. **Result:** A confirmation dialog box displays.
You want to delete alarm log records.	Select **Actions > Delete**. **Result:** A confirmation dialog box displays.

7 Click **OK**.

Result:

The selected alarm log records are archived, exported, or deleted, and the user is returned to the Log Administration form.

END OF STEPS

☐

Perform a manual alarm synchronization

Purpose Navis™ Optical PM - NP provides automatic alarm synchronization in many instances. A manual alarm synchronization may also be initiated by the user. Use this task to perform an manual alarm synchronization.

Before you begin For more information on alarm synchronization, refer to Chapter 4, "Alarm management concepts".

Task Perform the following steps to execute a manual alarm synchronization.

1. Access the Network Controller Map by executing **File -> Network Controller Map**.

   Result:

   The Network Controller Map is displayed.

2. On the map, right-click the EMS node with which the manual database synchronization should be performed.

   Result:

   A Node menu appears.

3. Select **Session -> DB SYNC**.

   Result:

   The Database Synchronization form is displayed.

4. In the **EMS** field, select the name of the EMS node with which the manual database synchronization should be performed.

5. Select **Alarm**.

   Result:

   An alarm synchronization occurs with all the network elements under control of this EMS.

END OF STEPS

☐

View alarms on a link between two network elements

Purpose Use this task to view alarms on a link between two network elements.

Definition: link A link is an icon on the Network Map that represents all of the connections between two network elements. A link appears as a thin line between network elements on the Network Map.

Task Perform the following steps to view alarms on a link.

1 From the Network Map, right-click on a link.

Important! The link must be between two network elements. This task cannot be performed for links between the following:

- network elements and aggregates
- aggregates and aggregates

Result:

The Link menu displays.

2 Select **Traffic Correlated Alarm List**.

Result:

The Traffic Correlated Alarm List form displays, filtered to show alarmed objects on the link.

3 ***Optional:*** From the Link menu, select **Regenerator Status**, if displayed.

Result:

The Regenerator Status form displays.

4 Select **Actions > Alarm List**.

Result:

The Alarm List form displayed, filtered to show alarms on the link.

END OF STEPS

☐

View alarms on a bridge

Purpose Use this task to view alarms on a bridge.

Definition: bridge A bridge is an icon on the Network Map that represents all of the connections between two areas. A bridge appears as a heavy line between areas on the Network Map.

Task

1 From the Network Map, right-click on a bridge.

Result:

The Link List form displays.

2 Select **Actions > Traffic Correlated Alarm List**.

Result:

The Traffic Correlated Alarm List form displays, filtered to show the alarmed objects on the bridge.

END OF STEPS

☐

View alarms for a network element

Purpose Use this task to view alarms for a network element.

Task Perform the following steps to view alarms for a network element.

1 On the Network Map, right-click on a network element.

Result:

The Node menu displays.

2 Select **Alarm List**.

Result:

The Alarm List displays alarms filtered for the selected network element.

END OF STEPS

☐

View alarms for an EMS

Purpose On the Network Controller Map, nodes representing EMSs, (including Navis™ Optical PM - NP), change color to indicated the alarm condition of the EMS. When a node is either red or yellow, EMS platform alarms are present on the EMS.

Use this task to determine what has caused a red or yellow alarm condition on EMS nodes on the Network Controller Map.

Task

1 From the Network Controller Map, note the name of the EMS that is either red or yellow.

2 Close the Network Controller Map.

Result:

The Network Controller Map closes, and the Network Map displays.

3 From the Network Map, select **Fault > Alarm List**.

Result:

The Filter/Sort for Alarm List form opens.

4 In the Filter 1 field, select **Source** and specify **EMS** as the source.

5 In the Filter 2 field, select **EMS Id** and specify the name of the EMS.

6 Select **OK**.

Result:

The Alarm List opens filtered for the alarms on the specific EMS. This list allows the user to determine the cause of the red or yellow alarm condition of the EMS on the Network Controller Map.

END OF STEPS

☐

Filter non-alarm events from the Network Event Summary form

Purpose

The Network Event Summary form provides automatic filters with which to view alarms. Alarms can be filtered by categories of non-alarm events.

Non-Alarm Events

Alarms can be filtered into five categories by selecting one of the following buttons in the **Non-Alarm Events** section of the Network Event Summary form:

- Restoration - opens a list of new successful restoration circuit orders. This is only available if the restoration feature is used.
- Restoration Failed - opens a list of new failed restoration circuit orders. This is only available if the restoration feature is used.
- Network Discrepancy - opens a list of the Optical Network Navigator managed cross connections which are not part of a connection in Navis™ Optical PM - NP.

Task

Perform the following steps to view filtered non-alarm events from the Network Event Summary form.

1 From the Network Map, select **Fault > Network Event Summary**. You may select either the service view or the alarm view.

Result:

The Network Event Summary form opens.

2 In the Non-Alarm Events section of the form, select a button under one of the five displayed categories.

Result:

The selected list of filtered non-alarm events displays.

END OF STEPS

☐

View alarm counts from the Network Event Summary

Introduction

Alarm counts can be viewed on the Network Event Summary form.

Different categories are displayed for the alarm view and the service view.

Alarm Counts - alarm view

In the Alarm View, the user selects a button in the **Uncorrelated Alarm Counts** section of the Network Event Summary to display a filtered Alarm List, categorized by alarm status.

Alarm Counts - service view

By expanding the **Traffic Correlated Object Counts** section on the Network Event Summary - Service View, the user displays columns of buttons which categorize alarms as follows:

- alarm status and service
- alarm status and layer

Selecting buttons in these areas opens either a filtered Traffic Correlated Alarm List for correlated alarms or a filtered Alarm List for uncorrelated alarms.

Task

Perform the following steps to view alarm counts from the Network Event Summary form.

1 From the Network Map, select **Fault > Network Event Summary**. You may choose either the alarm view or the service view.

Result:

The Network Event Summary form opens.

2 To expand/contract either the **Traffic Correlated Object Counts**, or **Uncorrelated Alarm Counts** section, select the up-arrow or down-arrow key, located next to the **Totals** row in either section.

Result:

The appropriate section expands/contracts. Categories of alarms and/or alarmed object counts display in columns of **Total Raised**, **Unack'd Raised**, and **Unack'd Clear**.

END OF STEPS

☐

Filter/sort alarms

Purpose

Most of the fault management forms allow the user to filter and/or sort the information that displays on the form. Use this task to filter and/or sort the information displayed on fault management forms.

Accessing filter/sort

The user can access the sort/filter window of fault management forms in the following ways:

- When accessing a fault management form from the Network Map main menu, the user is presented with the Filter/Sort window for that particular form.
- Once the user accesses a fault management form, new filter/sort criteria can be applied by either clicking the **New Query** button, or selecting **File > New Query**.

The user may erase previously applied filter/sort criteria by selecting the **Clear** button from the Filter/Sort window.

Before you begin

For more information refer to Chapter 4, “Alarm management concepts” in this information product.

Task

Perform the following steps to filter and sort information displayed on fault management forms.

1 Access the Filter/Sort window of the desired fault management form. For more information, refer to “Accessing filter/sort” (2-21).

Result:

The Filter/Sort window displays.

2 Select either the **Filter** tab or the **Sort** tab, as appropriate.

3 Select the filter/sort criteria from the first drop-down menu.

4 To select additional filter/sort criteria, click the **More** button.

Result:

Additional filter or sort drop-down menus display from which additional criteria can be selected.

5 Repeat Step 2 until all filter/sort criteria is selected.

6 Click **OK**.

Result:

The original form displays with the specified filter/sort applied.

END OF STEPS

Display Optical Network Navigator ports with failed and unknown status

Purpose Use this procedure to display a list of Optical Network Navigator alarmed ports with a status of “failed” or “unknown”.

Before you begin For more information refer to Chapter 4, “Alarm management concepts” in this information product.

Task

1 From the Network Map, select Fault > ONN Failed Link List.

Result:

The Filter/Sort of Network Navigator Failed Link List opens.

2 Select the appropriate sort/filter criteria and then select **OK**.

Result:

The Network Navigator Failed Link List opens, displaying a list of Optical Network Navigator alarmed ports with a status of “failed” or “unknown”.

END OF STEPS

☐

3 Performance monitoring tasks

Overview

Purpose This chapter describes performance monitoring tasks that can be performed for Navis™ Optical PM - NP.

Contents

Performance monitoring tasks	3-2
Display the installed date format	3-3
Set up a monitoring point	3-4
Set a threshold value for a performance parameter	3-6
Create a data report	3-8
Delete a monitoring point	3-11
Execute the performance monitoring export tool	3-12
Change the scheduled run time of the performance monitoring file transfer	3-13
Add special archiving features for performance monitoring	3-14

☐

Performance monitoring tasks

Overview

Purpose This chapter describes performance monitoring tasks that can be performed for Navis™ Optical PM - NP.

Contents

Display the installed date format	3-3
Set up a monitoring point	3-4
Set a threshold value for a performance parameter	3-6
Create a data report	3-8
Delete a monitoring point	3-11
Execute the performance monitoring export tool	3-12
Change the scheduled run time of the performance monitoring file transfer	3-13
Add special archiving features for performance monitoring	3-14

Display the installed date format

Purpose

Use this procedure to display the installed date format. The date format is set at installation. You must adhere to the installed date format when entering any dates into the system. The date format can be set to be either of the following:

- American (MM-DD-YYYY)
- European (DD-MM-YYYY), or YYYY-MM-DD, where DD=01-31, MM=01-12 and YYYY=1970-2037.

Specifying single-digit months or days

For either format, single-digit months or days can be represented using one digit or two. For example, ”01” or “1” can be used to specify the month of January.

Task

Perform the following steps to display the installed date format.

1 From the Network Map, select **Help**.

2 Select **Date Format**.

Result:

The installed date format is displayed.

END OF STEPS

☐

Set up a monitoring point

Purpose Use this procedure to set up a new monitoring point. Monitoring points are used to identify points in the network that can be used to monitor performance.

Related information For more information on performance monitoring, see Chapter 6, "Performance monitoring parameters" in this information product.

Task Complete the following task to set up a monitoring point.

1 From the Network Map, select **Performance > PM Port List > Display/Modify**

Result:

The PM Port List Query box displays.

2 In the **CKT/DTS ID** field, enter the circuit ID.

3 From the **Trail Type** drop-down menu, select the trail type.

4 From the **Measure Period** drop-down menu, select the measure period.

5 Click the **OK** button.

Result:

The PM Port list displays.

6 Select one or more ports from those displayed on the PM Port List.

7 This function must be performed at the EMS level. In the **Schedule Start Collection** area, select a starting period.

IF	**THEN**
You want collection to start immediately.	Select the **Start > Now** check box.
You do not want collection to start immediately.	Under **Actions** select a starting period as follows: • In the **Date** field, enter the start date. • In the **Time** field, enter the start time.

8 This function must be performed at the EMS level. In the **Schedule Stop Collection** area, select a stopping period. The default is to continue collecting indefinitely or until a user, at some later time, stops the collection.

IF	**THEN**
You want collection to stop immediately.	Select the **Stop > Now** check box.
If you do not want collection to stop immediately.	Under **Actions**, select a stopping period as follows: • In the **Date** field, enter the stop date. • (Optional) Enter the stop time in the **Time** field.

9 Click **OK**.

Result:

The monitoring point is set, and the PM Port List form closes.

END OF STEPS

☐

Set a threshold value for a performance parameter

Purpose Use this procedure to set or change the threshold levels for parameters on a network element that supports threshold setting and reporting.

Related information For more information on threshold setting for performance parameters, see Chapter 6, "Performance monitoring parameters".

Task Complete the following task to set or change the threshold levels for parameters on a network element that supports threshold setting and reporting.

1 From the Network Map, select **Performance > PM Path List> Display/Modify**.

Result:

The PM Path List Query Box displays.

2 Enter the appropriate information in the **Circuit ID**, **Location**, **Data Collection From Date,** and **Data Collection To Date** fields.

3 Click **OK**.

Result:

The PM Path List displays.

4 Select the path.

5 Select **Actions > Threshold Setting**.

6 In the **Trail Type-Measurement** scrolling lists, select the trail type and measurement periods.

7 Enter a threshold value for a particular parameter, and the port (either A, Z, or AZ) supporting that parameter.

For valid ranges, see the network element user manuals.

8 Click **Apply**.

Result:

Commands are sent to the appropriate network elements to set the new thresholds.

END OF STEPS

☐

Create a data report

Purpose Use this procedure to generate a report that contains performance monitoring data collected from the network. Data can be accessed on a port basis. The report can be displayed on the screen or can be sent to a printer.

Related information For related information, see Chapter 6, "Performance monitoring parameters".

Task Complete the following task to generate a report that contains performance monitoring data collected from the network.

1 From the Network Map, select **Performance > PM Path List > Display/Modify**.

Result:

The PM Path List Query Box containing Circuit ID, Location, and Data Collection displays.

2 Enter information in the **Circuit ID**, **Location**, and **Data Collection** fields.

3 Click the **OK** button.

Result:

The PM Path List displays.

4 Select a path.

5 Select **Actions > Data Reporting**.

Result:

The PM Data Report Query box displays.

6 From the scrolling list, select the trail type and measure period.

7 Accept the port/locations, or select the port from the list of available ports.

8 Enter the **Start Date/Time** for the time interval on which you wish to see a report.

Important! For 24-hour reports, enter the date only. Do not enter the time for 24- hour reports.

9 Enter the **Stop Date/Time** for the time interval on which you wish to see a report.

Result:

If Navis™ Optical PM - NP was not able to collect data during the scheduled time interval (either the network element was not available, or the time interval exceeds that of the scheduled Start/Stop date and time), then the periods that were not collected will be reported as NA (Not Available).

10 Click **OK**.

11 Select the parameters you wish to view on the report from the list. Select as many as you wish to display.

12 Select **Threshold Levels**.

The ITU standard filters are as follows:

- Level 2 contains the threshold values as per specified ITU standards.
- Level 1 is half the Level 2 threshold values.
- User-defined values are determined by the user.

13 Click **OK**.

14 If you wish to print the report, select **File > Print**.

Result:

The Printer Selection form displays.

15 Select a printer.

Result:

The report is sent to the printer.

16 Click **Apply** .

Result:

The collected data displays in the specified report format.

END OF STEPS

☐

Delete a monitoring point

Purpose Use this procedure to delete a monitoring point.

Related information For more information on performance monitoring, see Chapter 6, “Performance monitoring parameters” in this information product.

Task Complete the following task to delete a monitoring point.

1 From the Network Map, select **Performance > PM Path List > Display/Modify**.

Result:

The PM Path List Query Box displays.

2 Enter Circuit ID, Location, and Data Collection information.

3 Click **OK** .

Result:

The PM Path List displays.

4 Select the monitoring point.

5 Select **Actions > Delete**.

Result:

A confirmation window displays.

6 Click **Yes** .

Result:

The monitoring point is deleted.

END OF STEPS

☐

Execute the performance monitoring export tool

Performance monitoring administration

The following performance monitoring tasks are performed by the System Administrator.

- Execute the performance monitoring export tool
- Change the scheduled run time of the performance monitoring file transfer
- Add special archiving features for performance monitoring

For further information

For further information on performance monitoring administration tasks see *Navis™ Optical PM - NP Administration Guide*

☐

Change the scheduled run time of the performance monitoring file transfer

Performance monitoring administration

The following performance monitoring tasks are performed by the System Administrator.

- Execute the performance monitoring export tool
- Change the scheduled run time of the performance monitoring file transfer
- Add special archiving features for performance monitoring

For further information

For further information on performance monitoring administration tasks see *Navis™ Optical PM - NP Administration Guide*

☐

Add special archiving features for performance monitoring

Performance monitoring administration

The following performance monitoring tasks are performed by the System Administrator.

- Execute the performance monitoring export tool
- Change the scheduled run time of the performance monitoring file transfer
- Add special archiving features for performance monitoring

For further information

For further information on performance monitoring administration tasks see *Navis™ Optical PM - NP Administration Guide*

□

4 Alarm management concepts

Overview

Purpose This chapter describes fault management concepts for Navis™ Optical PM - NP.

Contents

Alarm collection	4-2
Alarm classification	4-4
Alarm correlation	4-7
Fault state determination	4-12
Alarm and alarmed object suppression	4-19
Service impact assessment	4-21
Alarm deletion	4-23
Alarm acknowledgement	4-24
Domain partitioning	4-26
Trouble ticketing	4-27

☐

Alarm collection

Introduction

Navis™ Optical PM - NP is notified for each EMS it manages about all of the following:

- Network element alarm raise and clear events reported to the EMS
- Network element loss of associated events
- EMS platform management alarms
- All TCA (threshold crossing alert) events
- All Optical Network Navigator alarm raise and clear events
- All Optical Network Navigator management alarms, including loss of association with another Optical Network Navigator module

Alarms received from the network

Navis™ Optical PM - NP validates each fault event (raise and clear) it receives from the EMS and checks the event for duplication. If the alarm does not exist, it is maintained and processed. Navis™ Optical PM - NP checks that the alarm is from a valid network element/EMS combination that it manages. Navis™ Optical PM - NP checks that the alarm is unique for a particular EMS/alarm ID combination, or EMS/actual probable cause/alarm source/raise time combination in the absence of an alarm ID.

Raise and clear events

If an alarm or TCA raise event occurs and it does not exist on the system, Navis™ Optical PM - NP maintains and processes the alarm or TCA raise event. If an alarm or TCA clear event occurs and it does not exist on the system, and if there is a peer raise event in the system, Navis™ Optical PM - NP maintains and processes the alarm or TCA clear event.

Double raise event

If a new raise alarm or TCA event is received, where an existing raise event exists, both records are kept. In this case, a clear event has been missed for the first raise, and the user will need to perform a database synchronization to resolve the instance of the double raise.

Clear with no raise events

If Navis™ Optical PM - NP receives a new clear event for which there is no raise event, the clear event is dropped.

Alarm synchronization

A synchronization of alarms can be performed with all supported EMSs and Optical Network Navigator modules.

Navis™ Optical PM - NP provides on-line alarm synchronization for a particular network element, for all the network elements controlled by an EMS, and for all management alarms and TCAs on an EMS.

Alarm synchronization is automatically initiated in the following instances:

- At system start up, Navis™ Optical PM - NP performs an alarm synchronization for all network elements as each EMS session is established.
- The system performs an alarm synchronization for a recovered network element, when the system receives a network element-status clear.
- The system performs an alarm synchronization for a recovered EMS for all controlled network elements.

The alarm synchronization can also be manually initiated by the user by performing database synchronizations with the EMSs and network elements. For more information, refer to *Navis™ Optical PM - NP Administration Guide*.

□

Alarm classification

EMS alarms

Alarms are sent by the EMS, along with their mapped G7 2.0L probable causes, to Navis™ Optical PM - NP. The alarms are then mapped by Navis™ Optical PM - NP to an Alarm Group and Alarm Category, which is used for sorting and filtering the alarms. The mappings of fault notifications to the alarm groups use a combination of the probable cause, alarm type, and service-affecting value. Navis™ Optical PM - NP also uses the mapping to determine whether correlation is attempted for each alarm group. For those groups which are correlated, Navis™ Optical PM - NP determines the fault state of the alarmed object.

Alarm groups

Navis™ Optical PM - NP uses a combination of the G7 2.0L probable cause, alarm type, and service impact to map fault notifications to the Alarm Groups. This combination also determines whether or not correlation is attempted for each Alarm Group. For those groups which should be correlated, the Alarm Group determines the processing required, and indicates the fault state of the source of the alarm. For more information on correlation, refer to “Alarm correlation” (4-7) in this information product.

The Navis™ Optical PM - NP Alarm Groups are as follows:

- Environment (MDI and MDO)
- Miscellaneous
- Timing
- Equipment - uncorrelated
- Equipment - correlated
- EMS
- Threshold Crossings
- Signal Fail - Primary
- Signal Fail - Loss of Multiframe
- Signal Fail - secondary
- Signal degrade
- Protection Switch
- Misconnections

- NMS
- Capacity Degrade

The Alarm Group for all alarms raised by the Navis™ Optical PM - NP is NMS, except for "NE loss of association alarms", which are mapped into the EMS Alarm Group. All of these are uncorrelated alarms.

Threshold crossing alerts

The following list describes how Navis™ Optical PM - NP handles TCAs:

- **Navis™ Optical EMS**: TCA data from Navis™ Optical EMS is converted into a G7 2.0L message and transmitted to Navis™ Optical PM - NP.
- **Navis™ Optical PM - NP:** Navis™ Optical PM - NP maps the probable cause to an alarm and handles the alarm using the normal alarm mechanisms.

If a G7 2.0L TCA event arrives containing multiple notifications, Navis™ Optical PM - NP splits them out and handles them individually. If they are passed on northbound, they are kept as separate entities.

A trail ID is appended to the TCA entry in the Alarm List, however the TCAs do not appear on the Traffic Correlated Alarm List. TCAs are not propagated.

TCAs are resynched southbound following loss of association between an EMS and network elements, between Navis™ Optical PM - NP and an EMS, or automatically at start up.

Alarm categories

Navis™ Optical PM - NP uses alarm categories to filter and sort alarms on forms for fault management. Alarms that do not require correlation are mapped to an alarm category as follows:

Table 4-1 Alarm categories

Alarm Group	**Alarm Category**
Environment	Environment
Miscellaneous	Non-traffic
Timing	Non-traffic
Equipment - uncorrelated	Non-traffic
EMS	EMS

Table 4-1 Alarm categories (continued)

Alarm Group	Alarm Category
Threshold Crossings	Threshold Crossing
Protection Switch	Non-traffic
NMS	NMS

Severity mapping Navis™ Optical PM - NP maps the severity of the alarm received from an EMS to the severities used in G7 2.0L as follows.

Table 4-2 Severity mapping

Navis™ Optical PM - NP Optical EMS	Navis™ Optical PM - NP Severity	Notes
Critical	Critical	No equivalent to this in the prompt scheme. No simple rules for knowing which prompt to make critical.
Major	Major	
Minor	Minor	
	Warning	
	Indeterminate	Indeterminate is used for the reported TCAs because the severity can be prompt or info depending on the source.

□

Alarm correlation

Introduction

Navis™ Optical PM - NP attempts to match the source of an alarm, of which it may or may not have knowledge, to a network resource in its managed network. The network resource to which the alarm is correlated becomes an alarmed object.

All alarms are mapped to an alarm group which requires correlation are referred to as “correlatable.”

Types of alarmed objects

There are three possible types of alarmed objects:

- Trail alarmed object
- Equipment alarmed object
- Port alarmed object

Regardless of the outcome of the correlation process, the alarm is mapped to the Traffic alarm category.

Alarmed objects for termination point alarms

When a correlatable alarms is issued by a termination point, it is correlated to a connection in the Navis™ Optical PM - NP database. There are four possible results of this correlation:

- A “catalogued connection” which is not associated with an Optical Network Navigator mesh connection is found. In this case, the alarm is linked to a trail alarmed object.
- A “catalogued connection” which is associated with an Optical Network Navigator mesh connection is found. In this case the alarm is not linked to an alarmed object.
- An “uncataloged connection” is found. In this case the alarm is linked to a port alarmed object.
- No connection is found. In this case the alarm is uncorrelated and is not linked to an alarmed abject.

Catalogued and uncataloged connections

In a transport network, a hierarchy of connections are defined. In the Navis™ Optical PM - NP database, it is possible to create a connection at one of the client layers without the server layer in existence. Both connections actually exist in the network, however, Navis™ Optical PM - NP does not know of the server’s existence.

Catalogued connection

Internally the Navis™ Optical PM - NP database is aware of the created connection. The connection is referred to as a catalogued connection.

A catalogued connections is associated with an Optical Network Navigator mesh connection only if the catalogued connection the alarm would be correlated to is:

- an optical channel mesh connection which is managed by Optical Network Navigator, or
- an optical link connections whose client optical channel link connection is used in an Optical Network Navigator mesh connection, or is unused, but allocated to an Optical Network Navigator domain.

Uncataloged connection

An uncataloged connection is any uncreated connection which has one or more catalogued client connections.

Alarmed objects for equipment alarms

Where the source of an alarm is a piece of equipment an equipment alarm alarmed object is created. This alarm may come with a list of termination points, which Navis™ Optical PM - NP can match with termination points used by “in-effect” trails to determine which trails are affected by the equipment failure.

Internal or external alarmed objects

When a failure occurs on a connection, Navis™ Optical PM - NP indicates whether the cause of that failure occurred inside or outside of the management domain. An internal failure is one that occurred inside the management domain. An external failure is one that occurred outside the management domain.

For each alarmed resource in the network, the alarmed object indicates if the failure is internal or external.

- All equipment alarmed objects are internal.
- For trail/port alarmed objects, whether the alarmed object is internal or external depends on if the port is on the boundary of the network.
    - If the alarm is raised on a boundary port, the alarmed object is external.
    - If the alarm is raised on a non-boundary port, the alarmed object is internal.

Optical Network Navigator alarmed objects

An alarmed object is considered to be part of an Optical Network Navigator domains only the following conditions are met:

- the alarmed object was created due to a connection alarm issued by an Optical Network Navigator
- the alarmed object was created due to a termination point alarm and was correlated to an optical link connection whose client optical channel link connection is under control of Optical Network Navigator.

Boundary and non-boundary ports

The following are descriptions of boundary and non-boundary ports.

Boundary ports

A boundary port is one which is on the edge of the management domain of Navis™ Optical PM - NP. A boundary port is identified by checking the following:

1. The port is a connection termination point (CTP) which is cross connected but not link connected to another termination point within the management domain. This means it is the final port on a catalogued connection which crosses the Navis™ Optical PM - NP domain boundary.
   A link connection to a black box does not count as a link connection to a termination point.
2. The port is a trail termination point (TTP) in an uncataloged connection, which has client connection termination points which the circumstance described in (1) above. This means it is the final port on an uncataloged connection which crosses the Navis™ Optical PM - NP domain boundary.

Non-boundary port

A non-boundary port is one which is in the middle of a connection.

Alarms types

The following alarms are ones that are correlated.

Protection switch alarms

There are two groups of alarms related to protection switching.

They are:

- PSF - Protection Switch Fail. This group of alarms indicate that protection switching has failed. This may be due to the protection switch being locked, or it may be because both the service circuit and protection have failed. Transmission protection switch failures are mapped to the signal fail-primary alarm group. Equipment protection switching failures are mapped to the “equipment - traffic correlated” alarm group if they are on the following:
    - trib cards
    - line cards
    - matrix and transfer boards
    - PPU’s (pointer processing units)

  Otherwise, equipment protection switching failures are mapped to the “equipment – uncorrelated” alarm group.
- PS - Protection Switch. This is raised when the switch operates and the traffic in one direction has switched from the service circuit SNC (subnetwork connection) to the protection SNC. This alarm clears when the switch reverts so the traffic is once again carried on the service circuit path.

Equipment alarms

Equipment alarms have an indication of whether or not they are service affecting. The possible service affecting values are:

- Unknown - (SA_UNKNOWN)
- Service failed - (SF_SERVICE_FAILED)
- Service Degraded - (SD_SERVICE_DEGRADED)
- Non-service affecting - (NSA_NON_SERVICE_AFFECTING)

All equipment alarms are service failed, service degraded or non-service affecting. All equipment alarms which are service failed or service degraded are correlated. This means they result in an equipment alarmed object.

For equipment failures which impact traffic:

- Alarms indicating a protected piece of equipment has failed are marked as service degraded.
- Alarm indicating all the equipment in a protecting relationship has failed are marked as service failed.

□

Fault state determination

Introduction

Navis™ Optical PM - NP considers all trails and subnetwork connections bidirectional. Therefore, a failure in either direction indicates that the trail or subnetwork connection is no longer working.

Whenever a new alarm raise or clear is correlated to an alarmed object, Navis™ Optical PM - NP determines the fault state.

Fault state values

The following are the fault state values used in Navis™ Optical PM - NP:

Failed

- For a trail alarmed object, a fault state value of failed means that traffic is not reaching at least one end point, either due to a direct failure or an alarmed server failure.
- For an equipment or a port alarmed object, it means there is no protecting entity.

Degraded

- For a trail alarmed object, this state means it has lost protection at that layer, or the signal being transmitted by this connection contains a high number of bit errors.
- For an equipment alarmed object or a port alarmed object, degraded means that either the working equipment or port has failed, or that the protection equipment or port has failed.

Capacity degraded

This fault state is only supported for virtual concatenation groups. For a trail alarmed object, there is no direct failure, but there is insufficient server capacity to support full capacity requested for the connection.

Working

For all alarmed objects, working means there are no alarms directly correlated to this object, and it is not affected by any alarmed server failure.

Direct fault state

The following are direct fault states for alarmed objects.

Port Alarmed Objects

The fault state for a port associated with active alarms is always “failed,” unless the boundary port is protected, or the only associated alarm is for a signal degrade, in which case the fault state value is “degraded.”

> **Important!** Boundary ports on a Y-protection scheme are marked as failed even if they are at the open end of the Y. It is the propagation of the failure onto the trail that may result in a degraded rather than a failed fault state.

Equipment alarmed objects

Navis™ Optical PM - NP uses the service-affecting value supplied with the alarm to set the fault state.

Trail alarmed object

The trail may be an optical link, digital link, or a path layer trail.

Protection of these trails may be as follows:

- A digital link may be protected by a bidirectional line switched ring (BLSR).
- An Optical Multiplex Section (OMS) may be protected by Optical Multiplex Section Protection (OMSP).
- An Optical Channel (OCh) path layer trail may be protected by Optical Ring Switch (ORS) Protection, or by Optical Network Navigator 1+1 or mesh protection.

For unprotected trails, at any layer associated with raise alarms, the fault state is “failed” unless the only associated alarms are signal degrade alarms, in which case the fault state value is “degraded.”

For an APS-protected digital link, the fault state is “degraded” if:

- Only signal degrade alarms have been correlated to this trail.
- A primary alarm is received on a port that is currently idle (traffic is using the other port).
  This may result in an incorrect fault state if two unrelated unidirectional failures are received, which result in one direction of traffic flowing on the service circuit SNC, and the other direction on the protection SNC.
- The fault state is “failed” if a primary alarm is received on a active port (one which is carrying traffic).

For a digital link in a 2- or 4-fiber BLSR protection scheme, the fault state is “failed” unless the only associated alarms are signal degrade alarms, in which case the fault state value is “degraded.”

For Optical Network Navigator protected optical channels, the following applies:

- Mesh protected: the fault state is always “failed”
- 1+1 protection: the fault state is “degraded” if one path has failed. If both paths have failed the fault state is “failed”.

Fault state determination for a partially protected connection is based on examining the unprotected and protected segments of the trail separately, and then determining the impact of the trail as a whole. Navis™ Optical PM - NP determines the fault state of the path to be the highest severity of any segment in the trail, whether it is protected or unprotected.

Navis™ Optical PM - NP determines the fault state for a protected connection based on examining both unreliable bidirectional subnetwork connections (SNCs). The fault state of the protected SNC is determined as follows:

1. If protection switch failure is received for this protected SNC, the fault state is “failed.”
2. If primary or secondary alarms are received on both unprotected SNCs, then the protected SNC is “failed.”
3. If a primary or secondary alarm is only received on one unprotected SNC, the protected SNC is “degraded.”

Fault state propagation

Objects on which alarms have been received are directly failed or degraded. Because SONET and optical layers are hierarchical in nature, a failure in the server layer has a consequential impact on any client layers, resulting in an indirect failure of the client layers.

Only the server fault state of “failed and “working” are propagated to the client layers. If the server fault state is “degraded,” the degraded state is not propagated.

To assess the impact on client layers, Navis™ Optical PM - NP propagates the fault state to the client trails for all newly alarmed objects. The fault state is also propagated to the client trails when the fault state of the alarmed object changes.

Indirect fault state determination

The following describes the indirect fault state of alarmed objects.

Trail alarmed objects

Faults on a server are propagated to all client trails.

The client trails each have their own fault state and become either failed or degraded as a result of the server failure. The fault state of an unprotected client matches the fault state of the server.

For protected client trails, Navis™ Optical PM - NP performs more complex assessments to determine the fault state.

If the server trail is a digital link, Navis™ Optical PM - NP checks whether it belongs to a protection scheme, such as APS.

Equipment alarmed objects

For equipment alarmed objects with an Affected TP List, Navis™ Optical PM - NP propagates the failure to any trails using those termination points. It then checks whether the trails are servers, and if necessary, propagates the failure through the connection layer.

Port alarmed objects

Port alarmed objects may be PDH, SONET, Optical, or LAN.

For PDH port alarmed objects the associated connection will either be a PDH circuit or a combo circuit. These will be services in their own right and therefore the fault will only be propagated to a single bi-directional trail, or potentially two uni-directional client trails.

For SONET and Optical port alarmed objects the fault must be propagated to any client TP’s of those ports, and thus to any trails using those client ports.

For Ethernet ports supporting virtual concatenation, there are no clients, therefore these connections can never be uncatalogued and so cannot have a port alarmed object created on them. Ethernet ports not supporting virtual concatenation, or ports of unspecified format (e.g. HSBB, LSBB), can have port alarmed objects created on them. In this case, the failure will be propagated to all clients of the connection.

Propagation of alarms from Optical Network Navigator

Alarms correlated directly to Optical Network Navigator domain link connections or to connections that serve the Optical Network Navigator domains are only propagated to Optical Network Navigator unprotected and 1+1 protected optical channels and their clients. Alarms that correlate directly to Optical Network Navigator domain optical channel connections propagate all clients as normal.

Overall fault state

It is possible for a trail to be both directly and indirectly failed. In this case, the Navis™ Optical PM - NP uses the highest value of these two failures.

Fault state reassessment following provisioning changes

Navis™ Optical PM - NP reassesses the fault state after the following provisioning changes:

- Trail creation
- Trail deletion
- Trail modification
- MS-SPRING creation
- Inserting optical layers in a digital link

Trail creation

When a trail is provisioned, Navis™ Optical PM - NP searches for:

- all alarms that can be correlated to the trail. If alarms are found, each alarm is processed as if the alarm event was just received. If there are associated alarms, then either the trail becomes a trail alarmed object of the originating port becomes a port alarmed object. For trail alarmed objects, Navis™ Optical PM - NP determines whether it is a primary or secondary alarmed object.
- all directly or indirectly failed serving connections. The provisioned trail becomes directly failed or degraded as appropriate due to a failed server, as a result of the fault state determination rules. If it is indirectly failed, then it appears in the Affected Trails List, but not in the Traffic Correlated Alarm List.

Trail deletion

If a deprovisioned trail is a trail alarmed object, or the port at either end was alarmed, Navis™ Optical PM - NP makes the trail alarmed object or port alarmed object historic. Each of the alarms correlated to the trail or port become uncorrelated alarms.

If a deprovisioned trail is one where the port at one end was the client of a port alarmed object, Navis™ Optical PM - NP checks whether there are other trails served by the port alarmed object. If there are no clients, the port alarmed object becomes historic and the associated alarm becomes an uncorrelated alarm.

Trail modification

When a user adds or removes protection subnetwork connections, or changes the route taken by a connection, including changes on one of the end points, Navis™ Optical PM - NP reassesses the state of the connection based on the new routing. As a result, alarms can change from correlated to uncorrelated or vice versa. If the connection state changes from failed of degraded to working, the alarm becomes historic. If the connection changes state from failed to degraded or vice versa, the alarm is updated on the Traffic Correlated Alarm List and the original alarm becomes historic. If the connection state changes and there are client connections, Navis™ Optical PM - NP performs a fault state propagation.

MS-SPRING creation

When the user completes a ring that supports MS-SPRING, Navis™ Optical PM - NP checks whether any of the constituent digital links are failed.

Inserting optical layers in a digital link

When a user adds optical layers into a digital link, Navis™ Optical PM - NP checks the fault state of the connections. If any are failed, then Navis™ Optical PM - NP performs a fault state propagation.

Network element behavior and management domain visibility

Navis™ Optical PM - NP makes some assumptions about network element operation when determining the fault state.

Several network elements report secondary alarms on a trail termination point as a result of a server failure. Several report protection switch fail. Additionally, some network elements support per instance report setting for alarms.

Where fault state determinations rely on using the end port server signal fail/alarm indication signal and/or protection switch fail to indicate that a protected connection has failed rather than just being degraded, this will only be guaranteed to be successful if both of the following conditions exist:

1. The network elements used by the trail generate these types of alarms.
2. The appropriate ports are within the management domain.

In the case when one or both ends of the client services are in the management domain, the secondary alarms on the end ports are used to indicate that the service has failed.

In the case where neither end is visible, then the presence of a protection switch fail is used to determine the fault state of “failed.”

In the case where the end ports are not visible to the management domain, and the network element supporting the protected cross connection does not generate protection switch fail, the fault state calculated by Navis™ Optical PM - NP is not guaranteed to be correct. □

Alarm and alarmed object suppression

Introduction

To limit the amount of information displayed to a user, Navis™ Optical PM - NP provides both alarm suppression and trail alarmed object suppression, so that only the cause of a problem is indicated.

When a server fails, the network element detecting that failure could generate alarms for all the clients of that server. Navis™ Optical PM - NP receives the alarms for the server failure as a primary alarm. It is possible (based on network element and EMS settings) to also receive the client alarms as secondary alarms. Navis™ Optical PM - NP evaluates and determines whether alarms are primary or secondary.

Since Navis™ Optical PM - NP correlates both primary and secondary alarms with trails, potentially the primary and secondary alarms will result in multiple trail alarmed objects.

Alarm suppression

The user can achieve simple alarm suppression on the Alarm List by filtering out all the alarms in the signal fail - secondary alarm group field.

Alarmed object suppression

For every trail alarmed object, Navis™ Optical PM - NP determines whether it is a primary or a secondary alarmed path. All port and equipment alarmed objects are primary and are never suppressed.

Alarmed trail suppression is available both as an installation option and as a filter option on the Traffic Correlated Alarm List. If trail alarm suppression is chosen at installation time, secondary alarmed paths do not appear on the Traffic Correlated Alarm List, however secondary alarmed paths do display in the Affected Trails List.

Where alarmed trail suppression is not set at installation, the user can filter out the secondary alarms on the Traffic Correlated Alarm List.

Primary and secondary alarms

For every trail or port alarmed object, Navis™ Optical PM - NP determines whether it is primary or secondary. This helps distinguish the root cause (primary) of a failure from the alarms which may be a consequence of that root cause alarm. Consequential (secondary) alarms may be suppressed or filtered from view by the user.

For connection alarms from Optical Network Navigator, primary or secondary alarms are defined as follows:

- Connection failure alarms, where the connection is mesh protected, are considered primary.
- Connection failure alarms, where the connection is unprotected, or 1+1 protected, are considered secondary.

□

Service impact assessment

Introduction

Navis™ Optical PM - NP assesses and reports on the service impact for alarmed objects. The service impact assessment information reported on user forms is the highest priority fault state of any of the impacted services. Each time the fault state of an alarmed object changes, Navis™ Optical PM - NP reevaluates the service impact.

Services

Services are trails that are in the path layer and are non-assignable. Non-assignable trails do not have clients. Only services with “in-effect” trails are considered when determining the service impact for an alarmed object.

Service impact of alarmed object

This section dezcribes the service impact of alarmed objects.

Trail alarmed objects

A trail alarmed object may be a service, or its client trails may be services. An alarmed object can carry many services, but only the highest priority failure is reported.

Equipment alarmed objects

For cards with equipment alarms with affected termination points, the service impact reported is the highest priority fault state of the affected trails.

For cards with no affected termination points, the service impact reported is the same as the fault state.

Port alarmed objects

For PDH and SONET path layer ports, the service impact is the fault state of the single impacted connection.

For all line ports and optical path layer ports, the service impact is the highest priority fault state of the affected trails.

Service impact values

The values for service impact, are:

Working - all the associated alarms on the alarmed object have been cleared, and its client services are not impacted by any other failures.

Service degraded - where the server is degraded or it will impact a client on a protected SNC.

Capacity degraded - the server failure contributes to a insufficient server capacity condition on a virtual concatenation group.

Service failed - where the server failure impacts a client on a protected segment and the fault state of the client is failed because of another alarm. Navis™ Optical PM - NP is not certain the server failure is the cause of the client failure.

No services - the alarmed object is not carrying any services.

Calculating - Navis™ Optical PM - NP is still doing fault propagation, this must be completed before the service impact can be determined.

□

Alarm deletion

Introduction

Navis™ Optical PM - NP has two types of alarm deletion:

1. Removal of alarms from the Alarm List.
2. Deletion of alarms from the system as a whole.

Delete alarms from the Alarm List

Navis™ Optical PM - NP provides two possible ways to remove alarms from the Alarm List:

1. A configured deletion option set a installation time. For more information, refer to "Installation options" (1-16) in this information product.
2. Automatic deletion initiated by the system because the system-configured limit has been reached. When the number of stored current alarms reaches 75% and 95% of the system limit, Navis™ Optical PM - NP raises instantaneous platform alarms.

Once alarms are removed from the Alarm List, Navis™ Optical PM - NP places them in the Alarm Log.

Deletion of alarm log records from the Alarm Log

The limit for the number of alarm log records that are held in the Alarm Log is 300,000. Navis™ Optical PM - NP provides three possible ways to remove alarms from the system as a whole:

- Manual deletion of alarm log records from the Alarm Log. Instantaneous alarms must always be manually deleted. For more information, refer to Chapter 2, "Fault management tasks".
- Automatic deletion by the system when an alarm has been in the Alarm Log for 30 days.
- Automatic deletion initiated by the system due to exhaustion of file storage. When the number of stored current alarms reaches 75% and 95% of the system limit, Navis™ Optical PM - NP raises instantaneous platform alarms. These serve to recommend that the user archive alarm records if necessary. For more information, refer to Chapter 2, "Fault management tasks". Upon reaching the 95% limit, Navis™ Optical PM - NP attempts to move 15% of the alarm log records from the system.

□

Alarm acknowledgement

Introduction

Alarm acknowledgement is about recognizing alarms raised on the network. A user can always acknowledge a raised alarm. Depending on options set for alarm deletion at installation, it may also be necessary for the user to acknowledge a clear.

Navis™ Optical PM - NP retains the following acknowledgement details:

- Acknowledgement date and time
- Acknowledgement user

Acknowledging alarms

Alarms are acknowledged from both the Alarm List and the Traffic Correlated Alarm List.

Traffic Correlated Alarm List acknowledgement

A user can acknowledge all alarms from the Traffic Correlated Alarm List, regardless of the fault management operational mode selected.

When a user requests acknowledgement from the Traffic Correlated Alarm list, all associated alarms are acknowledged. The acknowledgement details are displayed in both the Traffic Correlated Alarm List and associated Alarm List records. When new alarms are received, the acknowledgement details are reset in the Traffic Correlated Alarm List. This does not, however, reset the acknowledgement for the associated alarms in the Alarm List.

A user can request multiple records for acknowledgement at one time.

Alarm List acknowledgement

From the Alarm List, which alarms can be acknowledged depends on the fault management operational mode the user has selected.

- Alarm Approach Mode - In this mode, the user can acknowledge any of the alarms from the Alarm List.
  Acknowledgement details display in the Traffic Correlated Alarm List only if the alarmed object is acknowledged, and no new associated alarm is subsequently raised. If a new associated alarm is raised, then the acknowledgement details are reset.

In the case where, due to user acknowledgement from the Alarm List, there is more than one set of acknowledgement details associated with an alarmed object, only the most recently acknowledged alarm displays in the Traffic Correlated Alarm List. The user can access the Alarm List from the Traffic Correlated Alarm List to view the complete acknowledgement details for each associated alarm.

- Service Approach Mode - In this mode, a user can only acknowledge uncorrelated alarms from the Alarm List. Correlated alarms must be acknowledged from the Traffic Correlated Alarm List.

□

Domain partitioning

Background

Navis™ Optical PM - NP provides filtering for Service Domain Partitioning users.

Optical Network Navigator domain

The Optical Network Navigator domain manages connectivity between Optical Network Navigator controlled network elements, including their associated ports. Also included in the domain are ports on Optical Network Navigator controlled network elements that form the edge of the domain. Once this connectivity and these ports are assigned, they are available for the Optical Network Navigator to use in provisioning.

A termination point is considered part of the Optical Network Navigator domain if it is:

- an optical channel termination point which is part of the Optical Network Navigator domain.
- an optical link termination point which is assigned to the Optical Network Navigator domain.

□

Trouble ticketing

Introduction

Trouble tickets are used to record the information regarding how a problem is being resolved.

Trouble ticket process

Trouble tickets are created, modified or deleted by selecting the appropriate record on the Alarm List or Traffic Correlated Alarm List.

To attach a trouble ticket to an existing repeat alarm, the user must select the identical current alarm from the Alarm List. Once it is created, the trouble ticket applies to the current alarm its associated repeat alarms. The trouble ticket only displays the current alarm for the repeated alarm set.

Repeat alarms are only deleted for a trouble ticket when the identical current alarm in the Alarm List is deleted. When the current alarm is deleted, all repeat alarms are also deleted.

When all associated alarms or the alarmed object are deleted (made historic) from either the Alarm List or the Traffic Correlated Alarm List, the associated trouble ticket is automatically made historic.

When using the Service Approach Mode the user is not allowed to create trouble tickets for traffic correlated alarms in the alarm list. When using the Alarm Approach Mode, the user can create trouble tickets from either the Alarm List or the Traffic Correlated Alarm List.

□

5 Fault management fault lists

Overview

Purpose This chapter contains alarm lists for the network elements and EMSs that Navis™ Optical PM - NP supports.

Contents

Section I: Navis™ Optical EMS fault lists	5-2
Navis™ Optical EMS management alarms	5-3
Navis™ Optical EMS: WaveStar® BandWidth Manager and OC192 network elements fault list	5-4
Navis™ Optical EMS: WaveStar® OLS 1.6T Family fault list	5-6
Navis™ Optical EMS: LambdaRouter™ AOS fault list	5-7
Section II: Navis™ Optical PM - NP fault lists	5-8
Navis™ Optical PM - NP fault list	5-9

☐

Section I: Navis™ Optical EMS fault lists

Overview

Purpose This section contains fault lists for the Navis™ Optical EMS and network elements

Contents

Navis™ Optical EMS management alarms	5-3
Navis™ Optical EMS: WaveStar® BandWidth Manager and OC192 network elements fault list	5-4
Navis™ Optical EMS: WaveStar® OLS 1.6T Family fault list	5-6
Navis™ Optical EMS: LambdaRouter™ AOS fault list	5-7

☐

Navis™ Optical EMS management alarms

Overview

This list provides mapping and classification information for each alarm, identified by its unique fault type.

The table consists of the following fields:

- Fault: network element fault type.
- Text: the text for the network element fault type.
- G7 2.0 PC: the mapping to the G7 2.0 probable cause.
- R/NR: values of “R”, for reported to Navis™ Optical PM - NP, or “NR” for not reported to Navis™ Optical PM - NP.
- Persistency: lists whether the alarm is persistent or transient.

Displaying the fault list

The fault list can be viewed using browser software in the following ways:

- By clicking on the link below from the on-line version of this document
- By navigating to a file in the Navis™ Optical PM - NP software

Linking from the Navis™ Optical PM - NP on-line documentation

If you are viewing the HTML version of this document (accessed by executing **Help > On-line Documents** from the Network Map), click on the following link to access the fault list.

> **Important!** If you are viewing the .pdf version of this document on-line, the link does not display on this page.

Navigating to a file in the Navis™ Optical PM - NP software

The fault list file is included in the Navis™ Optical PM - NP software. You can open the fault list file with a browser if the Navis™ Optical PM - NP software is loaded on the personal computer. The following is the path and file for the fault list in the Navis™ Optical PM - NP software:

```
c:\jui\bin\jnm\itm\help\appl\lang\english\doc\fault-
   lists\snms_mgmt_alarms.html
```

> **Important!** The PC must contain the Navis™ Optical PM - NP software.

□

Navis™ Optical EMS: WaveStar® BandWidth Manager and OC192 network elements fault list

Overview

This list provides mapping and classification information for each alarm, identified by its unique Fault Type.

The table consists of the following fields:

- Fault: network element fault type.
- Text: the text for the network element fault type.
- G7 2.0 PC: the mapping of the fault to the G7 2.0 probable cause.
- NMS Service Affecting: a Navis™ Optical PM - NP service affecting value of SA_SERVICE_FAILED, SA_SERVICE_DEGRADED, SA_NON_SERVICE_AFFECTING or SA_UNKNOWN.
- Reporting to NMS: values of “R”, for reported to Navis™ Optical PM - NP, or “NR” for not reported to Navis™ Optical PM - NP.
- Persistency: lists whether the alarm is persistent or transient.

Displaying the fault list

The fault list can be viewed using browser software in the following ways:

- By clicking on the link below from the on-line version of this document
- By navigating to a file in the Navis™ Optical PM - NP software

Linking from the Navis™ Optical PM - NP on-line documentation

If you are viewing the HTML version of this document (accessed by executing **Help > On-line Documents** from the Network Map), click on the following link to access the fault list.

> **Important!** If you are viewing the .pdf version of this document on-line, the link does not display on this page.

Navigating to a file in the Navis™ Optical PM - NP software

The fault list file is included in the Navis™ Optical PM - NP software. You can open the fault list file with a browser if the Navis™ Optical PM - NP software is loaded on the PC. The following is the path and file for the fault list in the Navis™ Optical PM - NP software:

```
c:\jui\bin\jnm\itm\help\appl\lang\english\doc\fault-
   lists\BWM_etc.html
```

Important! The PC must contain the Navis™ Optical PM - NP software.

☐

Navis™ Optical EMS: WaveStar® OLS 1.6T Family fault list

Overview

This list provides mapping and classification information for each alarm, identified by its unique fault type.

The table consists of the following fields:

- Fault Type: network element fault type.
- Text: the text for the network element fault type.
- G7 2.0 PC: the mapping to the G7 2.0 probable cause.
- NMS Service Affecting: a Navis™ Optical PM - NP service affecting value of SA_SERVICE_FAILED, SA_SERVICE_DEGRADED, SA_NON_SERVICE_AFFECTING.
- Reporting to NMS: values of "R", for reported to Navis™ Optical PM - NP, or "NR" for not reported to Navis™ Optical PM - NP.
- Persistency: lists whether the alarm is persistent or transient.

Displaying the fault list

The fault list can be viewed using browser software in the following ways:

- By clicking on the link below from the on-line version of this document
- By navigating to a file in the Navis™ Optical PM - NP software

Linking from the Navis™ Optical PM - NP on-line documentation

If you are viewing the HTML version of this document (accessed by executing **Help > On-line Documents** from the Network Map), click on the following link to access the fault list.

> **Important!** If you are viewing the .pdf version of this document on-line, the link does not display on this page.

Navigating to a file in the Navis™ Optical PM - NP software

The fault list file is included in the Navis™ Optical PM - NP software. You can open the fault list file with a browser if the Navis™ Optical PM - NP software is loaded on the PC. The following is the path and file for the fault list in the Navis™ Optical PM - NP software:

```
c:\jui\bin\jnm\itm\help\appl\lang\english\doc\fault-
   lists\snms_ols1.6t.html
```

> **Important!** The PC must contain the Navis™ Optical PM - NP software.

☐

Navis™ Optical EMS: LambdaRouter™ AOS fault list

Overview

This list provides mapping and classification information for each alarm, identified by its unique Fault Type.

The table consists of the following fields:

- Fault Type: network element fault type.
- Text: the text for the network element fault type.
- G7 2.0 PC: the mapping of the fault to the G7 2.0 probable cause.
- NMS SA: a Navis™ Optical PM - NP service affecting value of SA_SERVICE_FAILED, SA_SERVICE_DEGRADED, SA_NON_SERVICE_AFFECTING or SA_UNKNOWN.
- Reporting to NMS: values of "R", for reported to Navis™ Optical PM - NP, or "NR" for not reported to Navis™ Optical PM - NP.
- Persistency: lists whether the alarm is persistent or transient.

Displaying the fault list

The fault list can be viewed using browser software in the following ways:

- By clicking on the link below from the on-line version of this document
- By navigating to a file in the Navis™ Optical PM - NP software

Linking from the Navis™ Optical PM - NP on-line documentation

If you are viewing the HTML version of this document (accessed by executing **Help > On-line Documents** from the Network Map), click on the following link to access the fault list.

> **Important!** If you are viewing the .pdf version of this document on-line, the link does not display on this page.

Navigating to a file in the Navis™ Optical PM - NP software

The fault list file is included in the Navis™ Optical PM - NP software. You can open the fault list file with a browser if the Navis™ Optical PM - NP software is loaded on the PC. The following is the path and file for the fault list in the Navis™ Optical PM - NP software:

```
c:\jui\bin\jnm\itm\help\appl\lang\english\doc\fault-
   lists\snms_lambdarouter.html
```

> **Important!** The PC must contain the Navis™ Optical PM - NP software.

☐

Section II: Navis™ Optical PM - NP fault lists

Overview

Purpose This section contains the Navis™ Optical PM - NP fault lists.

Contents

Navis™ Optical PM - NP fault list	5-9

☐

Navis™ Optical PM - NP fault list

Overview

This table provide a list of the system, element management and network element related alarms generated by the Navis™ Optical PM - NP.

The table consist of the following fields:

- Fault: this field contains the fault identifier.
- Text: this field contains the descriptive text displayed for the alarm.
- Sev: this field contains the default severity of the alarm. This can be CRITICAL, MAJOR, MINOR or WARNING.
- Level: this defines the alarm category as a network management alarm (NMS), an element management system alarm (EMS) or a network element related alarm (NE).
- Pers: this defines whether the alarm is persistent (PERS) or instantaneous (INST).
- Cause: this defines the cause of the alarm.
- Comments: this field contains any other relevant information.

Displaying the fault list

The fault list can be viewed using browser software in the following ways:

- By clicking on the link below from the on-line version of this document
- By navigating to a file in the Navis™ Optical PM - NP software

Linking from the Navis™ Optical PM - NP on-line documentation

If you are viewing the HTML version of this document (accessed by executing **Help > On-line Documents** from the Network Map), click on the following link to access the fault list.

> **Important!** If you are viewing the .pdf version of this document on-line, the link does not display on this page.

Navigating to a file in the Navis™ Optical PM - NP software

The fault list file is included in the Navis™ Optical PM - NP software. You can open the fault list file with a browser if the Navis™ Optical PM - NP software is loaded on the PC. The following is the path and file for the fault list in the Navis™ Optical PM - NP software:

```
c:\jui\bin\jnm\itm\help\appl\lang\english\doc\fault-
   lists\ws-nms.html
```

Important! The PC must contain the Navis™ Optical PM - NP software.

□

6 Performance monitoring parameters

Overview

Purpose This chapter describes performance monitoring concepts as related to Navis™ Optical PM - NP.

Contents

Section I: Performance monitoring parameters	6-3
Performance monitoring parameters	6-4
Termination point performance parameters	6-6
Monitoring points	6-10
Metropolis™ EON performance monitoring parameters	6-12
Ethernet performance monitoring data	6-13
Optical network termination point performance parameters	6-14
Section II: Threshold setting parameters	6-16
Threshold setting	6-17
Optical threshold crossing alert parameters	6-18
Threshold crossing alert parameters	6-19
Section III: Trail Types	6-23

Connection level and trail types: WaveStar® BandWidth Manager, WaveStar® TDM 2.5/10G, and WaveStar® OLS 1.6T	6-24

□

Section I: Performance monitoring parameters

Overview

Purpose The purpose of this section is to provide the user with information about the performance monitoring parameters utilized by Navis™ Optical PM - NP.

Contents

Performance monitoring parameters	6-4
Termination point performance parameters	6-6
Monitoring points	6-10
Metropolis™ EON performance monitoring parameters	6-12
Ethernet performance monitoring data	6-13
Optical network termination point performance parameters	6-14

☐

Performance monitoring parameters

Overview Navis™ Optical PM - NP supports both near-end and far-end parameters.

Performance parameters The following table lists performance monitoring parameters. Near-end parameters are prefixed with “ne”, and far-end parameters are prefixed with a “fe”. For example, ”nebbe” stands for “near-end backgrounds block errors”, and “fecv” stand for “far-end code violations”.

Table 6-1 Performance monitoring parameters

Parameter	Description
es	Errored Seconds
esa	Errored Seconds Type A
esb	Errored Seconds Type B
ses	Severely Errored Seconds
uas	Unavailable Seconds
bbe	Backgrounds Block Errors
cv	Code Violations
ofs	Out of Frame Seconds
loss	Loss of Signal Seconds
fc	Failure Counts
sefs	Severely Errored Frame Seconds
psc	Protection Switch Count
pscs	Protection Switch Count (Span Switching)
pscr	Protection Switch Count (Ring Switching)
psd	Protection Switch Duration
sas	Severely Errored Frame (SEF)/Alarm Indication Signal (AIS) Seconds
aiss	Alarm Indiction Signal Seconds
fecc	Forward Error Correction Corrected
fecu	Forward Error Correction Uncorrected
ppjcg	Positive Pointer Justification Generated
npjcg	Negative Pointer Justification Generated

Table 6-1 Performance monitoring parameters (continued)

Parameter	Description
ppjcd	Positive Pointer Justification Detected
npjcd	Negative Pointer Justification Detected
lbc	Laser Bias Current
lbc-pl	Pump Laser Efficiency
opr	Optical Power Received
opt	Optical Power Transmitted
spr-c	Signal Power Received — Optical Channel
spt-c	Signal Power Transmitted — Optical Channel
topr-ol	Total Optical Power Received — Optical Line
topt-ol	Total Optical Power Transmitted — Optical Line

☐

Termination point performance parameters

Termination point performance parameters

The following table lists the termination point performance parameters for the supported SONET network elements.

Table 6-2 Termination point performance parameters per supported network element

Monitored termination point	WaveStar® OLS 2.5G/10G	WaveStar® BWM	Metropolis™ DMX	Metropolis™ DMXpress	LambdaUnite
Physical (PITTP)	LBC OPT OPR	LBC OPT OPR			
Section (RSTTP)	NE-CV NE-ES NE-SES NE-SEFS NE-LOSS (OC192, OC48, OC12, OC3)	NE-CV NE-ES NE-SES NE-SEFS NE-LOSS (OC192, OC48, OC12, OC3)	NE-CV NE-SEFS (OC192, OC48, OC12, OC3, EC1)	NE-SEFS (OC48)	NE-CV NE-ES NE-SES NE-SEFS NE-LOSS (OC192, OC48, OC12, OC3)

Table 6-2 Termination point performance parameters per supported network element (continued)

Line (MSTTP)	NE-CV NE-ES NE-SES NE-UAS NE-AISS NE-FC NE-FECC - OC192 only NE-FECU - OC192 only NE-PSC - excludes 4F rings NE-PSCS - 4F rings only NE-PSCR - excludes 4F rings (OC192, OC48, OC12, OC3, EC1).	NE-CV NE-ES NE-SES NE-UAS NE-AISS NE-FC NE-FECC - OC192 only NE-FECU - OC192 only NE-PSC - excludes 4F rings NE-PSCS - 4F rings only NE-PSCR - excludes 4F rings (OC192, OC48, OC12, OC3, EC1).	NE-CV NE-ES NE-ESA NE-ESB NE-SES NE-UAS NE-PSC NE-PJC - (OC192, OC48, OC12, OC3, EC1).	NE-CV NE-ES NE-ESA NE-ESB NE-SES NE-UAS NE-PSC NE-PJC - (OC48).	NE-CV NE-ES NE-SES NE-UAS NE-AISS NE-FC NE-FECC - OC192 only NE-FECU - OC192 only (OC192, OC48, OC12, OC3)
STS-1	NE-CV NE-ES NE-SES NE-UAS NE-FC PPJCG NPJCG PPJCD NPJCD	NE-CV NE-ES NE-SES NE-UAS NE-FC PPJCG NPJCG PPJCD NPJCD	NE-CV FE-BE NE-ES NE-ESA NE-ESB NE-SES NE-UAS, DMP	NE-CV NE-BE NE-ES NE-ESA NE-ESB NE-SES NE-UAS, DMP	NE-CV NE-ES NE-SES NE-UAS NE-FC PPJCG NPJCG PPJCD NPJCD

Table 6-2 Termination point performance parameters per supported network element (continued)

STS-3c	NE-CV NE-ES NE-SES NE-UAS NE-FC PPJCG NPJCG PPJCD NPJCD	NE-CV NE-ES NE-SES NE-UAS NE-FC PPJCG NPJCG PPJCD NPJCD	NE-CV FE-BE NE-ES NE-ESA NE-ESB NE-SES NE-UAS, DMP	NE-CV FE-BE NE-ES NE-ESA NE-ESB NE-SES NE-UAS, DMP	NE-CV NE-ES NE-SES NE-UAS NE-FC PPJCG NPJCG PPJCD NPJCD
STS-12c	NE-CV NE-ES NE-SES NE-UAS NE-FC PPJCG NPJCG PPJCD NPJCD	NE-CV NE-ES NE-SES NE-UAS NE-FC PPJCG NPJCG PPJCD NPJCD	NE-CV FE-BE NE-ES NE-ESA NE-ESB NE-SES NE-UAS, DMP	NE-CV FE-BE NE-ES NE-ESA NE-ESB NE-SES NE-UAS, DMP	NE-CV NE-ES NE-SES NE-UAS NE-FC PPJCG NPJCG PPJCD NPJCD
STS-48c	NE-CV NE-ES NE-SES NE-UAS NE-FC PPJCG NPJCG PPJCD NPJCD	NE-CV NE-ES NE-SES NE-UAS NE-FC PPJCG NPJCG PPJCD NPJCD			NE-CV NE-ES NE-SES NE-UAS NE-FC PPJCG NPJCG PPJCD NPJCD

Table 6-2 Termination point performance parameters per supported network element (continued)

STS-192c		NE-CV NE-ES NE-SES NE-UAS NE-FC PPJCG NPJCG PPJCD			NE-CV NE-ES NE-SES NE-UAS NE-FC PPJCG NPJCG PPJCD NPJCD
VT1.5 (DS1/T1)			NE-CV FE-BE NE-ES NE-ESA NE-ESB NE-SES NE-UAS, DMP	NE-CV FE-BE NE-ES NE-ESA NE-ESB NE-SES NE-UAS, DMP	

□

Monitoring points

Performance monitoring monitoring points The following table lists the performance monitoring monitoring points for the supported SONET network elements.

Table 6-3 Supported performance monitoring points per supported network element

Monitored termination point	WaveStar® OLS 2.5G/10G	WaveStar® BWM	Metropolis™ DMX	Metropolis™ DMXpress
T1 Line			NE-ES	
T1 Path	NE-CV NE-ES NE-SES NE-SEFS NE-LOSS (OC192, OC48, OC12, OC3)		NE-CV FE-CV NE-ES FE-ES NE-SES FE-SES NE-UAS FE-UAS	
T3 Line	NE-CV NE-ES NE-SES NE-LOSS	NE-CV NE-ES NE-SES NE-LOSS	NE-CV NE-ES NE-SES	NE-CV NE-ES NE-SES

Table 6-3 Supported performance monitoring points per supported network element (continued)

T3 Path	NE-CV NE-ES NE-ESA NE-ESB NE-SES NE-SAS NE-AISS NE-UAS NE-FC PPJCG NPJCG PPJCD NPJCD FE-CV FE-ES FE-SES FE-UAS FE-FC	NE-CV NE-ES NE-ESA NE-ESB NE-SES NE-SAS NE-AISS NE-UAS NE-FC PPJCG NPJCG PPJCD NPJCD FE-CV FE-ES FE-SES FE-UAS FE-FC	NE-CV FE-CV NE-ES FE-ES NE-SES FE-SES NE-UAS FE-UAS NE-SEFS	NE-CV FE-CV NE-ES FE-ES NE-SES FE-SES NE-UAS FE-UAS NE-SEFS

□

Metropolis™ EON performance monitoring parameters

Metropolis™ EON monitoring points

The following table lists the Metropolis™ EON monitoring points.

Table 6-4 Metropolis™ EON monitoring points

SNMS-EML Name	Navis™ Name	Connection Level (GUI)	Analogue Counters OLS Metropolis™ EON
Optical Channel	OCHTTP	OchTrail	SPR-C
Section	RSTTP		NE-CV NE-ES NE-SES NE-SEFS
OTPS	PITTP	OL	OPR (sink) OPT (source) LBCL (source)
Optical Line	OTSTTP	OMS	TOPR-OL TOPT-OL OSNR-OL LBC-P1 LBC-P2 LBFC-P1 LBFC-P2

□

Ethernet performance monitoring data

Ethernet performance monitoring data The following table lists Ethernet performance monitoring data.

Table 6-5 Ethernet performance monitoring data

Monitored termination point	DMX	DMxpress
ENET (Ethernet port or VCG)	EDFC EDFE EINB EINF EONB EONF	EDFC EDFE EINB EINF EONB EONF

☐

Optical network termination point performance parameters

Background

Optical channel monitoring is possible independently with analog and digital counters, depending on the hardware present. Analog monitoring is possible whenever an OMON (Optical Monitor) device is present. Digital monitoring is possible whenever a WaveWrapper OTU or a OCh Repeater OTU is present. Navis™ Optical PM - NP does not check the presence of this equipment before allowing monitoring to be configured.

For WaveStar® OLS 1.6T, both digital and analog parameters share the optical channel termination point (OCHTTP).

WaveStar® OLS 1.6T optical parameters

The following table lists the optical network termination point performance parameters for WaveStar® OLS 1.6T.

Table 6-6 Optical network termination point performance parameters for WaveStar® OLS 1.6T

SNMS-EML Name	Navis™ Optical PM - NP Name	Digital Counters WaveStar® OLS400G R5.0 and prior	Digital Counters WaveStar® OLS400G R6.0 and above	Analog Counters All WaveStar® OLS400G releases
Optical Channel	OCHTTP	FEC-EC FEC-UBC		SPR-C (per channel signal power received) SPT-C (per channel signal power transmitted
RS	RSTTP	NE-CV-BBE NE-ES NE-SES NE-SEFS	NE-CV-BBE NE-ES NE-SES NE-SEFS	
Physical/OTPS	PITTP			OPR (optical power received) OPT (optical power transmitted) LBC (laser bias current)

Table 6-6 Optical network termination point performance parameters for WaveStar® OLS 1.6T (continued)

SNMS-EML Name	**Navis™ Optical PM - NP Name**	**Digital Counters WaveStar® OLS400G R5.0 and prior**	**Digital Counters WaveStar® OLS400G R6.0 and above**	**Analog Counters All WaveStar® OLS400G releases**
Optical Line	OTSTTP			TOPR-OL (total optical power received) TOPT-OL (Total optical power transmitted PLE-TPN (Pump laser efficiency — transmit pump N, N=1..6) PLE-RPN (pump laser efficiency — receive pump N, N=1..6)

☐

Section II: Threshold setting parameters

Overview

Purpose The purpose of this section is to provide the user with the threshold setting parameters utilized by Navis™ Optical PM - NP.

Contents

Threshold setting	6-17
Optical threshold crossing alert parameters	6-18
Threshold crossing alert parameters	6-19

☐

Threshold setting

Overview

An important component of the performance monitoring feature is the setting of a threshold value.

Threshold crossing alerts

A threshold value is set for each performance monitoring data parameter at a selected termination point on an SDH transport connection. When this connection is exceeded, a threshold crossing alert (TCA) is raised to indicate that the signal quality has fallen below a pre-set value.

Threshold crossing alert processing

The performance monitoring feature allows only for the viewing and setting of TCA parameters. All other aspects of TCAs are handled by the Navis™ Optical PM - NP fault management feature.

Navis™ Optical PM - NP allows the user to set each of the TCA parameter values for one or two ports associated with a selected transport connection, on a per granularity basis. The EMSs maintain a raise and a clear value for each TCA parameter. The EMSs set both values to the single value supplied by Navis™ Optical PM - NP.

□

Optical threshold crossing alert parameters

Optical threshold crossing alert parameters

The following lists the optical threshold crossing alert parameter settings. All the thresholds in the table are “Low” with the exception of LBC, which is “High.”

Table 6-7 Optical threshold crossing alert parameter settings

Monitored Termination Point	Digital Counters OLS 1.6T	Analog Counters OLS 1.6T
OCHTTP		SPR-C (per channel signal power received) SPT-C (per channel signal power transmitted
PITTP	[1]	LBC (laser bias current)[2]
OTSTTP		TOPR-OL (total optical power received) TOPT-OL (Total optical power transmitted PLE-TPN (Pump laser efficiency — transmit pump N, N=1..6) PLE-RPN (pump laser efficiency — receive pump N, N=1..6)

Notes:

1. The FEC counters are moved to the Physical layer. Navis™ Optical PM - NP does not show FEC counters against the Physical layer.
2. OPR and OPT thresholds cannot be modified by the user, therefore they are now shown in this table.

☐

Threshold crossing alert parameters

Threshold crossing alert parameters

The following table lists the threshold crossing alert parameters for the supported SONET network elements.

Table 6-8 Threshold crossing alert parameters per supported network element

Monitored termination point	WaveStar® OLS 2.5G/10G	WaveStar® BWM	Metropolis™ DMX	Metropolis™ DMXpress	LambdaUnite
Physical (PITTP)	LBC OPT OPR	LBC OPT OPR			
Section (RSTTP)	NE-CV-BBE NE-ES NE-SES NE-SEFS NE-LOSS (OC192, OC48, OC12, OC3)	NE-CV-BBE NE-ES NE-SES NE-SEFS NE-LOSS (OC192, OC48, OC12, OC3)	NE-CV-BBE NE-SEFS (OC192, OC48, OC12, OC3, EC1)	NE-SEFS (OC48)	

Table 6-8 Threshold crossing alert parameters per supported network element (continued)

Line (MSTTP)	NE-CV-BBE NE-ES NE-SES NE-UAS NE-AISS NE-FC NE-FECC - OC192 only NE-FECU - OC192 only NE-PSC - excludes 4F rings NE-PSCS - 4F rings only NE-PSCR - excludes 4F rings only NE-PSD - excludes 4F rings (OC192, OC48, OC12, OC3, EC1).	NE-CV-BBE NE-ES NE-SES NE-UAS NE-AISS NE-FC NE-FECC - OC192 only NE-FECU - OC192 only NE-PSC - excludes 4F rings NE-PSCS - 4F rings only NE-PSCR - excludes 4F rings only NE-PSD - excludes 4F rings (OC192, OC48, OC12, OC3, EC1).	NE-CV-BBE NE-ES NE-ESA NE-ESB NE-SES NE-UAS NE-PSC NE-PJC - (OC192, OC48, OC12, OC3, EC1).	NE-CV-BBE NE-ES NE-ESA NE-ESB NE-SES NE-UAS NE-PSC NE-PJC - (OC48).	
STS-1	NE-CV-BBE NE-ES NE-SES NE-UAS PPJCG NPJCG PPJCD NPJCD	NE-CV-BBE NE-ES NE-SES NE-UAS PPJCG NPJCG PPJCD NPJCD	NE-CV-BBE FE-BE NE-ES NE-ESA NE-ESB NE-SES NE-UAS, DMP	NE-CV-BBE NE-BE NE-ES NE-ESA NE-ESB NE-SES NE-UAS, DMP	

Table 6-8 Threshold crossing alert parameters per supported network element (continued)

STS-3c	NE-CV-BBE NE-ES NE-SES NE-UAS PPJCG NPJCG PPJCD NPJCD	NE-CV-BBE NE-ES NE-SES NE-UAS PPJCG NPJCG PPJCD NPJCD	NE-CV-BBE FE-BE NE-ES NE-ESA NE-ESB NE-SES NE-UAS, DMP	NE-CV-BBE FE-BE NE-ES NE-ESA NE-ESB NE-SES NE-UAS, DMP	
STS-12c	NE-CV-BBE NE-ES NE-SES NE-UAS PPJCG NPJCG PPJCD NPJCD	NE-CV-BBE NE-ES NE-SES NE-UAS PPJCG NPJCG PPJCD NPJCD	NE-CV-BBE FE-BE NE-ES NE-ESA NE-ESB NE-SES NE-UAS, DMP	NE-CV-BBE FE-BE NE-ES NE-ESA NE-ESB NE-SES NE-UAS, DMP	
STS-48c	NE-CV-BBE NE-ES NE-SES NE-UAS PPJCG NPJCG PPJCD NPJCD	NE-CV-BBE NE-ES NE-SES NE-UAS PPJCG NPJCG PPJCD NPJCD			
STS-192c		NE-CV-BBE NE-ES NE-SES NE-UAS PPJCG NPJCG PPJCD			

Table 6-8 Threshold crossing alert parameters per supported network element (continued)

VT1.5 (DS1/T1)			NE-CV-BBE	NE-CV-BBE	
			FE-BE	FE-BE	
			NE-ES	NE-ES	
			NE-ESA	NE-ESA	
			NE-ESB	NE-ESB	
			NE-SES	NE-SES	
			NE-UAS, DMP	NE-UAS, DMP	

□

Section III: Trail Types

Overview

Purpose The purpose of this section is to provide the user with the trail types utilized by the performance monitoring feature.

Contents

Connection level and trail types: WaveStar® BandWidth Manager, WaveStar® TDM 2.5/10G, and WaveStar® OLS 1.6T	6-24

□

Connection level and trail types: WaveStar® BandWidth Manager, WaveStar® TDM 2.5/10G, and WaveStar® OLS 1.6T

Connection level/trail types

The following table shows the connection level and trail types supported by the WaveStar® BandWidth Manager, TDM 2.5G/10G, and WaveStar® OLS 1.6T network elements.

Table 6-9 Connection level and trail types supported by the WaveStar® BandWidth Manager, TDM 2.5G/10G, and WaveStar® OLS 1.6T network elements.

CKT/DL Connection	Description	Performance monitoring Trail Types	WaveStar® BWM	TDM 2.5G/10G	WaveStar® OLS 1.6T
S0	**STM-0 DL**	**MS0** **RS0**	No No	No No	No No
S1	**STM-1 DL**	**MS1** **RS1**	Yes Yes	Yes Yes	No No
S4	**STM-4 DL**	**MS4** **RS4**	Yes No	Yes Yes	No No
S16	**STM-16 DL**	**MS16** **RS16**	Yes Yes	Yes Yes	No No
S64	**STM-64 DL**	**MS64** **RS64**	Yes Yes	Yes Yes	No No
AU4	**AU4**	**AU4CTP**	Yes	Yes	No
TU3	**TU3**	**TU3CTP**	No	No	No
TU2	**TU2**	**TU2CTP**	No	No	No
TU12	**TU12**	**TU12CTP**	No	No	No
E1	**CEPT-1 DL**	**P12**	No	No	No
E3	**CEPT-3 DL**	**No**	No	No	No
E4	**CEPT-4 DL**	**P4**	No	No	No
VC4S	**VC4 CKT**	**VC4**	No	No	No
VC3S	**VC3 CKT**	**VC3**	No	No	No
VC2S	**VC2 CKT**	**No**	No	No	No
VC12S	**VC12 CKT**	**VC12**	No	No	No
30N	**CEPT-1 CKT**	**P12**	No	No	No
480N	**CEPT-3 CKT**	**No**	No	No	No
1920N	**CEPT-4 CKT**	**P4**	No	No	No

Table 6-9 Connection level and trail types supported by the WaveStar® BandWidth Manager, TDM 2.5G/10G, and WaveStar® OLS 1.6T network elements. (continued)

CKT/DL Connection	Description	Performance monitoring Trail Types	WaveStar® BWM	TDM 2.5G/10G	WaveStar® OLS 1.6T
30N	**VC12S-30N Combo**	**VC12** **TU12**	No No	No No	No No
480N	**VC3S-480n Combo**	**VC3** **TU3**	No	No	No
672N	**VC3S-672N Combo (DS3)**	VC3 **TU3**	No	No	No
1920N	**VC4S-1920N Combo**	**VC4** **AU4**	No	No	No
DS3	**DS3 CKT**	**D3**	No	No	No
VC4-4c	**VC4-4c CKT**	**VC4-4c**	Yes	Yes	No
VC4-16c	**VC4-16c CKT**	**VC4-16c**	Yes	Yes	No
AU3S	**AU3 CKT**	**AU3**	Yes	No	No
OMS	**OMS CKT**	**OMS**	No	No	Yes
OChTrail	**OChTrail CKT**	**0CH**	No	No	Yes
OL	**OL CKT**	**OL**	No	No	Yes

☐

Lucent Technologies
Bell Labs Innovations

7 Reports Management

Overview

Purpose This chapter describes the reports that are provided by Navis™ Optical PM - NP.

Contents

About reports	7-2

☐

About reports

Introduction

Navis™ Optical PM - NP supports, on demand, predefined reports to assist you in your work activities. These reports provide data that are not available through regular dialog boxes, forms, or network maps.

Printing reports

All predefined reports are routed to the designated printers attached to the host.

To print a report, from the Network Map, execute **Reports > Remote Report** and select the submenu for the desired report.

List of reports

The following reports are available from Navis™ Optical PM - NP:

- Implementation Jeopardy Report: lists the pending facility orders whose DXC command implementation date is in jeopardy.
- Completion Jeopardy Report: lists the pending facility orders whose completion date is in jeopardy.

□

Index

Numerics

15 minute time periods for performance monitoring, 1-23

24-hour time periods for performance monitoring, 1-23

A

Acknowledge
  alarm, 2-3, 4-24
  Alarm List, 4-24
  Traffic Correlated Alarm List, 4-24

Affected Trail List form, 1-14

Aggregate
  alarms, 1-12

Aging period for restoration notification, 1-16

Alarm approach
  fault management operational mode, 1-7

Alarm count
  view, 2-20

Alarm deletion options, 1-16

Alarm groups, 4-4

Alarm log records
  archive, 2-12
  delete, 2-12, 4-23
  export, 2-12

Alarm propagation
  Optical Network Navigator, 4-15

Alarm settings
  recommendations, 1-5

Alarm storage limits, 1-16

Alarmed objects
  add to trouble tickets, 2-9
  equipment alarms, 4-8
  external, 4-8
  internal, 4-8
  suppression, 4-19
  termination point alarms, 4-7
  types of, 4-7

Alarms
  acknowledge, 2-3
  acknowledgement, 4-24
  add to trouble tickets, 2-9
  aggregate alarms, 1-12
  alarm groups, 4-4
  black box alarms, 1-12
  bridge alarms, 2-16
  categories, 4-5
  classification, 4-4
  clear with no raise events, 4-3
  collection, 4-2
  color coding, 1-10
  correlation, 4-7
  delete, 2-11, 4-23
  double raise events, 4-2
  DXC alarms, 1-11
  EMS alarms, 1-11, 4-4
  equipment, 4-10
  fault state determination, 4-12
  fault state values, 4-12
  how to filter, 2-21
  how to sort, 2-21
  link alarms, 1-10, 2-15
  network element alarms, 1-12
  node alarms, 2-17
  protection switch, 4-10

- raise and clear events, 4-2
- regenerator alarms, 1-11
- service impact assessment, 4-21
- severity, 4-6
- suppression, 4-19
- synchronize, 2-14, 4-3
- types, 4-10

Audience, xi

B

Black box
- alarms, 1-12

Boundary port, 4-9

Bridges
- alarms, 2-16

C

Catalogued connection, 4-8

Clear with no raise events, 4-3

Colors
- of aggregate alarms, 1-12
- of alarms, 1-10
- of black box alarms, 1-12
- of DXC alarms, 1-11
- of EMS node alarms, 1-11
- of link alarms, 1-10
- of network element alarms, 1-12
- of regenerator alarms, 1-11

Comments, xiv

Connection
- catalogued, 4-8
- uncataloged, 4-8

Connection level/trail types, 6-24

Conventions
- typographical, xii

Create
- trouble tickets, 2-7

D

Data collection
- performance monitoring, 1-27

Database synchronization, 2-1

Date format
- display, 3-3

Delete
- alarm, 2-11, 4-23
- monitoring point, 3-11
- trouble tickets, 2-10

Display
- installed date format, 3-3

Display Optical Network Navigator alarmed ports, 2-23

Documentation
- font usage, xii
- how to comment, xiv
- list of, xiii
- on CD-ROM, xiii
- on-line version, xiii

Domain partitioning, 4-26

Double raise events, 4-2

DXC
- alarms, 1-11

E

Element Management Systems (EMSs)
- supported, 1-4

EMS, 1-4

EMS alarms, 1-11, 4-4
- view, 2-18

Equipment alarmed object
- fault state, 4-13, 4-15

Equipment alarms, 4-10
- alarmed objects for, 4-8

External alarmed object, 4-8

F

Fault lists
- 2.5G, 5-4
- LambdaRouter™ AOS, 5-7
- Navis™ Optical EMS management alarms, 5-3
- Navis™ Optical PM - NP, 5-9
- OC192, 5-4
- WaveStar® BWM, 5-4
- WaveStar® OLS 1.6T Family, 5-6

Fault management
- accessing from Network Map, 1-9
- installation options, 1-16
- overview, 1-4

Fault management forms, 1-8, 1-13

Fault management operational mode, 1-7, 1-16

- alarm approach, 1-7
- changing, 1-7, 2-4
- service approach, 1-7
- setting via preferences, 2-4

Fault state

- direct, 4-12
- equipment alarmed object, 4-13, 4-15
- indirect, 4-14
- port alarmed object, 4-12, 4-15
- propagation, 4-14
- reassessment, 4-16
- trail alarmed object, 4-13, 4-14

Fault state determination, 4-12

Fault state values, 4-12

Filter

- alarms, 2-21
- non-alarm events, 2-19
- secondary alarms, 2-5

Font usage, xii

Forms for fault management, 1-8, 1-13

G

Graphical Layout form, 1-13

H

Help

- screen help, xiii

I

Information products

- font usage, xii
- how to comment, xiv
- how to order, xiv
- list of, xiii
- on CD-ROM, xiii
- on-line version, xiii

Installation options

- aging period for restoration notification, 1-16
- alarm deletion options, 1-16
- alarm storage limits, 1-16
- fault management, 1-16
- FM operational mode, 1-16
- interval time, 1-16
- number of events, 1-16

Intended audience, xi

Internal alarmed object, 4-8

Interval time, 1-16

L

Links

- alarms, 1-10, 2-15

Logs

- performance monitoring message log, 1-25

M

Message log, 1-25

Monitoring point

- delete, 3-11
- set up, 3-4

N

Navis™ Optical EMS management alarms, 5-3

Network elements

- alarms, 1-12
- behavior, 4-17
- supported, 1-5

Network Event Summary, 1-13

Network Map

- accessing fault management information, 1-9
- color-coded alarms, 1-10

Nodes

- alarms, 2-17

Non-alarm events

- filter, 2-19

Non-boundary port, 4-9

O

On-line documentation, xiii

On-line help
See: Screen help

Operational mode
See: Fault management operational mode

Optical Network Navigator domain, 4-26

Optical networks
  - termination point performance parameters, 6-14
  - threshold crossing alert parameters, 6-18

Ordering
  - information products, xiv

P

Performance menu, 1-25

Performance monitoring
  - data collection, 1-27
  - data reporting, 1-29
  - message log, 1-25
  - overview, 1-21
  - parameters, 6-4
  - time periods, 1-23

Performance monitoring data, 1-23
  - generate a report, 3-8

Performance parameters, 6-4
  - optical network termination point, 6-14
  - optical threshold crossing alert parameters, 6-18
  - set threshold values, 3-6

PM Data Export, 1-24

PM Path List, 1-29

PM Port List, 1-27

Port
  - boundary, 4-9
  - non-boundary, 4-9

Port alarmed object
  - fault state, 4-12, 4-15

Preferences, 1-15
  - changing fault management operational mode, 2-4

Primary and secondary alarms
  - suppression, 4-19

Propagation
  - fault state, 4-14

Protection switch alarms, 4-10

R

Raise and clear events, 4-2

Regenerators
  - alarms, 1-11

Reports, 7-2
  - create a data report, 3-8

Restoration notification, 1-16

S

Screen help, xiii

Secondary alarms
  - filter, 2-5

Service approach
  - fault management operational mode, 1-7

Service impact
  - values, 4-21

Service impact assessment
  - alarm, 4-21

Settings
  - user settings, 1-15

Sort
  - alarms, 2-21

Suppression
  - alarm, 4-19
  - alarmed objects, 4-19
  - Primary and secondary alarms, 4-19

Synchronize
  - alarms, 2-14, 4-3

T

TCAs
  See: Threshold crossing alerts (TCAs)

Termination point alarms
  - alarmed objects for, 4-7

Threshold crossing alerts (TCAs), 1-26, 1-29, 4-5, 6-17
  - parameters, 6-18

Threshold values
  - how to set, 3-6, 6-17

Traffic Correlated Alarm List form, 1-13

Trail alarmed object
  - fault state, 4-13, 4-14

Trouble ticket, 4-27

Trouble tickets
  - add alarm, 2-9
  - create, 2-7
  - delete, 2-10

Typographical conventions, xii

U

Uncataloged connection, 4-8

User settings, 1-15

V View

  alarm counts, 2-20

  EMS alarms, 2-18