Lucent Technologies
Bell Labs Innovations

Navis™ Optical Network Management System (NMS)

Release 7.0

Maintenance Guide

365-309-263R7.0
Issue 1
July 2002

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 365-309-263. To order Navis™ Optical 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 (866 582-3688).

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.

Lucent Technologies

Contents

Section V: WaveStar® ITM-SC-to-Navis™ Optical NMS error codes

6 Performance monitoring parameters

Section I: Performance monitoring parameters

List of Tables

About this information product

Purpose

This chapter is a preface that provides an overview of this information product.

The purpose of this Maintenance Guide is to instruct users how to maintain the Navis™ Optical Network Management System (NMS) Release 7.0 and the network.

Reason for reissue

This Maintenance Guide, Issue 1, is a new information product that supports Navis™ Optical NMS, Release 7.0.

Safety labels

This information product does not use safety labels.

Intended audience

This information product is written for operations personnel who will be maintaining Navis™ Optical NMS.

How to use this information product

This section provides information that will help users of this guide.

Chapter descriptions

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

Section	Title	Description
Preface	About this information product	Describes this information product's purpose, its intended audience, and how to use the document.
Chapter 1	Chapter 1, "Overview"	Describes how maintenance is performed for Navis™ Optical NMS.
Chapter 2	Chapter 2, "Fault management tasks"	Describes tasks that are performed to set up and use fault management.
Chapter 3	Chapter 3, "Performance monitoring tasks"	Describes tasks that are performed to set up and use performance monitoring.
Chapter 4	Chapter 4, "Alarm management concepts"	Describes how alarms are collected and managed.
Chapter 5	Chapter 5, "Fault Management Fault Lists"	Provides alarm lists.
Chapter 6	Chapter 6, "Performance monitoring parameters"	Describes performance monitoring parameters.
Chapter 7	Chapter 7, "Reports Management"	Describes runable reports.
Index	Index	Enables the user to quickly find information on specific topics.

Conventions used

This information product uses the following typographical conventions to distinguish between computer input and output.

- Text and numbers that the user inputs to the computer 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 information product is part of a set of documents that supports Navis™ Optical NMS.

List of documents

The document set that supports Navis™ Optical NMS includes:

1. *Navis™ Optical NMS Getting Started Guide,* (365-309-260) provides information needed when you are learning how to use the Navis™ Optical NMS software. It describes how to start and stop Navis™ Optical NMS, how to use the software, and how to interpret the graphical user interface. This document includes tasks and conceptual information.
2. *Navis™ Optical NMS Applications and Planning Guide*, (365-309-261) describes the features and applications, provides a product description, describes the hardware platforms for the product, and describes system planning and engineering, ordering, and product support. This document contains conceptual information only.
3. *Navis™ Optical NMS Provisioning Guide,* (365-309-262) instructs users how to use Navis™ Optical NMS to provision network equipment. This document includes tasks and conceptual information.
4. *Navis™ Optical NMS Maintenance Guide*, (365-309-263) instructs users on how to maintain Navis™ Optical NMS and the network.
5. *Navis™ Optical NMS Administration Guide,* (365-309-264) instructs users on how to administer Navis™ Optical NMS and the network. This document includes tasks and conceptual information.

Glossary

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

On-line documentation

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

1. An on-line version, in HTML format, of this document set is provided as part of the Navis™ Optical NMS software.
2. An on-line version, in HTML format, of this document set is available on CD-ROM.
   Navis™ Optical NMS User Documentation CD-ROM, (365-309-265) includes the full set of documents listed above.

Screen help

The Navis™ Optical NMS software includes screen help for each form, which describes the purpose of the form, each of the fields, and each of the buttons.

How to comment

To comment on this information product, go to the Online Comment Form (http://www.lucent-info.com/comments) or email your comments to the Comments Hotline (ctiphotline@lucent.com).

Customer satisfaction is extremely important to Lucent Technologies. All users are encouraged to provide feedback on the Navis™ Optical NMS information products.

How to order

To order Navis™ Optical NMS 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 Overview

Overview

Purpose

This chapter provides an overview of the fault management and performance monitoring components supported by Navis™ Optical NMS.

Contents

Section I: Fault management

Overview

Purpose

This section describes the Navis™ Optical NMS fault management system.

Contents

Fault management overview

Introduction

The fault management subsystem of the Navis™ Optical NMS receives and processes 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 NMS 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 NMS for analysis.
3. The analysis determines whether there is a problem within a network element or a problem with 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 NMS provides fault management through the following element management systems:

- Navis™ Optical Element Management System (EMS)
- WaveStar® Integrated Transport Manager-Subnetwork Controller (ITM-SC)

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:

- WaveStar® BandWidth Manager
- WaveStar® TDM 2.5/10G
- WaveStar® OLS 1.6T (formerly 400G)
- LambdaUnite™ MultiService Switch (MSS)
- WaveStar® LambdaRouter All Optical Switch (AOS) 256
- WaveStar® LambdaRouter AOS 128
- Metropolis® Enhanced Optical Networking (EON)
- WaveStar® ADM 155E
- WaveStar® ADM 4/1 STM-1
- WaveStar® ADM 4/1 STM-4
- WaveStar® ADM 16/1
- WaveStar® ADM 16/1 Compact
- WaveStar® AM 1
- WaveStar® AM 1 Plus
- WaveStar® TM 1
- WaveStar® OLS 80G
- WaveStar® DACS
- ISM-1, ISM-4, and ISM-5E
- SLM (ADM or Terminal), including regenerators
- PHASE network elements, including regenerators

Functionality

The fault management functionality supported by Navis™ Optical NMS consists of:

- 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 selected approach determines the fault management forms presented to the user and the filtering 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 the 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 specified settings affect the subsequent user sessions. For more information, refer to "Change the fault management operational mode" (2-4).

□

Fault management forms

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

- **Network Event Summary - Alarm View**: displays all of the alarms on the system and is used to view alarm summary information when the Alarm Approach is selected.
- **Network Event Summary Service Domain - Alarm View**: Service Domain users are presented with a Service Domain variation of the Network Event Summary form.
- **Network Event Summary - Service View**: 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.
- **Network Event Summary Service Domain - Service View**: Service Domain users are presented with a Service Domain variation of the Network Event Summary form.
- **Traffic Correlated Alarm List**: indicates alarms that affect trails. These are alarms which have been correlated to an object, because they affect traffic.
- **Alarm List**: displays a list of all Navis™ Optical NMS, EMS and network element alarms.
- **Affected Trail List**: allows users to view a list of trails associated with a selected alarm or alarmed object.
- **Trouble Ticket forms**: allows users 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**: allows users to view details about all alarmed objects that are historic, and to archive and export this information.
- **Network Navigator Failed Link List**: allows users to display Optical Network Navigation System ports with a status of “failed” and “unknown”.
- **Alarm Log - Alarm View**: allows users to view details about all alarms, and to archive and export this information.

- **Log Administration - Service View**: allows users to perform archive, export and delete functions for records from the Alarm Log - Service View.
- **Log Administration - Alarm View**: allows users to perform archive, export and delete functions for records from the Alarm Log - Alarm View.

□

Accessing fault management information from the Network Map

Overview This section discusses how 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 WaveStar® ITM-SC Alarm List or the Navis™ Optical NMS Alarm List for that network element.

Nodes The user selects a node on the Network Map to cut through to the WaveStar® ITM-SC or Navis™ Optical EMS 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 (CEPT-1, CEPT-3, CEPT-4, non-assignable VC-n) 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. Specifically, for a digital link in alarm, at least one of the following exists:
  - Non-channelized VC-4
  - Channelized VC-4 carrying at least one non-channelized VC-3
  - Channelized VC-4 carrying at least one non-channelized VC-12

  - Channelized VC-4 carrying at least one channelized VC-3 carrying CEPT-3
  - Channelized VC-4 carrying at least one channelized VC-12 carrying CEPT-1
- **Blue**: identifies the working or unprotected section of a trail (for Display Route).
- **Purple**: identifies a protected section of a trail (for Display Route)..

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

EMS nodes

The node representing an EMS (including Navis™ Optical NMS) changes 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 NMS 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 NMS uses the following colors for Navis™ Optical NMS 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 NMS, 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 NMS 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 NMS 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 NMS 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 NMS 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 green since communication links are not connected to them from the Navis™ Optical NMS, Navis™ Optical EMS, or WaveStar® ITM-SC controllers.

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 in the following order:

- 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 NMS 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 NMS, 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.
- **Pink**: indicates that an improper disconnect order 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 that enable 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 NMS is installed. They are:

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

Fault management operational mode

Navis™ Optical NMS 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.

Read-only viewing for geographic domain users

The default is that geographic domain users see only alarm and alarmed object records for their domain. At installation, this can be changed so that the geographic domain user can view all records, but they are restricted to acknowledge, delete, or raise trouble ticket records in their domain only.

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

□

Lucent Optical Network Navigation System

Overview

The Lucent Optical Network Navigation System (Lucent ONNS) is the software and hardware present in a LambdaRouter™ AOS network element that performs management functions, such as configuration management and fault management, on optical connections across a network of LambdaRouter™ AOS network elements.

Interaction with Navis™ Optical NMS

The Lucent ONNS essentially acts as the network manager for the domain of optical connections it controls. The Navis™ Optical NMS domain provides capacity to the Lucent Optical Network Navigation System domain, which provides capacity back to the Navis™ Optical NMS. Each management system tracks the fault state of its connectivity, and then uses Navis™ Optical NMS to display combined fault state information to the user.

Fault management

Fault management performs the following for the Lucent ONNS:

- Identification of connections which are currently failed. Fault management identifies which mesh Lucent ONNS connections cannot be re-routed, and have therefore failed, and which 1+1 or unprotected connections 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:

- Lucent ONNS mesh connections do not have a defined route. For these connections, Navis™ Optical NMS considers that the Lucent ONNS 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 connections take in the network.
- Lucent ONNS 1+1 protected connections are identified as “working” or “failed” by the Lucent ONNS. Fault management will use its normal protected mechanism to mark the connection as degraded.

Alarm synchronization

Lucent ONNS does not store autonomous notifications which it sends northbound. As a result, if Navis™ Optical NMS or Lucent ONNS, or the links between them go down, the autonomous notifications are lost. Therefore Navis™ Optical NMS does not support alarm resynchronization for the Lucent ONNS.

□

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 NMS performance monitoring system.

Contents

Performance monitoring overview

Purpose

The purpose of Navis™ Optical NMS 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 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 NMS Administration Guide* 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 NMS 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.

Service domains

Navis™ Optical NMS allows a user to manipulate performance monitoring data only on circuits for which the user has access permissions.

Supported network elements

Navis™ Optical NMS supports performance monitoring for the following network elements:

- ISM
- PHASE network elements
  - LXC 16/1
  - LXC 4/1
  - ADM 16/4
  - ADM 4/4
  - TM 4/4
  - TM 16/4
- SLM
- WaveStar® ADM 4/1 (formerly WaveStar ADM 155C)
- WaveStar® ADM 155E
- WaveStar® ADM 16/1
- WaveStar® ADM 16/1 Compact
- WaveStar® AM 1/WaveStar® TM 1
- WaveStar® AM 1 Plus
- WaveStar® BandWidth Manager
- WaveStar® DACS
- WaveStar® OLS 1.6T
- WaveStar® TDM 2.5/10G

□

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 SDH 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 NMS 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 NMS, except for WaveStar AM 1 Plus, use two time periods to accumulate unidirectional performance parameters.

They are:

- 15 minutes
- 24 hours

If 24-hour monitoring is selected, and the network element is controlled by the ITM-SC, monitoring begins at midnight that night.

In the case of WaveStar AM 1 Plus, bidirectional performance parameters are collected for 24-hour periods.

Peformance monitoring data export/file transfer

Navis™ Optical NMS automatically requests each EMS to recover all performance monitoring data collected during the previous 24 hours, from midnight to midnight. Navis™ Optical NMS 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.
- **PM Data Archive**: Not supported in this release.

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.

- **Threshold Viewing**: Allows the user to view the values of threshold that are currently set on a port. Threshold setting/viewing is only possible for monitored ports. Threshold viewing is not currently supported by any network elements controlled by WaveStar® ITM-SC or Navis™ Optical EMS.
- **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 Performance Monitoring Message Log form, which contains DXC performance monitoring output messages.

Threshold crossing alerts

The Alarm List displays Threshold Crossing Alerts, which alerts users of threshold levels that crossed the set thresholds.

□

Performance Monitoring 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 termination 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 selects one hour performance monitoring data.

Additionally, the user may select whether the performance monitoring data is collected from the trail, or from its associated tandem connection. If tandem connection is selected, the user specifies whether Net (Network) or Out (Outgoing) performance monitoring data is collected.

Tandem connections

In the case of tandem connection monitoring where there is no protection, there may be one tandem connection for any one trail. Where SNCP/S is employed, (worker and stand-by connections) there are two tandem connections for any one trail. In this case, a tandem connection is associated with the worker connection and a tandem connection is associated with the stand-by connection.

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 NMS), 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 NMS 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 NMS 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 NMS 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.

A set of performance monitoring data is defined as:

- one set of standard performance monitoring data
- one set of tandem connection monitoring Net (Network) performance monitoring data, or
- one set of tandem connection monitoring Out (Outgoing) performance monitoring data

If the user selects a tandem connection and the ports are not in a monitored state, Navis™ Optical NMS selects the extremity ports by default. For WaveStar® BandWidth Manager, WaveStar® OLS 1.6T,

and PHASE network elements, Navis™ Optical NMS selects connection termination points as the extremity ports.

□

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 port listing

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 NMS 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 NMS host, as a performance monitoring Option, with special off-line adjustments:
   - The filter table can be reinitialized anytime the Navis™ Optical NMS is off line.
   - The filter tables are editable with a UNIX editor.
   - The next initialization of the Navis™ Optical NMS 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.

□

Performance Monitoring Data Archive

Introduction This feature is not supported in this release.

□

2 Fault management tasks

Overview

Purpose

This chapter describes fault management tasks that can be performed for Navis™ Optical NMS.

Related topics

The following topics are related to fault management.

Uncorrelated Cross-connects

The Uncorrelated Cross-connects feature allows a user to view cross-connects made in the network that are not requested by Navis™ Optical NMS and are not in the Navis™ Optical NMS database. For more information, refer to *Navis™ Optical NMS Provisioning Guide*.

Improper Disconnects

The Improper Disconnects feature allows a user to view ports or cross-connects that were improperly disconnected from outside the Navis™ Optical NMS environment. For more information, refer to *Navis™ Optical NMS Provisioning Guide*.

Preplan Restoration

Preplan Restoration allows a dedicated backup route to be specified for paths and circuits. For more information, refer to *Navis™ Optical NMS Provisioning Guide* and *Navis™ Optical NMS Administration Guide*.

Database synchronization

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

Contents

Acknowledge an alarm

Purpose

Use this task to acknowledge alarms from the Traffic Correlated Alarm List and the Alarm List

Important! Service Domain users may not acknowledge alarms.

Before you begin

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

Task

Perform the following task 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

Use this task to change the fault management operational mode for an individual user login ID.

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 task 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 Trouble Ticket Details form is accessible from either the Traffic Correlated Alarm List or the Alarm List.

Important! Service Domain users may not access Trouble Ticket forms.

Before you begin

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

Task

Perform the following task 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 Trouble Ticket Details form is accessible from either the Traffic Correlated Alarm List or the Alarm List.

Important! Service Domain users may not access Trouble Ticket forms.

Before you begin

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

Task

Perform the following task 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

Use this task to manually delete trouble tickets.

Trouble tickets are automatically deleted by Navis™ Optical NMS 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.

Important! Service Domain users may not access Trouble Ticket forms.

Before you begin

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

Task

Perform the following task 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

□

View the Alarm List from a network element menu

Purpose Use this task to view the Alarm List from a network element menu.

Task Perform the following task to view the Alarm List from a network element menu

1 To be done

Result:

.....

END OF STEPS

□

Delete an alarm from the Alarm List

Purpose Use this task to delete an alarm from the Alarm List

Navis™ Optical NMS automatically deletes instantaneous 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.

Important! Service Domain users may not delete alarms.

Task Perform the following task 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

Use this task to archive, export, and delete alarm log records.

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.

> **Important!** Service Domain users may not access alarm log information.

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 task 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

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

Before you begin

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

Task

Perform the following task 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 -> Start EMS Synchronization**.

Result:

The Database Synchronization form is displayed.

4 Select **Alarm** from the **Type** drop-down list.

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 task 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 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.

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 Perform the following task to view the alarms on a bridge.

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 task 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 EMS alarms

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

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

Task Perform the following task to view EMS alarms.

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

Use this task to filter non-alarm events from the Network Event Summary form.

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.
- Improper Disconnect: opens a list of new improper disconnect events.
- Uncorrelated Cross-connect: opens a list of new uncorrelated cross-connect events.
- Network Discrepancy: opens a list of the Optical Network Navigation System managed cross connections which are not part of a connection in Navis™ Optical NMS.

Task

Perform the following task 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

Purpose

Use this task to view alarm counts from the Network Event Summary form.

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 **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 task to view alarm counts from the Network Event Summary form.

1 From the Network Map, select **Fault > Network Event Summary**.

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

Use this task to filter and/or sort the information displayed on fault management forms.

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

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 task 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” (2-23).

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 Lucent ONNS ports with failed and unknown status

Purpose Use this task to display a list of Optical Network Navigation System 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 Perform the following task to display Lucent ONNS ports with failed and unknown status.

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 Navigation System alarmed ports with a status of “failed” or “unknown.”

END OF STEPS

□

Navis™ Optical NMS support of SDSL option card

Purpose

The purpose of this feature is to support transport of PDH or SDH signals between an AM1+ network element and either another AM1+ or a third party modem across existing copper links using SDSL protocol. The AM1+ option card prepares signals to be sent across the SDSL link by adapting it to an SDSL format. SDSL links between two AM1+ NEs equipped with SDSL option cards can carry either TU-12 or E1 signals. SDSL links between AM1+ and a third party modem can carry TU-12 or E1 signals depending on the modem used.

The AM1+ with SDSL option card is managed by WaveStar® ITM-SC.

Appliction

The application for this feature is for leased lines into the SDH network using existing copper resource.

Setting alarm reporting and severities

Alarm reporting and alarm severities must be set on a per port basis for the SDSL link from the WaveStar® ITM-SC “Event Parameters for Existing Resources” screen.

Selecting **Enable/Disable Low Order Path Alarms** on the VC12 TTP (located on the Navis™ Optical NMS aggregated AM1+ node Graphical Layout) cuts-through to the EMS for setting parameters for the selected VC-12 TTP.

Recognizing the Alarm Locating Suffix (AlarmLocSuffix)

In order to minimize the database strain of managing all master and slaves separately, Navis™ Optical NMS consolidates its view of each SDSL master and its slave nodes into one AM1+ node. To allow the user to determine the exact location of alarms from the consolidated node, WaveStar® ITM-SC will append a suffix onto the TMAG portl or equip_id values for alarms from the AM1+ in the SDSL case.

This suffix will be of the form: /NTU<SlaveNodeAlias>TP<remoteSlotNumber>.<RemotePortNumber> (this suffix indicates that the alarm has come from a slave (NTU) and which slave it is), or /LTU (this indicates that the alarm has come from the master AM1+).

The suffix will appear appended onto the normal Source information on the FM screens of the Graphical User Interface.

Navis™ Optical NMS separates the suffix from the source information internally and sends it to External Management Systems via TMF interface within the Additional Info field.

□

3 Performance monitoring tasks

Overview

Purpose

This chapter describes performance monitoring tasks that can be performed for Navis™ Optical NMS.

Contents

Display the installed date format

Purpose

Use this task 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 task 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 task 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

Perform 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 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 task 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

Perform 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 1, 2, or 1 or 2) 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 task 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

Perform 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! The time box disappears when you select 24 hour granularity so it is not possible to enter a time.

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

Result:

If Navis™ Optical NMS 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 task to delete a monitoring point.

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

Task Perform 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 NMS Administration Guide*.

□

4 Alarm management concepts

Overview

Purpose

This chapter describes fault management concepts for Navis™ Optical NMS.

Contents

Alarm collection

Introduction

Navis™ Optical NMS 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 Lucent ONNS alarm raise and clear events.
- All Lucent ONNS management alarms, including loss of association with another Lucent ONNS module.

Alarms received from the network

Navis™ Optical NMS validates each fault event (raise and clear) it receives from an EMS and checks the event for duplication. If the alarm passes validation and uniqueness tests, then it is maintained and processed. In validation, Navis™ Optical NMS checks that the alarm is from a valid network element/EMS combination that it manages. During uniqueness testing, Navis™ Optical NMS checks that the alarm is not a duplicate of a particular alarm already received by the NMS.

Raise and clear events

If an alarm or TCA raise event occurs and it does not exist on the system, Navis™ Optical NMS 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 NMS 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 NMS 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 Lucent ONNS Optical Network modules.

Navis™ Optical NMS 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 NMS 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 NMS Administration Guide*.

□

Alarm classification

EMS alarms

Alarms are sent by the EMS, along with their mapped G7 2.0L probable causes, to Navis™ Optical NMS. The alarms are then mapped by Navis™ Optical NMS 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 NMS also uses the mapping to determine whether correlation is attempted for each alarm group. For those groups which are correlated, Navis™ Optical NMS determines the fault state of the alarmed object.

Alarm groups

Navis™ Optical NMS 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" (4-8) in this information product.

The Navis™ Optical NMS Alarm Groups are as follows:

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

- TCM Fail Primary
- TCM Fail Secondary
- TCM Signal Degrade
- TCM Misconnections

The Alarm Group for all alarms raised by the Navis™ Optical NMS 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

Navis™ Optical NMS can receive TCAs as either alerts or alarms with the probable cause of ″TCA.″ In order to process all TCAs, Navis™ Optical NMS converts all alerts to alarms (maintaining the probable cause of TCA) and processes them as detailed below.

1. 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.
2. TCAs (both alarms and alerts) can be either persistent or instantaneous.
   - Persistent TCAs are cleared when an interval occurs which has error counts below threshold.
   - Instantaneous TCAs are never cleared and must be acknowledged and deleted by the user.
3. TCAs are resynced southbound following loss of association between an EMS and network elements, between Navis™ Optical NMS and the EMS, or automatically at start up.
4. Navis™ Optical NMS will forward these alerts and alarms northbound in the format in which they were initially recieved. (i.e. original alerts are converted back to alert format.)

The following list describes how Navis™ Optical NMS handles TCAs:

- **Navis™ Optical EMS:** TCA data from Navis™ Optical EMS is converted into a G7 2.0L message and transmitted to Navis™ Optical NMS.
- **WaveStar® ITM-SC:** Navis™ Optical NMS converts the G7 2.0L message into a standard probable cause.
- **Navis™ Optical NMS:** Navis™ Optical NMS 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 NMS 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 NMS and an EMS, or automatically at start up.

Alarm categories

Navis™ Optical NMS 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
Threshold Crossings	Threshold Crossing
Protection Switch	Non-traffic
NMS	NMS

Severity mapping

Navis™ Optical NMS maps the severity of the alarm received from an EMS to the severities used in G7 2.0L as follows:

Table 4-2 Severity mappings for Navis™ Optical EMS

WaveStar® ITM-SC Severity	Navis™ Optical EMS	Severity	Notes
	Critical	Critical	No equivalent to this in the prompt scheme. No simple rules for knowing which prompt to make critical.
Prompt	Major	Major	
Deferred	Minor	Minor	

Table 4-2 Severity mappings for Navis™ Optical EMS (continued)

WaveStar® ITM-SC Severity	Navis™ Optical EMS	Severity	Notes
Info	Warning	Warning	
Indeterminate	Indeterminate	Indeterminate	Indeterminate is used for TCAs reported by the WaveStar® OLS 80G and WaveStar® DACS because the severity can be Prompt or Info depending on the source.

Navis™ Optical NMS performs mappings of severities for northbound equipment over some interfaces as required (e.g. TIM). These mappings are as follows:

- **Critical**: Prompt.
- **Major**: Prompt.
- **Minor**: Deferred.
- **Warning**: Info.
- **Indeterminate**: Indeterminate.

□

Alarm correlation

Introduction

Navis™ Optical NMS 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 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 NMS database. There are four possible results of this correlation:

- A "catalogued connection" not associated with a Lucent ONNS mesh connection is found. In this case, the alarm is linked to a trail alarmed object.
- A "catalogued connection" associated with a Lucent ONNS 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 NMS 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 NMS does not know of the server's existence.

Catalogued connection

Internally the Navis™ Optical NMS database is aware of the created connection. The connection is referred to as a ***catalogued connection***.

A catalogued connection is associated with a Lucent ONNS mesh connection only if the catalogued connection the alarm would be correlated to is:

- An optical channel mesh connection which is managed by Lucent ONNS, or
- An optical link connection whose client optical channel link connection is used in a Lucent ONNS mesh connection, or is unused, but allocated to a Lucent ONNS 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 NMS can match with termination points used by "in-effect" trails to determine which trails are affected by the equipment failure.

Alarmed objects for connection alarms

When an alarm is issued by a connection, Navis™ Optical NMS will attempt to correlate it to a connection in the Navis™ Optical NMS database. There are two possible results of this correlation:

1. A catalogued connection which is found. In this case an alarmed object is created.
2. No connection is found. In this case the alarm is uncorrelated and is not linked to an alarmed object.

Internal or external alarmed objects

When a failure occurs on a connection, Navis™ Optical NMS indicates whether the cause occurred inside or outside 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.

Lucent ONNS alarmed objects

An alarmed object is considered to be part of a Lucent ONNS domain only the following conditions are met:

- The alarmed object was created due to a connection alarm issued by a Lucent ONNS.
- 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 a Lucent ONNS.

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 NMS. 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 NMS 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 NMS 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 is one alarm group related to protection switching:

- **PSF (Protection Switch Fail)**: indicates 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 (pointer processing unit)

  Otherwise, equipment protection switching failures are mapped to the "equipment – uncorrelated" alarm group.

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.

ISDN Primary Rate Interface Alarms from AM 1 Plus

Navis™ Optical NMS handles ISDN primary rate interface (PRI) alarms from the AM 1 Plus as follows:

- External alarms are marked as external and correlated to the 2 Mb/s PDH connection.
- Internal alarms are marked as internal and correlated to the VC-12 connection instead of the 2Mb/s PDH connection.

□

Fault state determination

Introduction

Navis™ Optical NMS 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 NMS determines the fault state.

Fault state values

The following are the fault state values used in Navis™ Optical NMS:

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 NMS 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 MSP (Multiplex Section Protection) or MS-SPRING/BLSR (Bidirectional Line Switched Ring).
- An optical multiplex section (OMS) may be protected by optical multiplex section protection (OMSP) in the WaveStar® OLS 80G only.
- A VC-n path layer trail may be protected by SNCP.
- An optical channel (OCh) path layer trail may be protected by optical ring switch (ORS) Protection or by Lucent ONNS 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 MSP-protected digital link or end-to-end SNC protected VC-4, 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-fiber or 4-fiber MS-SPRING/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 Lucent ONNS-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 NMS 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 NMS 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.”

Reassessment of fault state

Navis™ Optical NMS reassess the fault state whenever a new alarm raise or clear is correlated to an alarmed object.

Fault state propagation

Objects on which alarms have been received are directly failed or degraded. Because SDH 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 NMS 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.

Example 1: If a Multiplex section fails, supporting a VC-4, which in turn supports 20 VC-12 trails, Navis™ Optical NMS propagates the failure to the VC-4 and then to the VC-12s.

Example 2: If the failure on the multiplex section is then cleared and the fault state returns to "working," this fault state will again be propagated to the VC-4 that it supports and in turn to the VC-12s being supported by that VC-4.

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. For example, if a Multiplex section fails, supporting a VC-4, which in turn supports 63 VC-12 trails, then the failure must be propagated first to the VC-4, and then to the VC-12s.

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. However, if a server is degraded rather than failed, the degraded state is not propagated to its clients (so as to improve system performance).

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

If the server trail is a digital link, Navis™ Optical NMS checks whether it belongs to a protection scheme, such as MS-SPRING or MSP.

Equipment alarmed objects

For equipment alarmed objects with an Affected TP List, Navis™ Optical NMS 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, SDH, LAN or optical.

For PDH port alarmed objects, the fault is propagated to a single bidirectional trail or two unidirectional client trails.

For SDH and optical port alarmed objects, the fault is propagated to any client termination points of those ports, and therefore to any trails using those client trails.

For Ethernet ports supporting virtual concatenation , there are no clients defined in CM. Therefore, these connections can never be uncatalogued and so cannot have a port alarmed object created on them. For other Ethernet ports, or ports of unspecified format (e.g. HSBB, LSBB), these can have port alarmed objects created on them. In this case, the failure will be propagated to all clients of the connection, in the same way as for SDH and optical ports.

Propagation of alarms from Lucent ONNS

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

Tandem Connection Monitoring

Propagation of tandem connection monitoring (TCM) related faults for the correlated connection to clients of the connection proceeds as for other transmission faults.

LOM conditions are an exception to this.

Overall fault state

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

Fault state reassessment following provisioning changes

Navis™ Optical NMS 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 NMS 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, or it becomes a port alarmed object. For trail alarmed objects, Navis™ Optical NMS 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 NMS 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 NMS 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 NMS 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 or 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 NMS performs a fault state propagation.

MS-SPRING creation

When the user completes a ring that supports MS-SPRING, Navis™ Optical NMS 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 NMS checks the fault state of the connections. If it detects any failures, Navis™ Optical NMS performs a fault state propagation.

Network element behavior and management domain visibility

Navis™ Optical NMS 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 failures. 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 failure 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 NMS is not guaranteed to be correct.

□

Alarm and alarmed object suppression

Introduction

To limit the amount of information displayed to a user, Navis™ Optical NMS 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 NMS 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 NMS evaluates and determines whether alarms are primary or secondary.

Since Navis™ Optical NMS 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 NMS 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 NMS 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 Lucent ONNS, 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 NMS 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 NMS 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

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 SDH path layer ports, the service impact is the fault state of the single impacted connection.

For PDH, SDH, and optical 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 NMS 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 NMS is still doing fault propagation, this must be completed before the service impact can be determined.

□

Alarm deletion

Introduction

Navis™ Optical NMS has two types of alarm deletion:

1. Discarding of new alarms.
2. Deletion of alarms from the system as a whole.

Delete alarms from the Alarm List

Navis™ Optical NMS provides two possible ways to remove alarms from the Alarm List:

1. A configured deletion option set at installation time. For more information, refer to "Installation options" (1-18) 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 NMS raises instantaneous platform alarms.

Once alarms are removed from the Alarm List, Navis™ Optical NMS 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 NMS 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 NMS 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 NMS 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 NMS 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.

□

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 and 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.

□

Domain partitioning

Background

Navis™ Optical NMS provides filtering for Geographic Domain Partitioning and Service Domain Partitioning users.

Geographic Domain Partitioning users

Geographic Domain Partitioning users have a definable set of network elements assigned to them.

For a Geographic Domain Partitioning user, the records they can view depends on the installation option “Read Only Viewing for GD Users.” By default, Geographic Domain Partitioning users see only alarm and alarmed object records for their domain. At installation, this can be changed so that the Geographic Domain user can view all records, but they are restricted to acknowledge, delete, or raise trouble tickets records in their domain only.

Service Domain Partitioning users

Only information related to the service domain and resources exclusive to the service domain is presented to the Service Domain Partitioning user. The Service Domain Partitioning user is only informed of failures on connections.

If a failure exists on a connection being assigned to the service domain, the user is alerted as if the failure has just occurred. If a failure exists on connectivity that is used to provision a connection within the service domain, the user is alerted as if the failure has just occurred.

The following functionality applies to the Service Domain Partitioning user:

- Service Domain Partitioning users are presented with a service domain variation of the Network Event Summary form called the Network Event Summary Service Domain form. The information applies to both the Alarm View and Service View forms. The Network Event Summary Service Domain forms are filtered for the Service Domain Partitioning user.
- The Alarm List and Traffic Correlated Alarm List forms are filtered for the Service Domain Partitioning user.
- Alarm acknowledgement and alarm deletion are not enabled for a Service Domain Partitioning user.

- Service Domain Partitioning users do not have access to the Alarm Log forms.
- Service Domain Partitioning users do not have access to the Trouble Ticket forms, and cannot view trouble ticket IDs on the Alarm List and Traffic Correlated Alarm List forms.

Direct connection failures

The Service Domain Partitioning user is alerted of failures directly impacting connections in their domain via the Network Event Summary Service Domain form.

Indirect connection failures

The Service Domain Partitioning user is alerted of impacts on service domain connections from alarmed connections outside of the service domain via the **Affected Trails List** button on the Network Event Summary Service Domain - Service View form. This button highlights whenever the fault state of a connection within the service domain changes from “working” as the result of a direct or indirect failure propagating from a service immediately outside of the service domain.

Lucent ONNS domain

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

A termination point is considered part of the Lucent ONNS domain if it is:

- an optical channel termination point which is part of the Lucent ONNS domain.
- an optical link termination point which is assigned to the Lucent ONNS domain.

□

Northbound interface

Overview

The optional northbound interface forwards all alarms provided by the EMSs, together with any information added by the Navis™ Optical NMS, to the upstream systems. These systems then undertake any fault management tasks defined for it by the service provider.

The northbound interface services the diverse needs of upstream operating systems that require data from the Navis™ Optical NMS fault management and performance monitoring applications.

Specifications

The CORBA-based northbound interface is based on G7 2.0 with some proprietary extensions.

The ASCII Northbound Interface (also known as the TIM interface) provides for a unidirectional transfer of alarm data to the upstream systems.

□

5 Fault Management Fault Lists

Overview

Purpose

This chapter contains alarm lists for the network elements and EMSs that Navis™ Optical NMS supports.

Contents

Section I: WaveStar® ITM-SC fault lists and management alarms

Overview

Purpose

This section contains fault lists and management alarms for the WaveStar® ITM-SC EMS and network elements.

Contents

WaveStar® ITM-SC network element fault list

Overview

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

The table consists of the following fields:

- **Fault Type**: the WaveStar® ITM-SC fault type.
- **Text**: the text for the WaveStar® ITM-SC fault.
- **G7 PC**: the mapping to the G7 2.0 probable cause.
- **NMS-SA**: Navis™ Optical NMS service affecting value. The following are the service affecting values in the list:
  - SA_NSA: SA_NONSERVICE_AFFECTING
  - SA_SD: SA_SERVICE DEGRADED
  - SA_SF: SA_SERVICE FAILED
  - SA_UK: SA_UNKNOWN
- **NMS Reported**: values of “R”, for reported to Navis™ Optical NMS, or “NR” for not reported to Navis™ Optical NMS.

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 NMS software

Linking from the Navis™ Optical NMS 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 NMS software

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

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

Important! The PC must contain the Navis™ Optical NMS software.

□

WaveStar® ITM-SC management alarms

Overview

This fault list provides mapping and classification information for each alarm, identified by its unique identifier (ID).

The table consists of the following fields:

- **ID**: the WaveStar® ITM-SC unique identifier of the fault.
- **Fault**: the WaveStar® ITM-SC fault.
- **Text**: the text for the WaveStar® ITM-SC fault.
- **TMF PC**: the TMF probable cause mapping.

Additional information

The following is additional information about the mapping.

- EMS alarms of Level EMS have been mapped to TMF Probable Cause EMS_FAULT. This includes geographic redundancy alarms where they report on communications between WaveStar® ITM-SCs or impact all managed network elements
- EMS alarms of Level Element, Category Management have been mapped to TMF Probable Cause NE_MGNT_FAIL, except for the direct reporting of loss of association. This includes geographic redundancy alarms, where the geographic redundancy alarm is in connection with a specified network element.
- EMS alarms of Level Element, Category Management, reporting direct loss of association with an network element, have been mapped to TMF Probable Cause UNIDENTIFIED and are not reported, as this information is provided to Navis™ Optical NMSby means of DCS event notifications.
- EMS alarms of Level Element, Category PRC or USR_ATTN have been mapped to TMF Probable Cause UNIDENTIFIED, as they do not constitute faults in either the WaveStar® ITM_SC or its communications with a network element.

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 NMS software

Linking from the Navis™ Optical NMS 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 NMS software

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

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

> **Important!** The PC must contain the Navis™ Optical NMS software.

□

Section II: Navis™ Optical EMS fault lists and management alarms

Overview

Purpose

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

Contents

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 NMS, or “NR” for not reported to Navis™ Optical NMS.
- **Persistency**: lists whether the alarm is persistent or transient.

Displaying management alarms

Management alarms 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 NMS software

Linking from the Navis™ Optical NMS 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 NMS software

The fault list file is included in the Navis™ Optical NMS software. You can open the fault list file with a browser if the Navis™ Optical NMS software is loaded on the PC. The following is the path and file for the Navis™ Optical EMS management alarm in the Navis™ Optical NMS 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 NMS software.

□

Navis™ Optical EMS: WaveStar® TDM 2.5/10G, 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 NMS 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 NMS, or "NR" for not reported to Navis™ Optical NMS.
- **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 NMS software

Linking from the Navis™ Optical NMS 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 NMS software

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

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

Important! The PC must contain the Navis™ Optical NMS software.

□

Navis™ Optical EMS: WaveStar® OLS 1.6T 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 NMS 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 NMS, or “NR” for not reported to Navis™ Optical NMS.
- **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 NMS software

Linking from the Navis™ Optical NMS 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 NMS software

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

```
c:\jui\bin\jnm\itm\help\appl\lang\english\doc\fault-
   lists\snms_ols400g.html
```

> **Important!** The PC must contain the Navis™ Optical NMS 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 NMS 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 NMS, or “NR” for not reported to Navis™ Optical NMS.
- **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 NMS software

Linking from the Navis™ Optical NMS 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 NMS software

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

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

> **Important!** The PC must contain the Navis™ Optical NMS software.

□

Section IV: Navis™ Optical NMS fault lists

Overview

Purpose This section contains the Navis™ Optical NMS fault lists.

Contents

Navis™ Optical NMS fault list

Overview

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

The table consist of the following fields:

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

Linking from the Navis™ Optical NMS 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 NMS software

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

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

Important! The PC must contain the Navis™ Optical NMS software.

□

Section V: WaveStar® ITM-SC-to-Navis™ Optical NMS error codes

Overview

Purpose

This section lists all the error codes which can be returned to Navis™ Optical NMS in a "deny" message. A short explanation is given for each error code.

Error codes

Navis™ Optical NMS processes the low-order alarms from ADM 155E and WaveStar® ADM 4/1 (formerly WaveStar® ADM 155C) network elements.

For paths/circuits that are provisioned through one-step provisioning (also referred as combo circuits), both PDH circuit alarms and SDH path alarms are correlated to the appropriate one step provisioned path.

In addition, equipment alarms on port cards that are not correlated to digital links (such as, end ports of a circuit/path) are also identified with one-step provisioned circuits.

Navis™ Optical NMS receives and processes alarms from the ITM-SC that are generated by WaveStar® ADM 4/1 (formerly WaveStar® ADM 155C) with STM-4 line ports.

Navis™ Optical NMS processes alarms from 45 Mb/s ports that are generated by PHASE, WaveStar® ADM 4/1, and WaveStar® ADM 16/1 network elements and correlates them to appropriate digital links/circuits with appropriate event notifications. In the case of one-step provisioned paths/circuits (circuit type = VC3S-672N), both PDH path/circuit and SDH path alarms terminating on the PDH port are correlated to the same path/circuit.

Contents

Port provisioning and cross-connection commands

Port provisioning and cross-connection commands

E001 Unknown command received.

An “xconreq” message has been received with an unknown ″command″ type, for example, not one of PROV, DPRV, CHNG, CONN, DISC,VRFY or MDFY.

or

The combination of ″typ″, ports and rate does not match a known cross-connection request.

E002 Unknown rate received in port provisioning request.

A “PROV” command has been received with an unknown “rate” value for the network element concerned.

E003 Unknown rate received in port deprovisioning request.

A ″DPRV″ command has been received with an unknown ″rate″ value for the network element concerned.

E004 Invalid rate received in a cross-connection verification request.

A ″CHNG″ (in effect) command has been received with an unknown ″rate″ value for the network element concerned.

E006 Invalid port(s) specified in xconreq (includes both cross connection and port provisioning requests).

At least one of the ports (EIDs) specified was not valid:

- value is out of range
- port type is inappropriate for the requested rate.
- two of the ports are on the same LP.

E007 - MSP flag set to Y for a port which does not support MSP.

The only ports that support MSP and can have msp flag set to Y are:

- Line ports
- Tributary ports on SLM RDI network elements.

E008 - Failed Operation - Unable to provision physical port.

(UIJ_DACSCAN_PROV_PORT failed or could not be set up). Possible causes include bad data in the original request and loss of association with the network element.

See ITM-SC log file for possible further information.

E010 - Failed Operation - Unable to deprovision physical port.

(UIJ_DACSCAN_PROV_PORT failed or could not be set up). Possible causes include bad data in the original request and loss of association with the network element.

See ITM-SC log file for possible further information.

E012 - Failed Operation - Verification of port(s) failed. Specified parameters do not match actual port(s).

E013 - Invalid Data - User error during logical port prov / deprov / verify, unexpected chass or port type.

E014 - Inconsistent signal mapping specified. Mismatch between rate and ineparam4.

E015 - Inconsistent timeslot 0 specified. Mismatch between rate and ineparam5.

E022 - Failed Operation - Cross Connect/Port Verify failed. Specified cross connect/port does not exist.

E023 - Failed Operation - Unable to create specified cross connect.

The lower level operation to create all or part of the cross-connection failed (UIJ_DACSCAN_PROV_XC failed or could not be set up). This may be due to a problem on the network element such as loss of association. Note that previous parts of the cross-connection may have been set up and may need to be deleted via the ITM-SC.

See ITM-SC log for possible further information.

E024 - Failed Operation - Unable to disconnect cross connect.

The lower level operation to disconnect all or part of the cross-connection failed (UIJ_DACSCAN_PROV_XC failed or could not be set up). This may be due to a problem on the network element such as loss of association. Note that previous parts of the cross-connection may have been disconnected and it may be necessary to tidy up using the ITM-SC.

See ITM-SC log for possible further information.

E025 - Failed Operation - Unable to deprovision VC4 logical port.

The command to deprovision the VC4 logical port failed (UIJ_DACSCAN_PROV_TP_VC4 failed or could not be set up). A possible cause is loss of association with the network element.

Check the state of the network element communications and the validity of the VC4 port.

E026 - Failed Operation - Unable to deprovision VC12 or VC3 logical ports as part of DISC.

The command to deprovision the VC12 or VC3 logical port was refused by the network element or associated ITM-SC subsystems (UIJ_DACSCAN_PROV_TP_VC3/12 failed or could not be set up). A possible causes is loss of association with the network element. Note that the cross-connection disconnect will have already been completed.

Check the state of the network element communications and the validity of the VC12 port.

E027 - Failed Operation - Unable to deprovision VC4 logical port as part of DISC.

The command to deprovision the VC4 logical port was refused by the network element or associated ITM-SC subsystems (UIJ_DACSCAN-_PROV_TP_VC4 failed or could not be set up). A possible cause is loss of association with the network element. Note that the cross-connection disconnect will have already been completed.

Check the state of the network element communications and the validity of the VC4 port.

E028 - Failed Operation - Unable to deprovision VC4 logical port.

The operation to disconnect physical port from the VC4 TTP failed (UIJ_DACSCAN_PROV_XC failed or could not be set up). A possible cause is loss of association with the network element. Note that the VC4 PTIs will already have been reset.

Check the state of the network element communications and the validity of the VC4 port.

E029 - Failed Operation - Unable to deprovision protecting port in msp pair.

Request failed (UIJ_DACSCAN_PROV_PORT failed or could not be set up). Possible causes are loss of association with the network element or the MSP scheme not being in the state expected.

Use ITM-SC to check the network element and MSP state.

E030- Internal Error - Error occurred while obtaining msp data for node.

E031 - Msp flag does not match availability.

If msp flag is 'Y' then the network element must have MSP provisioned. If msp is 'N' then the network element must NOT have MSP provisioned on the specified port.

E032 - Invalid rate.

For ADM 155/PHASE/WaveStar® ADM 16/1/WaveStar® ADM 4/1, the rate must be one of V4, C1, C3, C1DL, C3DL,D3 or D3DL. Also the rate specified in the command must be consistent with the type of card present.

E033 - Failed Operation - Unable to provision VC4 logical/physical port.

Provisioning the VC4 failed due either to invalid data in the original request or a problem with changing the network element configuration, such as loss of associate with the network element (The ITM-SC server process has reported the job as failed).

E034- Failed Operation - Unable to provision VC12 logical/physical port.

E035 - Failed Operation - Unable to provision VC4 logical/physical port.

E036 - Failed Operation - Unable to provision VC3 logical/physical port.

E037 - Failed Operation - Unable to provision protecting port in MSP pair.

Request to put the protecting port of an MSP scheme into service failed. Possible causes are bad data in the original request and loss of association with the network element.

E038 - Invalid Data - User error during port provisioning.

Rate incorrect for specified port.

E039 - Internal Error - Error occurred while finding service LPU.

E040 - Failed Operation - Unable to provision VC12 physical port.

Error occurred while setting transmission parameters.

E046 - Ports and/or Cross Connect does not have a valid status for this cross connection to proceed

E047 - Failed Operation - Unable to provision physical port.

Error occurred while setting msp parameters.

E048 - Failed Operation - Unable to verify logical port.

Specified port does not exist or match actual port.

E049 - Error while verifying PTI parameters.

For ADM 155, ISM, RR (NERA Radio), SLM, and WaveStar® ADM 4/1, the PTI (path trace identifiers) must not be set for 2Mb/s ports.

Current PTI values could not be read, perhaps due to bad data in the original request (UIR_LOGICAL_PORT_VERIFY failed).

E050 - Incompatible cross connection already exists.

One or more of the ports specified in the requested cross-connection is already involved in a cross-connection which is incompatible with the requested cross-connection.

E051 - Error while verifying port mode.

Port TTP supplied in CHNG is not enabled for alarm reporting.

E052 - Cannot store the (ckt) CCL details in the database.

E053 - Cannot delete the (ckt) CCL details from the database.

E054 - Cannot store the (dl) CCL details in the database.

E055 - Cannot delete the (dl) CCL details from the database.

E056 - Cannot store the (ckt1) CCL details in the database.

E057 - Cannot delete the (ckt1) CCL details from the database.

E058 - Invalid shelf type in xconreq

E059 - MSP Switch Type not consistent with value specified in ineparam6

See E1007.

E101- Invalid Data - Unknown node in request.

There is no network element with the name specified in the request.

Check the ITM-SC node list for a list of node names.

E110 - Invalid 'msp' value or failure when reading MSP state.

The msp field in an xconreq message must be either 'Y' or 'N' if used. This error code will also be output if the ITM-SC is unable to determine the MSP state of the specified port.

E111 - Invalid ineparam6 value in port provisioning or verification command.

The message field ineparam6 must only be "UNI" or "BI" if used.

The message field ineparam2 must only be ″AMI″ or ″B8ZS″ if used.

E112 - Failed Operation - port not in service.

During a verification, it was found that the specified port was not in service.

E113 - Failed Operation - Protection port not in service.

A verification of a ports with MSP protection found that the protecting port was not in service.

Check/correct the state of the protecting port and MSP scheme using the ITM-SC.

E120 - Invalid Data - Invalid equip type for VC4 facility.

E121 - Invalid 'chass' value for VC4 facility.

Channel assignment (chass) value must be 'Y' for a VC4 facility request

E122 - Invalid Data - VP specified for VC4 facility.

E123 - Failed Operation - Provision Logical Port (VC3) Failure.

E124 - Failed Operation - Invalid transmission parameters supplied.

E125 - Provisioning command failed.

An attempt to PROV/CHNG/DPRV an SDH physical port at S16DL, S4DL or V4DL has failed.

E126 - Provisioning command failed.

An attempt to PROV/CHNG/DPRV a PDH physical port at C1, C1DL, C3, C3DL, D3, D3DL, C4 or C4DL has failed.

E130 - Failed Operation - Provision VC4 TUG Structure Failure - LP1 port.

Operation to structure ISM LP1 VC4 TUG for VC3s failed or could not be set up. This can be caused by a loss of association with the

network element or by the VC4 already being in-use in an unstructured cross-connect.

Check the status of the network element and VC4 using the ITM-SC.

E131 - Failed Operation - Provision VC4 TUG Structure Failure - LP2 port.

Operation to structure ISM LP2 VC4 TUG for VC3s failed or could not be set up. This can be caused by a loss of association with the network element or by the VC4 already being in-use in an unstructured cross-connect.

Check the status of the network element and VC4 using the ITM-SC.

E132 - Failed Operation - Provision VC4 TUG Structure Failure - tributary port.

Operation to structure ISM tributary VC4 TUG for VC3s failed or could not be set up (UIIJ_DACSCAN_PROV_VC4_TUG failed). This can be caused by a loss of association with the network element or by the VC4 already being in-use in an unstructured cross-connect.

Check the status of the network element and VC4 using the ITM-SC.

E133 - Failed Operation - DeProvision VC4 TUG Structure Failure.

Operation to deprovision ISM VC4 TUG failed or could not be set up (UIIJ_DACSCAN_PROV_VC4_TUG failed). This can be caused by a loss of association with the network element or by the presence of cross-connects using the TUG structure.

Check the status of the network element and cross-connections using the ITM-SC.

E134 - Failed Operation - Provision VC4 TUG Structure Failure (XC modify).

Operation to TUG structure the VC4 for the protecting port when adding protection or to reset TUG structuring when removing protection, failed (UIJ_DACSCAN_PROV_VC4_TUG failed).

E135 - Failed Operation - Provision VC4 TUG Structure Failure (VC4 facility / VP).

E140- Failed Operation - De-Provision Virtual Port (VC4 XC) Failure

Operation to disconnect and deprovision a virtual port failed (UIJ_DACSCAN_VIRTUAL_PORT_PROV failed).

E141 - Failed Operation - Provision Virtual Port (Prov XC) Failure.

Operation to provision and connect a virtual port failed (UIJ_DACSCAN_VIRTUAL_PORT_PROV failed).

E142- Failed Operation - Virtual Port verification failure.

E150 - XC validation: Invalid 'rate' value for cross connection.

Rate must be V4, TUG3, or VC12.

E151 - XC validation: 'from' or 'to' port not specified for cross connection.

Both fromport and toport fields in the xconreq message are necessary for all cross-connections.

E152 - XC validation: 'newto' for cross connection is not a line port.

The newto field of the xconreq message, if specified must be an LP.

E153 - XC validation: 'newfrom' not a line port.

The newfrom field of the xconreq message, if specified must be an LP.

E154 - XC validation: 'typ' invalid for MDFY XC.

For a MDFY (modify command) the 'typ' field in the xconreq message must be either 'P' or 'U'.

E155 - XC validation: Unrecognized/Unsupported 'typ' value

Valid typ field is one of: 'T', 'O', 'P', 'U', 'A', 'Z' or 'B'. - some of these may not be supported for a particular release, in which case TMAG should be referred.

E156 - XC validation: Two VP's specified for XC.

E157 - XC validation: VP & rate invalid for type 'T' XC.

E158 - XC validation: 'newto' specified for unprotected XC.

Only fromport and toport should be set for an unprotected cross-connection.

E159 - XC validation: 'newfrom' specified for unprotected XC.

Only fromport and toport should be set for an unprotected cross-connection.

E160 - XC validation: Invalid rate for type 'O' XC.

Rate must be TUG3 for typ O (one-way) cross-connections.

E161 - XC validation: 'newto' specified for type 'O' XC.

Only fromport and toport should be set in a type O (one-way) cross-connection since this is an unprotected type.

E162 - XC validation: 'newfrom' specified for type 'O' XC.

Only fromport and toport should be set in a type O (one-way) cross-connection since this is an unprotected type.

E163 - XC validation: VP & rate invalid for type 'P' XC.

E164 - XC validation: VP specified as 'toport' for type 'P' XC.

E165 - XC validation: 'newto' not specified for type 'P' XC.

The newto field of the xconreq message must be set for a type P (protected) cross-connection and newto length is not zero.

E166 - XC validation: 'newfrom' specified for type 'P' XC.

The newfrom field of the xconreq message must NOT be set for a type P (protected) cross-connection.

E167 - XC validation: Type 'A' Cross Connection Incorrectly specified.

For a type A (one-way protected add) cross-connection:

- rate must be TUG3
- fromport must be a TP
- toport must be an LP
- newto must be zero
- newfrom must NOT be specified.

E168 - XC validation: Type 'Z' Cross Connection Incorrectly specified.

For a type Z (one-way protected drop) cross-connection:

- rate must be TUG3
- fromport must be a LP
- toport must be an TP
- newto must NOT be specified
- newfrom length must be non-zero

E169 - XC validation: Type 'B' Cross-Connection Incorrectly specified

For a typ B (broadcast) cross-connection:

- rate must be TUG3
- newto and newfrom are of non-zero length

E170 - Provision cross connect - 'fromend' or 'toend' not specified

Fromend and toend nodes have not been specified for an SLM RDI cross-connect.

E171 - Verify XCon - 'fromend' or 'toend' not specified

E172 - Invalid 'rate' value for modify X

E173 - Failed Operation - Unknown trib type detected in NE

E174 - Failed Operation - Verify XC - 'fromend' or 'toend' mis-match

E175 - Failed Operation - Modify VC4 Struct Facility Failure

E176 - Failed Operation - Modify XC Failure

E177 - Failed Operation - Failure in generating PXC switch-event

E178 - Tributary port type is incorrect for the type of command

The port type present in the equipment does not match that required by the connection request.

E179 - Invalid Data - XC request submitted for SLM LTA

E180 - Unknown "pti_mode"

The value for pti_mode was not "enable", "disable", "", or "no_change". For CONN commands, only "enable" and "disable" are valid.

E181 - Failed Operation - PROV - pti_t not specified

E182 - Failed Operation - PROV - pti_e not specified.

E183 - Failed Operation - CHNG - pti_mode mismatch.

E184 - Invalid pti_mode in request.

E185 - Failed Operation - PROV - pti_t exceeds maximum permitted length

E186 - Failed Operation - PROV - pti_e exceeds maximum permitted length

E190 - Invalid ineparam1

For a virtual port cross-connect the “typ” must be “T” or “P” (for example, two-way or two-way protected).

E191 - Tug Group or Ch Type invalid

The xconreq contains invalid tug group or channel type.

E192 - Tug Comparison Failed

The xconreq has a different tug structure than the xconreq already structured.

E193 - Failed Operation - CHNG - Expected PTI not as specified

E194 - Failed Operation - CHNG - Transmitted PTI not as specified

E195 - Failed Operation - CHNG - PTI mismatch detection not as specified

E196 - Failed Operation - CHNG - Expected and transmitted PTI not as specified

E197 - Failed Operation - CHNG - Expected and transmitted PTI and mismatch detection not as specified

E198 - Failed Operation - CHNG - Expected PTI and mismatch detection not as specified

E197 - Failed Operation - CHNG - Transmitted PTI and mismatch detection not as specified

E199 - Failed Operation - Invalid internal response for a cross connect request

E200 - Failed Operation - Invalid internal response before a cross connect request due to:

- Failure of AU4 concatenation
- Failure of AU3/AU4 clear signal
- Failure of TUG structure Creation/Modification
- Set/Reset failure for CTP alarm monitoring

E201 - V4DL MSP PROV - newfrom not specified or not valid.

E202 - Requested C1 Actual Interface Type incorrect.

- Actual Interface Type specified by ineparam7 is neither ″NORMAL″ nor ″ISDN-PRI″
- Actual Interface Type specified by ineparam7 is ″ISDN-PRI″ but node is not WaveStar® AM1 Plus

E203 - Node is not an AM1 Plus.

E204 - Requested D1 Line Coding is incorrect.

E205 - Current D1 Line Coding is different from PROV request, and a TP with that line-coding is associated with either the source or sink of a cross-connect.

E206 - PDH Line Monitoring ingress & egress are not set to the same correct value.

E207 - fromfr incorrect.

E208 - STM4 V4 Port Provisioning: unable to check existance of AU4 CTP/VC4 TTP XC.

E209 - STM4 V4 CHNG: AU4 CTP/VC4 TTP XC does not exist.

E210 - STM4 V4 Port Provisioning: AU4 CTP and/or VC4 TTP are cross-connected to other TP(s).

Error codes for switch request and retrieve commands

Error codes for switch requests and retrieve commands

E501 - Unable to perform switch operation

Request to perform a switch operation or verify has failed. For switch requests, this could be caused by loss of association with the network element. For both switch requests and switch retrieves, this could be caused by the protection scheme not existing as expected.

Check the status of the network element and the protection scheme using the ITM-SC.

E502 - Unknown switch request command.

E503 - Bad port format for protected VC4 port in switch request.

E504 - Invalid shelf type in switch event.

E505 - Bad port format for protecting VC4 port in switch request.

E506 - Invalid or missing protected port in switch request.

The port (EID) specified was missing or not valid:

- value is out of range
- port type is inappropriate for the requested rate
- The port specified in the command for the protected port was not recognized as a valid port which has protection. For example, LP20 and LP60 on ADM 4/1, LP1 on ISM and LP1, TP1.1,TP1.2, etc. on SLM.

E507 - Invalid or missing service port in switch request.

See E506.

E508 - Invalid or missing protecting port in switch request.

See E506.

E509 - Bad port format for protected port in switch retrieve.

E510 - Bad port format for service port in switch retrieve.

E511 - Bad port format for protecting port in switch retrieve.

E512 - Bad switch request received.

E513 - MSP scheme failed.

E514 - Protected port not in MSP scheme.

E515 - Unable to determine switch request type from data received.

E516 - Unable to determine switch retrieve type from data received.

E517 - Bad ports specified

Two of the ports (protected, protecting and service) are the same in a switch request.

E518 - Bad ineparam6 specified

Ineparam6 must be ″UNI″ for SLM tributaries with MSP.

E520 - Unknown switch command type

The switch command type was not ’S’ (switch) or ’R’ (retrieve).

E521 - Invalid Rate in protection switch command

Command = R: rate must be V12,C1,V3,C3 or D3.

Command = S: for MSP rate must be S16DL or V4DL.

For SNCP rate, must be V12, C1, V3, C3, D3, V4, or C4.

E522 - MSP not supported

In the current release, switch event type MSP is not supported.

E523 - Invalid type in protection switch command

For command R, type in switch event must be SNCP.

For command S, type in switch event must be SNCP or MSP.

E524 - pdh_level not same

For SNCP all 3 ports must be same pdh_level (2Mb, 34Mb or 45Mb)

E525 - Port and rate not consistent

The port type must be consistent with rate.

E526 - Unknown request in switch_event

The switch_event contains an invalid or missing request.

E527 - Request in switch_event is LCK

LCK request is not allowed for Protected cross-connect switch_event.

E528 - MSP switch_event contains an STM-4 port

For WaveStar® ADM 4/1 nodes, MSP switch requests are not allowed on STM-4 ports.

E529 - Invalid rate field supplied in switch event.

E530 - Failed to allocate memory for a MSP switch request

E531 - Failed to send a MSP switch request UIJ.

Could not add the UIJ to the outgoing message queue.

E532 - Unable to determine the port type from the Equipment ID String. (EID)

E533 - Unable to Parse the EID

The structure of the Equipment ID, or some of its elements was/were invalid.

E534 - Protected slot should be odd.

E535 - Unable to get a valid protected port type from the database.

E536 - Unable to get a valid protecting port type from the database.

E537 - Database protected port type is inconsistent with the switch request (TMAG) rate

E538 - Database protecting port type is inconsistent with the switch request (TMAG) rate

E539 - Failed Operation - Invalid internal response for a MSP switch request

□

Error codes for resynchronization requests

Error codes for resynchronization requests

E601 - TID specified in an all nodes resync request.

E602 - Unknown resync type.

E603 - Data for resync not found.

For example, bad TID specified.

□

Error codes for performance monitoring requests

Error codes for performance monitoring requests

E701 - Port format or trail type incorrect for performance monitoring command.

E702 - Unknown granularity in performance monitoring command.

E703 - Bad VC12 port format for performance monitoring command.

E704 - Bad VC4 port format for performance monitoring command.

E705 - Bad MS or RS port format for performance monitoring command.

E706 - Failed to find termination point.

E707 - Invalid status code received from PM server.

E708 - Failed to create performance monitoring report file.

It was not possible to complete the creation of the requested data file. There are several possible causes for this:

- start and/or stop times are invalid
- report file name already in use
- PM server failed to open/create file
- Internal PM server resource error

E709 - Failed to transfer report file to host machine.

E710 - Bad counter type.

E711 - Could not find environment variable $EMSDACSCANRE-PORTDIR

E712 - Unknown tid (NE node name) or ITM-SC is not the primary manager of the node

E713 - Bad performance monitoring command

E714 - No connection to PM server or PM feature is not licensed or timer out of range or no counters specified.

E715 - Unknown shelf or unknown equipment type.

E716 - Database access error

E717 - Failed to transfer PM archive request file from WaveStar NMS

E718 - Sequence error in PM archive request file

E719 - NE resources exceeded

A resource on a network element has been exceeded. For example, the user may have tried to set more than the maximum allowed monitoring points.

E720 - Invalid TCM type for PM.

E721 - Invalid TCM section for PM.

E722 - Invalid NE type for TCM PM.

E723 - Invalid port type for TCM PM.

E724 - Start time does not chronologically precede the stop time

E725 - Start and Stop times fail their boundary checks

E726 - Start or Stop times are in the future

□

Error codes specific to WaveStar® ADM 155e and WaveStar® ADM 4/1 network elements

Error codes specific to WaveStar® ADM 155e and WaveStar® ADM 4/1 network elements

E801 - Incorrect transmission parameters for a 2Mbit/s port

The transmission parameters in the C1 circuit provisioning must be ″ASYNC″ and ″UNMON″.

E804 - VC4 TTP could not be found

E806 - Port could not be identified

Type of port could not be determined. Probably due to bad data in the command. (ITM-SC server process rejected the identify port request.)

E807 - Deprovision of VC4 denied since a VC3 or VC12 cross connection exists

The request to deprovision the VC4 termination point has been denied because it is still being used for a lower order cross-connection (VC3 or VC12). These must be disconnected first.

Existing cross-connections can be viewed on the ITM-SC user interface.

E820 - Cross connect verify failed

The connection specified in a CONN, CHNG, DISC, MDFY or switch retrieve could not be checked against the existing configuration. This could be caused by:

- A VC4 level cross-connection has been requested but a VC4 TTP exists - use ITM-SC to delete the VC4 TTP.
- A VC12 or VC3 level cross-connect has been requested but the VC4 TTP does not exist - use ITM-SC to create the TTP.
- bad port data in the original request

E821 - Incompatible cross connection already exists

One or more of the ports specified in the requested cross-connection is already involved in a cross-connection which is incompatible with the requested cross-connection.

Check the current cross-connections via the ITM-SC.

E822 - Incorrect channel assignment (″chass″) value

For PDH tributaries, the chass must be “Y.”

For SDH tributaries, the chass must be “N.”

E825 - Failed to delete protection on cross connection

The operation to delete the protection arm of a cross-connection failed. This is the first stage of a disconnection so the cross-connection will be unaffected by the failure.

E827 - Failed to enable or disable PTI miss-match detection on port

The operation to enable or disable the PTI miss-match detection and set the PTI values failed. A possible cause is loss of association with the network element.

(UIJ_DACSCAN_PROV_TP_VC12 failed or couldn’t be set up)

E828 - Requested VC12 cross-connection is not possible

On WaveStar ADM 4/1, there is a hardware limitation on the connection of 2Mbit/s tributary ports on 32x2Mbit/s cards. The 32x2 cards can be recognized as 16x2 units in adjacent ″slots″, for example, slots 21 & 22, 31 & 32 etc. The limitation is that these ports may only be connected to the LP on the same side of the shelf, for example, TP21.1 to LP20 but not LP60. This of course means protected cross-connections are not possible on this type of unit.

E830 - Unable to add protection because ports are already in an MSP scheme.

The VC4 protection is mutually exclusive with the MSP scheme.

E831 - PROV, DPRV or CHNG with MSP requested on ADM4/1 STM-4 ports.

Port provisioning commands which involve MSP cannot be performed on WaveStar ADM 4/1 STM-4 ports.

E832 - msp on ADM4/1 STM-4 ports.

msp=Y and rate=V4DL not allowed for STM4 - see TMAG Appendix 7, Section 6, Rule 1.

□

Error codes specific to PHASE and WaveStar® ADM 16/1 network elements

Error codes specific to PHASE and WaveStar® ADM 16/1 network elements

E850 - Cannot store the (dl) CCL details in the database.

E851 - Cannot store the (ckt) CCL details in the database.

E852 - Cannot store the (ckt1) CCL details in the database.

E853 - Cannot delete the (dl) CCL details from the database.

E854 - Cannot delete the (ckt) CCL details from the database.

E855 - Cannot delete the (ckt1) CCL details from the database.

E856 - Failed Operation - Unable to set the PTI values when provisioning VC3TTP.

E857 - Failed Operation - Unable to deprovision Synchronous Physical Port.

E858 - Failed Operation - Unable to reset PTI values when deprovision V3 Logical port.

E859 - Port validation failed. Port roles are reversed.

E860 - Provisioned ports not part of same MSP scheme.

E861 - Unknown MSP status.

E862 - Invalid PTI fields

E863 - Verify port failed. Cannot find MOI in the database.

E864 - Verify port failed. Neither port involved in MSP.

E865 - Verify port failed. Ports involved in different MSP or only one of them is involved in MSP.

E866 - Port validation failed. Confusion over dual-ended and uni.

Valid combinations are:

- Single Ended & UNI
- Dual Ended & BI

E867 - Port validation failed. Could not find msTTP in database.

E868 - Invalid field in request. Empty string, zero value or not NONE.

Generated when dest, tid, command, rate, fromport, cac or clo is a null string. Generated when msgno or layout have the value 0. Generated when pti_mode=nochange, rate=V12 or C1, command=PROV and the pti fields do not have the value NONE. Generated when pti_mode=nochange, rate=V12 or C1, command=CHNG and the pti fields do not have the value NONE or null string.

fromfr and tofr is NULL.

E869 - Invalid field in request. Shelf type does not match rate.

E870 - Invalid EID in request.

E871 - PTI information not supplied.

E872 - Inconsistent signal mapping specified. Mismatch between rate and ineparam4.

E873 - Invalid field in request. Cannot find fromport details in database.

E874 - Invalid field in request. Mismatch between V4 stm_level and AU4 number.

E875 - Invalid field in request. Mismatch between rate and stm_level.

E876 - Invalid field in request. Mismatch between pdh_level and rate.

E877 - Invalid fromfr.

E878 - Invalid tofr.

E879 - Internal cross connection provisioning problem.

The internal cross-connection is either not provisioned, not provisioned correctly, or could not be provisioned. For example, no free CCU VC4s were available.

E880 - *fr is incompatible with Port Level.

Network Level Address is incompatible with port level.

E881 - *fr is incompatible with rate.

Network Level Address is incompatible with rate.

E882 - Conflicting Line Coding

The line coding (AMI or B8ZS) needs to be the same for each port in the group.

E888 - Port is carrying traffic.

Cannot DPRV this port since it is carrying low-order traffic.

E889 - High order SNC/P and MS-SPRING are mutually exclusive.

An attempt was made to create (via CONN or MDFY P) a high order protected cross-connect when MS-SPRING was in place.

E890 - Invalid pti_mode.

When the command is PROV, the mode can be “enable” or “disable.” When the command is CHNG, the mode can be “enable,” “disable,” or NULL.

E891 -Invalid ineparam4

Invalid combination of ineparam4 and ineparam5. Bad value was ineparam4.

E892 -Invalid ineparam5

Invalid combination of ineparam4 and ineparam5. Bad value was ineparam5.

E895 -Cross Connect is either unidirectional, protected or not external

A VC3 or VC12 path was found to be in one of the above states.

E896 - Internal cross connection does not exist for vc4 path

An internal cross-connection does not exist. It may be unidirectional, protected, or external.

E897 - External HO cross connect is not in place

Attempt to PROV or DPRV a LO cross-connect when an external HO cross-connect is not in place. Possible causes are no provisioned HO cross-connect or internal CCU cross-connect.

E901 - Invalid equipment type in xconreq.

E902 - Invalid shelf type in xconreq.

In XCONREQ validation, supported shelves are CS17/TM4, CS17/TM16, CS19/TM4, CS19/TM16, CSADMN4/ADM44, CSADMN4/ADM164.

E903 - TUG XC pointers not read within timeout period.

Cross-connect pointers for a TUG port should be readable. If not, the substructuring of the containing VC4 port has failed.

E904 - DB access failed during XC directionality check.

Unexpected failure of database access.

E905 - DB access failed during XC to port termination list check.

Unexpected failure of database access.

E906 - XC verification failed due to invalid XC state.

Current state of cross-connect stored in database is not recognized during verification.

E907 - Reset PTI UIJ job failed.

UIJ job has reported failure.

E908 - TUG sub-structuring UIJ job failed.

UIJ job has reported failure.

E909 - Failure to access TUG XC pointers.

Unexpected database failure while attempting to access cross-connect pointers for a TUG port.

E910 - UIJ message building failed.

Failed to build a UIJ message structure prior to sending to the UIS.

E911 - Provision PTI UIJ job failed.

UIJ job has reported failure.

E912 - DB access failed during XC id check.

Unexpected failure of database access.

E913 - PTI validation failed on CHNG command.

Verification of PTI data in XCONREQ against database has failed.

E914 - XC validation failed, toport and newto must be line.

For bidirectional protected cross-connects, Navis™ Optical NMS toport and newto must be line ports.

E915 - XC validation failed, fromport must be trib.

For bidirectional protected cross-connect on WaveStar® TM 1 or WaveStar® AM 1, Navis™ Optical NMS from port must be tributary.=

E916 - AU4 number out of range for SDH port.

AU4 number in range 1 to 16 expected.

E917 - AU4 number present, but port is PDH.

AU4 number of 0 expected.

E918 - PTI validation failed.

Validation of XCONREQ PTI data has failed.

E919 - Invalid rate for given shelf.

Invalid rate for ADM or TM shelf. Should be V4 or C4.

E920 - More than 1 trib port specified.

For ADM or TM shelf, only one port can be tributary.

E921 - From or to port must be line for PHASE ADM shelf.

For ADM shelf, Navis™ Optical NMS from or Navis™ Optical NMS to port must be line.

E922 - Ports in XC must be on different units.

Slot numbers for each port were not all different.

E923 - More than 1 line port for PHASE TM shelf.

Only one line port allowed for WaveStar® TM 1 shelf.

E924 - No protection allowed for PHASE TM shelf.

XCONREQ should not attempt protection on WaveStar® TM 1 shelf.

E925 - Failure verifying port exists in database.

Navis™ Optical NMS port (or VC4 supporting TUG) not accessible in database.

E926 - Port is not allowed to be part of an MSP group.

On ADM shelf, with MDFY or CONN command and cross-connect type P, Z, S or B with new from, no port may be part of MSP group.

E927 - Port can not be connected to themselves.

E928 - UIJ Job Failed.

UIJ job has reported failure.

E929 - Error while verifying transmission parameters.

Supplied CHNG transmission parameters do not match those of the actual port.

E950 - XC validation failed, toport and newto must be on different lines.

For bidirectional protected cross-connects, Navis™ Optical NMS toport and newto must be on different lines.

E951 - Port has invalid directionality.

E952 - AU4 port is in concatenation group, command refused.

E953 - tsp_flag is invalid, command refused.

E954 - XC validation: newto is not set.

E955 - XC validation: newfrom is not set.

E956 - XC validation: Invalid newto/newfrom for typ B cross connection.

E960 - “rate” parameter invalid for TCM.

E961 - “typ” parameter invalid for TCM.

E962 - fromport must be specified for TCM

E963 - TCM NIM pair conditions not met.

E964 - Phase NE must be LXC4/16 to support TCM.

E965 - NE does not support TCM (hardware or software not upgraded).

E966 - pti_mode param invalid for TCM, must be ″enable″ or ″disable″.

E967 - Cross connnect not in valid state for TCM.

E968 - Failed to create TCM point.

E969 - Failed to delete TCM point.

E970 - Failed to change SNCP protection (TCM pair).

E971 - The TP is not cross connected. Cannot create TCM point since the TP is not cross connected (is not in a path yet).

E972- Node model type error , must not be MSSPRING.

□

Miscellaneous error codes

Miscellaneous error codes

E998 - Feature not supported in current release.

E999 - Software or system fault.

See EMS log file for further details. If necessary, the system will restart to regain integrity.

□

Error codes specific to WaveStar® OLS 80G network elements

Error codes specific to WaveStar® OLS 80G network elements

E1000 - Invalid node type.

Attempt to provision/de-provision a repeater node.

E1001 - Invalid TP.

Requested TP does not have an Input AND Output Port.

E1002 - Rate Mismatch

Rates for Input/Output are not correctly matched to requested rate.

E1003 - Invalid Port.

A request was made to provision an OMSP protected port that is not part of an OMSP protection scheme.

E1004 - Invalid apsd_enabled value for this Node.

apsd_enabled should be set to false for a uni-directional port.

E1005 - Invalid omspOpState.

omspOpState was expected to be enabled.

E1006 - Invalid protectionGroupType

protectionGroupType was expected to be ″plus″.

E1007 - protectionSwitchMode is not consistent with the value requested in ineparam6.

Valid values of ineparam6 are:

Table 5-1 Valid values for ineparam6

ineparam6	protectionSwitchMode
BI	revertive
UNI	nonrevertive

E1008 - fromport supplied inconsistent with the primary line of the OMSP group.

E1009 - An attempt to provision OMSP (MSP=Y) on a Single Ended Terminal type.

E1011 - No MIB object exists for Line Port.

E1012 - Invalid ch_type in cross connect request.

Valid examples of ch_type are V4DL, S4DL, S16DL and LSBB

E1013 - Invalid Expected Item Code.

E1014 - Invalid Association.

Error codes for Navis™ Optical NMS/WaveStar® ITM-SC login

Error codes for Navis™ Optical NMS/ITM-SC login

INAI - Agent Id does not match the WaveStar® ITM-SC host

SNVS - Navis™ Optical NMS not recognized by WaveStar® ITM-SC

ARAS - WaveStar® ITM-SC already associated with a Navis™ Optical NMS

SVMM - Mismatch of software versions between Navis™ Optical NMS and WaveStar® ITM-SC

□

Error codes specific to WaveStar® DACS network elements

Error codes specific to WaveStar® DACS network elements

E12100 - E12131 - Internal GUMS failure response for a cross connect request

E12300 - E12301 - Internal GUMS failure response for MSP switch request

□

6 Performance monitoring parameters

Overview

Purpose

This chapter describes performance monitoring concepts as related to Navis™ Optical NMS.

Contents

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 NMS.

Contents

Performance monitoring parameters

Overview

Navis™ Optical NMS 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

Table 6-1 Performance monitoring parameters (continued)

Parameter	Description
npjcg	Negative Pointer Justification Generated
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

SDH termination point performance parameters - WaveStar® ITM-SC managed network elements

SDH termination point performance parameters

The following table lists the termination point performance parameters for ISM, SLM, WaveStar® ADM 155e, WaveStar® ADM 4/1, WaveStar® ADM 16/1, and WaveStar® ADM 16/1 Compact.

Table 6-2 Termination point performance parameters for WaveStar® ITM-SC managed network elements

Monitored Termination Point	ISM R3.5	SLM R5.0	WaveStar® ADM155e, WaveStar® ADM4/1 V5	WaveStar® ADM16/1	WaveStar® ADM 16/1Compact
VC12TTP	NE-ES NE-SES NE-UAS NE-CV-BBE	—	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS
VC11TTP (DS1)	—	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS	—
VC3TTP	NE-ES NE-SES NE-UAS NE-CV-BBE	—	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS
VC4TTP	NE-ES NE-SES NE-UAS NE-CV-BBE	NE-ES NE-SES NE-UAS NE-CV-BBE	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS
TU12CTP	—	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS
TU2CTP	—	—	—	—	—
TU3CTP	—	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS
AU3CTP	—	—	—	—	—

Table 6-2 Termination point performance parameters for WaveStar® ITM-SC managed network elements (continued)

Monitored Termination Point	ISM R3.5	SLM R5.0	WaveStar® ADM155e, WaveStar® ADM4/1 V5	WaveStar® ADM16/1	WaveStar® ADM 16/1Compact
AU4CTP	—	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS
AU4–4C CTP (VC4–4C)	—	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS
AU4–16C CTP (VC4–16C)	—	—	—	—	—
MSTTP	NE-ES NE-SES NE-UAS BE-CV-BBE (MS4 & MS1)	NE-ES NE-SES NE-UAS BE-CV-BBE (MS16, MS4 & MS1)	NE-CV-BBE NE-ES NE-SES NE-UAS (MS1)	NE-CV-BBE NE-ES NE-SES NE-UAS (MS1, MS4, MS16)	NE-CV-BBE NE-ES NE-SES NE-UAS MS1, MS4, MS16)
RSTTP	—	NE-ES NE-SES NE-UAS BE-CV-BBE (RS16, RS4)	—	NE-CV-BBE NE-ES NE-SES NE-UAS (RS16)	NE-CV-BBE NE-ES NE-SES NE-UAS (RS16)
Physical PITTP[1]	—	—	—	—	—
TCM VC12TTP	—	—	—	—	—
TCM VC3TTP	—	—	—	—	—
TCM VC4TTP	—	—	—	—	—
TCM TU12CTP	—	—	—	—	—
TCM TU2CTP	—	—	—	—	—
TCM TU3CTP	—	—	—	—	—

Notes:

1. For these parameters, the network elements report “good” or “not good.” In graphical terms, these parameters are represented as either one large bar for “not good” and no bar for “good.”

SDH termination point performance parameters - WaveStar® ITM-SC managed network elements

The following table lists the termination point performance parameters for PHASE ADM/TM, PHASE LXC, PHASE LR, WaveStar® AM 1/TM 1, WaveStar® AM 1 Plus, and WaveStar® DACS.

Table 6-3 Termination point performance parameters for PHASE, WaveStar® AM, and WaveStar® DACS network elements

Monitored Termination Point	Phase ADM/TM	Phase LXC	WaveStar® AM-1/TM-1	WaveStar® AM-1 Plus	WaveStar® DACS
VC12TTP	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	—
VC11TTP (DS1)	—	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS	—
VC3TTP	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	—

Table 6-3. Termination point performance parameters for PHASE, WaveStar® AM, and WaveStar® DACS network elements (continued)

Monitored Termination Point	Phase ADM/TM	Phase LXC	WaveStar® AM-1/TM-1	WaveStar® AM-1 Plus	WaveStar® DACS
VC4TTP	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-ES NE-SES NE-UAS NE-CV-BBE FE-ES FE-SES FE-UAS FE-CV-BBE
TU12CTP	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—	—	NE-ES NE-SES NE-UAS NE-CV-BBE FE-ES FE-SES FE-UAS FE-CV-BBE
TU2CTP	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—	—	—

Table 6-3 Termination point performance parameters for PHASE, WaveStar® AM, and WaveStar® DACS network elements (continued)

Monitored Termination Point	Phase ADM/TM	Phase LXC	WaveStar® AM-1/TM-1	WaveStar® AM-1 Plus	WaveStar® DACS
TU3CTP	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—	—	NE-ES NE-SES NE-UAS NE-CV-BBE FE-ES FE-SES FE-UAS FE-CV-BBE
AU3CTP	—	—	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS
AU4CTP	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS

Table 6-3. Termination point performance parameters for PHASE, WaveStar® AM, and WaveStar® DACS network elements (continued)

Monitored Termination Point	Phase ADM/TM	Phase LXC	WaveStar® AM-1/TM-1	WaveStar® AM-1 Plus	WaveStar® DACS
AU4–4C CTP (VC4–4C)	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS
AU4–16C CTP (VC4–16C)	—	—	—	—	—
MSTTP	NE-CV-BBE NE-ES NE-SES NE-UAS [2]	NE-CV-BBE NE-ES NE-SES NE-UAS [2]	NE-CV-BBE NE-ES NE-SES NE-UAS (MS1)	NE-CV-BBE NE-ES NE-SES NE-UAS (MS1, MS4)	NE-ES NE-SES NE-UAS NE-CV-BBE FE-ES FE-SES FE-UAS FE-CV-BBE (MS16, MS4, MS1)
RSTTP	NE-CV-BBE NE-ES NE-SES NE-UAS[2]	NE-CV-BBE NE-ES NE-SES NE-UAS[2]	—	—	NE-ES NE-SES NE-UAS NE-CV-BBE RS16, RS4, RS1)
Physical PITTP[1]	—	—	—	—	—

Table 6-3 Termination point performance parameters for PHASE, WaveStar® AM, and WaveStar® DACS network elements (continued)

Monitored Termination Point	Phase ADM/TM	Phase LXC	WaveStar® AM-1/TM-1	WaveStar® AM-1 Plus	WaveStar® DACS
TCM VC12TTP	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—	—	—
TCM VC3TTP	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—	—	—
TCM VC4TTP	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—	—	—

Table 6-3. Termination point performance parameters for PHASE, WaveStar® AM, and WaveStar® DACS network elements (continued)

Monitored Termination Point	Phase ADM/TM	Phase LXC	WaveStar® AM-1/TM-1	WaveStar® AM-1 Plus	WaveStar® DACS
TCM TU12CTP	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—	—	—
TCM TU2CTP	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—	—	—
TCM TU3CTP	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—	—	—

Notes:

1. For these parameters, the network elements report “good” or “not good.” In graphical terms these parameters are represented as either one large bar for “not good” and no bar for “good.”
2. See “PHASE network element-specific rates” (6-14) for network element specific details.

PHASE network element-specific rates

The following table lists the rates supported for PHASE network elements

Table 6-4 Supported PHASE network element rates

Phase Network Element	Rate Supported
ADM 4/4	MS1, MS4, RS1, RS4
ADM 16/4	MS1, MS4, MS16, RS1, RS4, RS16
TM4/4	MS1. MS4, RS1,RS4
TM 16/4	MS1, MS4, MS16, RS1, RS4, RS16
LXC 4/1	MS1, MS4, RS1, RS4
LXC 16/1	MS1, MS4, MS16, RS1, RS4, RS16

SDH termination point performance parameters - Navis™ Optical EMS-managed network elements

SDH termination point performance parameters

The following table lists the termination point performance parameters for WaveStar® TDM 2.5/10G, WaveStar® BandWidth Manager, and LambdaUnite™ MSS.

Table 6-5 Termination point parameters for WaveStar® TDM 2.5/10G, WaveStar® BandWidth Manager, and LambdaUnite™ MSS

Monitored Termination Point	WaveStar® TDM 2.5/10G	WaveStar® BandWidth Manager	LambdaUnite™ MSS	LambdaUnite™ MSS	LambdaRouter™ AOS
VC12TTP	—	—	—	—	—
VC11TTP (DS1)	—	—	—	—	—
VC3TTP	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	—
VC4TTP	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	—
TU12CTP	—	—	—	—	—
TU2CTP	—	—	—	—	—
TU3CTP	—	—	—	—	—
AU3CTP	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	—
AU4CTP	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	—
AU4–4C CTP (VC4–4C)	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	—

Table 6-5 Termination point parameters for WaveStar® TDM 2.5/10G, WaveStar® BandWidth Manager, and LambdaUnite™ MSS (continued)

Monitored Termination Point	WaveStar® TDM 2.5/10G	WaveStar® BandWidth Manager	LambdaUnite™ MSS	LambdaUnite™ MSS	LambdaRouter™ AOS
AU4–16C CTP (VC4–16C)	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	—
AU4-64C CTP (VC4-64C)	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	—
MSTTP	NE-CV-BBE NE-ES NE-SES NE-UAS (MS64, MS16, MS4, MS1)	NE-CV-BBE NE-ES NE-SES NE-UAS (MS64, MS16, MS4, MS1)	NE-CV-BBE NE-ES NE-SES NE-UAS NE-FECC NE-FECU (MS64, MS16, MS4, MS1)	NE-CV-BBE NE-ES NE-SES NE-UAS NE-FECC NE-FECU (MS64, MS16, MS4, MS1)	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-SES FE-UAS (MS64, MS16)
RSTTP	NE-CV-BBE NE-ES NE-SES NE-UAS (RS64, RS16, RS4, RS1)	NE-CV-BBE NE-ES NE-SES NE-UAS (RS64, RS16, RS1)	NE-CV-BBE NE-ES NE-SES NE-UAS (MS64,MS16, MS4, MS1)	NE-CV-BBE NE-ES NE-SES NE-UAS (RS64,RS16, RS4, RS1)	NE-CV-BBE NE-ES NE-SES NE-UAS (RS64, RS16)
Physical PITTP[1]	LBC OPT OPR	LBC OPT OPR	LBC OPT OPR	LBC OPT OPR (PHYS16, PHYS64)	LBC OPT OPR (PHYS16, PHYS64)
TCM VC12TTP	—	—	—	—	—
TCM VC3TTP	—	—	—	—	—
TCM VC4TTP	—	—	—	—	—
TCM TU12CTP	—	—	—	—	—
TCM TU2CTP	—	—	—	—	—
TCM TU3CTP	—	—	—	—	—

Notes:

1. For these parameters, the network elements report “good” or “not

good". In graphical terms these parameters are represented as either one large bar for "not good" and no bar for "good".

□

Ethernet performance monitoring data

Ethernet performance monitoring data

The following table lists Ethernet performance monitoring data.

Table 6-6 Ethernet performance monitoring data

Monitored termination point	Metropolis™ DMX Access Multiplexer	Metropolis™ DMXpress Access Multiplexer
ENET (Ethernet port or VCG)	EDFC EDFE EINB EINF EONB EONF	EDFC EDFE EINB EINF EONB EONF

SDH termination point bidirectional performance parameters

SDH termination point bidirectional performance parameters

The following table lists the termination point bidirectional performance parameters for WaveStar® AM 1 Plus.

Table 6-7 Termination point bidirectional performance parameters for WaveStar® AM 1 Plus

Monitored Termination Point	WaveStar® AM 1 Plus R2.0
VC12TTP	NE-CV-BBE NE-ES NE-SES FE-CV-BBE FE-ES FE-SES BI-UAS
VC11TTP	NE-CV-BBE NE-ES NE-SES FE-CV-BBE FE-ES FE-SES BI-UAS
VC3TTP	NE-CV-BBE NE-ES NE-SES FE-CV-BBE FE-ES FE-SES BI-UAS
VC4TTP	NE-CV-BBE NE-ES NE-SES FE-CV-BBE FE-ES FE-SES BI-UAS

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 NMS 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). Additionally, the digital FEC counters are supported for WaveStar® OLS 1.6T R3.0, 3.1, 4.0 and 5.0.

WaveStar® OLS 1.6T optical parameters

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

Table 6-8 WaveStar® OLS 1.6T optical parameters

Navis™ Optical EMS-EML Name	Navis™ Optical NMS Name	Digital Counters WaveStar® OLS 1.6T R5.0 and prior	Digital Counters WaveStar® OLS 1.6T R6.0 and above	Analog Counters All WaveStar® OLS 1.6T releases
Optical Channel	OCHTTP	FEC-EC FEC-UBC	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)
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)

Metropolis™ EON optical parameters

The following table lists the optical network termination point performance parameters for Metropolis™ EON.

Table 6-9 Metropolis™ EON optical parameters

Navis™ Optical EMS-EML Name	Navis™ Optical NMS Name	Connection Level	Analog Counters
Optical Channel	OCHTTP	OchTrail	SPR-C OSNR-C FEC-EC FEC-UBC
Section	RSTTP	—	NE-CV-BBE NE-ES NE-SES NE-SEFS
Physical/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

LambdaXtreme™ optical parameters

The following table lists the optical network termination point performance parameters for LambdaXtreme™.

Table 6-10 LambdaXtreme™ optical parameters

Navis™ Optical EMS-EML Name	Navis™ Optical NMS Name	Connection Level	Analog Counters
Optical Channel	OCHTTP	OchTrail	SPR-C SPT-C FEC-EC FEC-UBC
OTPS	PITTP	OL	OPR (sink) OPT (source)
Optical Line	OTSTTP	OMS	TOPR-OL TOPT-OL

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 NMS.

Contents

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 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 NMS fault management feature.

Navis™ Optical NMS 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 NMS.

□

SDH threshold crossing alert parameters: WaveStar® ITM-SC managed network elements

SDH threshold crossing alert parameters

The following table lists the termination point performance parameters for WaveStar® ADM 16/1, WaveStar® ADM 16/1 Compact, WaveStar® AM 1/TM 1, WaveStar® AM 1 Plus, PHASE LXC, WaveStar® DACS.

Table 6-11 Termination point performance parameters for WaveStar® ADM, WaveStar® AM, PHASE, and WaveStar® DACS network elements

Monitored Termination Point	WaveStar® ADM 16/1	WaveStar® ADM 16/1 Compact	WaveStar® AM 1/TM 1	WaveStar® AM 1 Plus	PHASE LXC	WaveStar® DACS
VC12TTP	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—
VC11TTP	NE-CV-BBE NE-ES NE-SES NE-UAS	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS	—	—
VC3TTP	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—
VC4TTP	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS

Table 6-11 Termination point performance parameters for WaveStar® ADM, WaveStar® AM, PHASE, and WaveStar® DACS network elements (continued)

Monitored Termination Point	WaveStar® ADM 16/1	WaveStar® ADM 16/1 Compact	WaveStar® AM 1/TM 1	WaveStar® AM 1 Plus	PHASE LXC	WaveStar® DACS
TU12	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	NE-ES NE-SES NE-UAS NE-CV-BBE FE-ES FE-SES FE-UAS FE-CV-BBE
TU2	—	—	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—
TU3	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	NE-ES NE-SES NE-UAS NE-CV-BBE FE-ES FE-SES FE-UAS FE-CV-BBE
AU3CTP	—	—	—	—	—	NE-ES NE-SES NE-UAS NE-CV-BBE FE-ES FE-SES FE-UAS FE-CV-BBE

Table 6-11 Termination point performance parameters for WaveStar® ADM, WaveStar® AM, PHASE, and WaveStar® DACS network elements (continued)

Monitored Termination Point	WaveStar® ADM 16/1	WaveStar® ADM 16/1 Compact	WaveStar® AM 1/TM 1	WaveStar® AM 1 Plus	PHASE LXC	WaveStar® DACS
AU4CTP	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS
AU4–4cCTP (VC4–4C)	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	—	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS
AU4–16cCTP (VC4–4C)	—	—	—	—	—	—
MSTTP	NE-CV-BBE NE-ES NE-SES NE-UAS (MS1, MS4, MS16)	NE-CV-BBE NE-ES NE-SES NE-UAS (MS1, MS4,MS16)	NE-CV-BBE NE-ES NE-SES NE-UAS (MS1)	NE-CV-BBE NE-ES NE-SES NE-UAS (MS1, MS4)	NE-CV-BBE NE-ES NE-SES NE-UAS“LXC network element specific rates” (6-28)	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS (MS16, MS4, MS1)
RSTTP	NE-CV-BBE NE-ES NE-SES NE-UAS (RS16)	NE-CV-BBE NE-ES NE-SES NE-UAS (RS16)	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS[3]	NE-CV-BBE NE-ES NE-SES NE-UAS (RS16) (RS16, RS4, RS1)
Physical PITTP[1]	—	—	—	—	—	—

Table 6-11 Termination point performance parameters for WaveStar® ADM, WaveStar® AM, PHASE, and WaveStar® DACS network elements (continued)

Monitored Termination Point	WaveStar® ADM 16/1	WaveStar® ADM 16/1 Compact	WaveStar® AM 1/TM 1	WaveStar® AM 1 Plus	PHASE LXC	WaveStar® DACS
TCM VC12TTP	—	—	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—
TCM VC3TTP	—	—	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—
TCM VC4TTP	—	—	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—
TCM TU12CTP	—	—	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—

Table 6-11 Termination point performance parameters for WaveStar® ADM, WaveStar® AM, PHASE, and WaveStar® DACS network elements (continued)

Monitored Termination Point	WaveStar® ADM 16/1	WaveStar® ADM 16/1 Compact	WaveStar® AM 1/TM 1	WaveStar® AM 1 Plus	PHASE LXC	WaveStar® DACS
TCM TU2CTP	—	—	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—
TCM TU3CTP	—	—	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS FE-CV-BBE FE-ES FE-SES FE-UAS	—

Notes:

1. For these parameters, the TCA thresholds are fixed and cannot be set via Navis™ Optical NMS. The user may only enable and disable the TCAs. The default setting is “enabled”.
2. See “LXC network element specific rates” (6-28) for details of rates supported.
3. See “PHASE network element-specific rates” (6-14) for details of rates supported.

LXC network element specific rates

The following table lists the rates supported for LXC network elements.

Table 6-12 Rates supported per LXC network element

LXC Network Element	Rate Supported
LXC 4/1	MS1, MS4, RS1, RS4
LXC 16/1	MS1, MS4, MS16, RS1, RS4, RS16

SDH threshold crossing alert parameters - Navis™ Optical EMS-managed network elements

SDH threshold crossing alert parameters

The following table lists the termination point performance parameters for WaveStar® BandWidth Manager, WaveStar® TDM 2.5/10G, and LambdaUnite™ MSS.

Table 6-13 Termination point performance parameters for WaveStar® BandWidth Manager, WaveStar® TDM 2.5/10G, and LambdaUnite™ MSS

	WaveStar® BandWidth Manager	WaveStar® TDM 2.5/10G	LambaUnite™ MSS
VC12TTP	—	—	—
VC11TTP	—	—	—
VC3TTP	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS
VC4TTP	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS
TU12	—	—	—
TU2	—	—	—
TU3	—	—	—
AU3CTP	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS
AU4CTP	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS
AU4–4cCTP	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS

Table 6-13 Termination point performance parameters for WaveStar® BandWidth Manager, WaveStar® TDM 2.5/10G, and LambdaUnite™ MSS (continued)

	WaveStar® BandWidth Manager	WaveStar® TDM 2.5/10G	LambaUnite™ MSS
AU4–16cCTP	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS	NE-CV-BBE NE-ES NE-SES NE-UAS
AU4-64cCTP	—	—	NE-CV-BBE NE-ES NE-SES NE-UAS
MSTTP	NE-CV-BBE NE-ES NE-SES NE-UAS NE-FECC NE-FECU (MS64, MS16, MS4, MS1)	NE-CV-BBE NE-ES NE-SES NE-UAS NE-FECC NE-FECU (MS64, MS16, MS4, MS1)	NE-CV-BBE NE-ES NE-SES NE-UAS (MS64, MS16, MS4, MS1)
RSTTP	NE-CV-BBE NE-ES NE-SES NE-UAS (RS64, RS16,MS1)	NE-CV-BBE NE-ES NE-SES NE-UAS (RS64, RS16, RS4, RS1)	NE-CV-BBE NE-ES NE-SES NE-UAS (RS64, RS16, RS4, RS1)
Physical PITTP[1]	LBC OPT OPR	LBC OPT OPR	LBC OPT OPR

Notes:

1. For these parameters, the TCA thresholds are fixed and cannot be set via Navis™ Optical NMS. The user may only enable and disable the TCAs. The default setting is “enabled.”

□

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 6-14 Optical threshold crossing alert parameter settings

Monitored Termination Point	Digital Counters WaveStar® OLS 1.6T R5.0 and prior	Digital Counters WaveStar® OLS 1.6T R6.0 and above	Analog Counters All WaveStar® OLS 1.6T releases
OCHTTP	FEC-EC FEC-UBC	—	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. For WaveStar® OLS 1.6T R6.0 and later, the FEC counters are moved to the Physical layer. Navis™ Optical NMS 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.

□

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

Trail types

Trail types

The Navis™ Optical NMS performance monitoring feature is based on trails and transport connections. Trails must be provisioned by configuration management on the network elements before performance monitoring can be started on the Navis™ Optical NMS for the trail.

For performance monitoring, the ITU-T definition of trail is used. According to the ITU-T definition, two access points delimit a trail, one at each end of the trail. The trail ends are associated with network connections. Although performance monitoring is based on a trail, the monitored points do not have to necessarily be the trail end points. Supported network elements support performance monitoring on Trail Termination Points (TTP) and Connection Termination Points (CTP).

The trail types listed below are supported at the network element level, from where the Navis™ Optical NMS can obtain and display performance monitoring data. This assumes that the associated performance monitors on the trail have been started at the network element from the EMS.

- RS0: Regenerator Section (STM-0)
- RS1: Regenerator Section (STM-1)
- RS4: Regenerator Section (STM-4)
- RS16: Regenerator Section (STM-16)
- RS 64: Regenerator Section (STM-64)
- MS0: Multiplex Section (STM-0)
- MS1: Multiplex Section (STM-1)
- MS4: Multiplex Section (STM-4)
- MS16: Multiplex Section (STM-16)
- MS64: Multiplex Section (STM-64)
- VC-3: Virtual Container 3 (VC-3)
- VC-4: Virtual Container 4 (VC-4)
- VC4-4c: Concatenated VC4-4c
- VC4-16c: Concatenated VC4-16c
- VC4-64c: Concatenated VC4-64c

- VC-12: Virtual Container 12 (VC-12)
- VC11 (as part of the simple combo circuit VC12-VC11-24N) for WaveStar® ADM16/1 only.

For specific definitions and algorithms used to calculate these measurements, refer to ITU-T G.821 and G.826. Recommendations of acceptable threshold requirements can be found in ITU-T G.784.

□

Connection level/trail types: WaveStar® DACS, WaveStar® ADM 16/1, WaveStar® ADM 16/1 Compact, and WaveStar® ADM 4/1

Connection level/trail types

The following table shows the connection level/trail types supported by the WaveStar® DACS, WaveStar® ADM 16/1, WaveStar® ADM 16/1 Compact, WaveStar® ADM4/1 network elements.

Table 6-15 Connection level/trail types supported by WaveStar® DACS and WaveStar® ADM network elements.

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

Table 6-15 Connection level/trail types supported by WaveStar® DACS and WaveStar® ADM network elements. (continued)

CKT/DL Connection	Description	Performance monitoring Trail Types	WaveStar® DACS	WaveStar® ADM 16/1	WaveStar® ADM 16/1 Compact	WaveStar® ADM 4/1
1920N	**CEPT-4 CKT**	**P4**	No	No	No	No
30N	**VC12S-30N Combo**	**VC12** **TU12**	No No	Yes No	No No	Yes No
480N	**VC3S-480n Combo**	**VC3** **TU3**	No	No	No	Yes
672N	**VC3S-672N Combo (DS3)**	**VC3** **TU3**	No	Yes	No	Yes
1920N	**VC4S-1920N Combo**	**VC4** **AU4**	No	Yes	No	No
DS3	**DS3 CKT**	**D3**	No	No	No	No
VC4-4c	**VC4-4c CKT**	**VC4-4c**	Yes	No	No	No
VC4-16c	**VC4-16c CKT**	**VC4-16c**	No	No	No	No
AU3S	**AU3 CKT**	**AU3**	No	No	No	No
OMS	**OMS CKT**	**OMS**	No	No	No	No
OChTrail	**OChTrail CKT**	**OCH**	No	No	No	No
OL	**OL CKT**	**OL**	No	No	No	No

Connection level/trail types: LXC 16/1, WaveStar® AM 1/TM 1, WaveStar® BandWidth Manager, WaveStar TDM 2.5/10G, and WaveStar® OLS 1.6T

Connection level/trail types

The following table shows the connection level/trail types supported by the LXC 16/1, WaveStar® AM 1/TM 1, WaveStar® BandWidth Manager, WaveStar TDM 2.5/10G, and WaveStar® OLS 1.6T network elements.

Table 6-16 Connection level/trail types supported by the LXC 16/1, WaveStar® AM 1/TM 1, WaveStar® BandWidth Manager, WaveStar TDM 2.5/10G, and WaveStar® OLS 1.6T network elements

CKT/DL Connection	Description	Performance monitoring Trail Types	LXC 16/1	WaveStar® AM 1/TM 1	WaveStar® BandWidth Manager	WaveStar® TDM 2.5/10G	WaveStar® OLS1.6T
S0	**STM-0 DL**	**MS0** **RS0**	No No	No No	No No	No No	No No
S1	**STM-1 DL**	**MS1** **RS1**	Yes Yes	Yes No	Yes Yes	Yes Yes	No No
S4	**STM-4 DL**	**MS4** **RS4**	Yes Yes	No No	Yes No	Yes Yes	No No
S16	**STM-16 DL**	**MS16** **RS16**	Yes Yes	No No	Yes Yes	Yes Yes	No No
S64	**STM-64 DL**	**MS64** **RS64**	No No	No No	Yes Yes	Yes Yes	No No
AU4	**AU4**	**AU4CTP**	Yes	No	Yes	Yes	No
TU3	**TU3**	**TU3CTP**	Yes	No	No	No	No
TU2	**TU2**	**TU2CTP**	Yes	No	No	No	No
TU12	**TU12**	**TU12CTP**	Yes	No	No	No	No
E1	**CEPT-1 DL**	**P12**	No	No	No	No	No
E3	**CEPT-3 DL**	**No**	No	No	No	No	No
E4	**CEPT-4 DL**	**P4**	No	No	No	No	No
VC4S	**VC4 CKT**	**VC4**	Yes	Yes	No	No	No
VC3S	**VC3 CKT**	**VC3**	Yes	Yes	No	No	No
VC2S	**VC2 CKT**	**No**	No	No	No	No	No
VC12S	**VC12 CKT**	**VC12**	Yes	Yes	No	No	No
30N	**CEPT-1 CKT**	**P12**	No	No	No	No	No

Table 6-16 Connection level/trail types supported by the LXC 16/1, WaveStar® AM 1/TM 1, WaveStar® BandWidth Manager, WaveStar TDM 2.5/10G, and WaveStar® OLS 1.6T network elements (continued)

CKT/DL Connection	Description	Performance monitoring Trail Types	LXC 16/1	WaveStar® AM 1/TM 1	WaveStar® BandWidth Manager	WaveStar® TDM 2.5/10G	WaveStar® OLS1.6T
480N	**CEPT-3 CKT**	**No**	No	No	No	No	No
1920N	**CEPT-4 CKT**	**P4**	No	No	No	No	No
30N	**VC12S-30N Combo**	**VC12** **TU12**	Yes No	No No	No No	No No	No No
480N	**VC3S-480n Combo**	**VC3** **TU3**	Yes	No	No	No	No
672N	**VC3S-672N Combo (DS3)**	VC3 **TU3**	Yes	No	No	No	No
1920N	**VC4S-1920N Combo**	**VC4** **AU4**	Yes	No	No	No	No
DS3	**DS3 CKT**	**D3**	No	No	No	No	No
VC4-4c	**VC4-4c CKT**	**VC4-4c**	No	No	Yes	Yes	No
VC4-16c	**VC4-16c CKT**	**VC4-16c**	No	No	Yes	Yes	No
AU3S	**AU3 CKT**	**AU3**	No	No	Yes	No	No
OMS	**OMS CKT**	**OMS**	No	No	No	No	Yes
OChTrail	**OChTrail CKT**	**0CH**	No	No	No	No	Yes
OL	**OL CKT**	**OL**	No	No	No	No	Yes

Connection level/trail types: ISM, SLM, ADM 155E, and PHASE network elements

Connection level/trail types

The following table shows the connection level/trail types supported by the ISM, SLM, WaveStar® ADM155E, and PHASE network elements.

Table 6-17 Connection level/trail types supported by the ISM, SLM, WaveStar® ADM155E, and PHASE network elements

CKT/DL Connection	Description	PM Trail Types	ISM	SLM	WaveStar® ADM 155e	PHASE
S0	**STM-0 DL**	**MS0** **RS0**	No No	No No	No No	No No
S1	**STM-1 DL**	**MS1** **RS1**	Yes No	Yes No	Yes No	Yes Yes
S4	**STM-4 DL**	**MS4** **RS4**	Yes No	Yes Yes	No No	Yes Yes
S16	**STM-16 DL**	**MS16** **RS16**	No No	Yes Yes	No No	Yes Yes
S64	**STM64 DL**	**MS64** **RS64**	No No	No No	No No	No No
AU4	**AU4**	**AU4CTP**	No	No	No	Yes
TU3	**TU3**	**TU3CTP**	No	No	No	No
TU2	**TU2**	**TU2CTP**	No	No	No	No
TU12	**TU12**	**TU12CTP**	No	No	No	No
E1	**CEPT-1 DL**	**P12**	No	No	No	No
E3	**CEPT-3 DL**	**No**	No	No	No	No
E4	**CEPT-4 DL**	**P4**	No	No	No	No
VC4S	**VC4 CKT**	**VC4**	Yes	Yes	Yes	Yes
VC3S	**VC3 CKT**	**VC3**	Yes	No	Yes	Yes
VC2S	**VC2 CKT**	**No**	No	No	No	No
VC12S	**VC12 CKT**	**VC12**	Yes	No	Yes	Yes
30N	**CEPT-1 CKT**	**P12**	No	No	No	No
480N	**CEPT-3 CKT**	**No**	No	No	No	No
1920N	**CEPT-4 CKT**	**P4**	No	No	No	No

Table 6-17 Connection level/trail types supported by the ISM, SLM, WaveStar® ADM155E, and PHASE network elements (continued)

CKT/DL Connection	Description	PM Trail Types	ISM	SLM	WaveStar® ADM 155e	PHASE
30N	**VC12S-30N Combo**	**VC12** **TU12**	Yes	No	Yes	Yes
480N	**VC3S-480n Combo**	**VC3** **TU3**	Yes	No	Yes	Yes
672N	**VC3S-672N Combo**	**No**	No	No	Yes	Yes
1920N	**VC4S-1920N Combo**	**VC4** **AU4**	Yes	Yes	No	Yes
DS3	**DS3 CKT**	**DS3**	No	No	No	No
VC4-4c	**VC4-4c CKT**	**VC4-4c**	No	No	No	No
VC4-16c	**VC4-16c CKT**	**VC4-16c**	No	No	No	No
AU3S	**AU3 CKT**	**AU3**	No	No	No	No
OMS	**OMS CKT**	**OMS**	No	No	No	No
OChTrail	**OChTrail CKT**	**OChTrail**	No	No	No	No
OL	**OL CKT**	**OL**	No	No	No	No

7 Reports Management

Overview

Purpose

This chapter describes the reports that are provided by Navis™ Optical NMS.

Contents

About the reports

Introduction

Navis™ Optical NMS 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 NMS:

- 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.
- Preplan Restoration Report: (Optional) Lists the circuit orders that are restored using the preplan circuit paths.
- Preemption Report: (Optional) Lists the preempted circuits, and the correlation between the preempted circuit and the service circuit that caused the preemption.

□

Index