Lucent Technologies
Bell Labs Innovations

WaveStar™ SubNetwork Management System (SNMS)

Maintenance Guide

190-224-121
Release 4.2
Issue 1.0
December 2000

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. Information is subject to change; however, Lucent Technologies assumes no responsibility for any errors that may appear in this document.

FCC Warning Statement

This equipment generates, uses, and can radiate radio frequency energy. If not installed, used, and maintained in accordance with the instruction manual, it may cause interference to radio communications. Operation of this equipment in a residential area may cause interference, in which case users will be required to take whatever measures may be required to correct the interference at their own expense.

Trademarks

WaveStar is a trademark of Lucent Technologies.
INFORMIX is a registered trademark of Informix Software, Inc.
Lantronix is a registered trademark of Lantronix.
Microsoft is a registered trademark and Windows is a trademark of Microsoft Corporation.
Hewlett-Packard, HP, and HP-UX are registered trademarks of Hewlett-Packard.
Pentium is a registered trademark of Intel Corporation.
UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Warranty

Lucent Technologies provides a limited warranty for this product. For more information, consult your local Account Representative.

Customer Assistance or Technical Support

You may call the toll-free hotline at 1-800-225-4672 for customer assistance and troubleshooting 24 hours a day. See your Lucent Technologies account representative for further details.

In the continental United States, when you need additional technical assistance, the Lucent Technologies Regional Technical Assistance Center (RTAC) is your first point of contact. RTAC engineers are highly trained and skilled at resolving issues involving Lucent Technologies products. Technical assistance is available 24 hours a day, 7 days a week. Contact the RTAC at 1-800-225-RTAC (7822).

Outside the continental United States, contact your Local Customer Support (LCS) or the support organization designated by your Lucent customer team representative.

Ordering Information

The ordering number for this document is 190-224-121.

To order this document within the continental United States, call 1-888-582-3688 (1-888-LUCENT8).

To order this document outside the continental United States, call your Lucent customer team representative.

Lucent Technologies values your comments!

Lucent Technologies
Bell Labs Innovations

WaveStar SubNetwork Management System WaveStar SNMS Maintenance Guide Release 4.2

190-224-121 1.0 Date: December 2000

Lucent Technologies welcomes your comments on this information product. Your opinion is of great value and helps us to improve.

1. Was the information product:

	Yes	*No*	*Not applicable*
In the language of your choice?	☐	☐	☐
In the desired media (paper, CD-ROM, etc.)?	☐	☐	☐
Available when you needed it?	☐	☐	☐

Please provide any additional comments:

_____

_____

2. Please rate the effectiveness of this information product:

	Excellent	*More than satisfactory*	*Satisfactory*	*Less than satisfactory*	*Unsatisfactory*	*Not applicable*
Ease of use	☐	☐	☐	☐	☐	☐
Level of detail	☐	☐	☐	☐	☐	☐
Readability and clarity	☐	☐	☐	☐	☐	☐
Organization	☐	☐	☐	☐	☐	☐
Completeness	☐	☐	☐	☐	☐	☐
Technical accuracy	☐	☐	☐	☐	☐	☐
Quality of translation	☐	☐	☐	☐	☐	☐
Appearance	☐	☐	☐	☐	☐	☐

If your response to any of the above questions is "*Less than satisfactory*" or "*Unsatisfactory,*" please explain your rating.

_____

_____

3. If you could change one thing about this information product, what would it be?

_____

_____

4. Please write any other comments about this information product:

_____

_____

Please complete the following if we may contact you for clarification or to address your concerns:

Name: _____ Date: _____

Company/organization: _____ Telephone number: _____

Address: _____

Email address: _____ Job function: _____

If you choose to complete this form online, go to http://www.lucent-info.com/comments
Otherwise fax to 407 767 2760 (U.S.) or +1 407 767 2760 (outside the U.S.) or email comments to ctiphotline@lucent.com

Contents

About This Information Product

Introduction

Summary

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

Contents

This chapter discusses the following topics:

Purpose of This Information Product

Purpose

The purpose of this Maintenance Guide is to instruct users how to maintain network elements managed by the WaveStar™ Subnetwork Management System (SNMS). It provides users with the information and procedures necessary to:

- Retrieve, report, and log alarms and events generated by WaveStar SNMS and managed network elements
- Acknowledge alarms and events occurring in the managed network
- Collect and view performance monitoring (PM) data from network elements

Intended audience

This guide is written primarily for operations personnel who will be using WaveStar SNMS to maintain NE subnetworks and NE equipment.

Reason for issue

This Maintenance Guide, Issue 1.0, is a new document that supports WaveStar SNMS, Release 4.2.

Using this Information Product

Introduction

This section provides information to assist users of this information product.

Conventions used

Menu and submenu selections from the WaveStar SNMS Map window are shown in **boldface type**.

The terms “choose” and “select” are used interchangeably throughout this Guide. Both terms represent the following operations:

- Activating a button, such as OK, Cancel, or Help
- Activating a menu, such as a pull-down menu on the menu bar
- Selecting an item from a menu
- Selecting an NE/aggregate symbol on the Map window
- Selecting an item from a scroll list
- Moving window focus to a fext field to type an entry in the field

How this Guide is organized

The following table describes the structure and content of each chapter in this Guide.

Section	Title	Description
Preface	About This Information Product	Describes this document’s purpose and intended audience, how to use the document, and how to comment on it
Chapter 1	Alarm Management	Describes tasks performed to manage alarms and transient condition (TC) events generated by WaveStar SNMS and the network elements it manages
Chapter 2	Performance Management	Describes tasks performed to collect and view performance monitoring (PM) data for network elements managed by WaveStar SNMS
Chapter 3	System Introduction	Provides a general introduction to WaveStar SNMS and its functions/ features

Section	Title	Description
Chapter 4	Alarm Management Concepts	Describes the monitoring alarms and conditions in a subnetwork of network elements managed by WaveStar SNMS. It also provides general information about the Log Management features provided by WaveStar SNMS for displaying and viewing alarm data, NE commands/ responses, and other messages generated by WaveStar SNMS and managed network elements
Chapter 5	Performance Management Concepts	Describes the Performance Management features of WaveStar SNMS
Chapter 6	Glossary	Provides a glossary of terms and a list of acronyms

Related Documents

Introduction

This information product is part of a set of documents that supports WaveStar SNMS.

List of documents

The document set that supports WaveStar SNMS includes:

- *WaveStar SNMS Maintenance Guide*—this document instructs users on how to maintain network elements managed by WaveStar SNMS
- *WaveStar SNMS Administration Guide*—this document instructs users on how to administer WaveStar SNMS and the managed network elements
- *WaveStar SNMS Provisioning Guide*—this document instructs users how to use WaveStar SNMS to provision the managed network elements
- *WaveStar SNMS Installation Guide*—this document instructs system administrators and other operations personnel how to install WaveStar SNMS

On-line documentation

Online versions of the document set listed above are available through the Help feature in the WaveStar Graphical User Interface (GUI).

On-line help

The WaveStar SNMS software includes on-line help for each window with a Help button. Each window has an associated help screen that describes the purpose of the window, basic window navigation, field descriptions, and button functions.

How to Comment on Information Products

Introduction

Customer satisfaction is extremely important to Lucent Technologies. All users are encouraged to provide feedback on WaveStar SNMS information products.

Customer comment form

A customer comment form appears immediately after the title page of this document. Please fill out the form and fax it to the number provided on the form.

How to Order Information Products

Methods

To order WaveStar SNMS information products:

- Contact your Lucent Technologies customer team representative
- Contact the Lucent Technologies Customer Information Center (CIC):
  - — From the United States, call 1-888-LUCENT8, prompt 1
  - — From Canada, call 1-317-322-6619
  - — From Europe, the Middle East, and Africa, call 1-317-322-6416
  - — From Asia, the Pacific Region, China, the Caribbean, and Latin America, call 1-317-322-6411

Alarm Management

1

Introduction

Summary

This chapter describes procedures for managing alarms and transient condition (TC) events generated by WaveStar SNMS and the network elements it manages.

Before you begin

Read the Alarm Management Concepts chapter to acquire an understanding of the Fault Managment and Log Management functions provided by WaveStar SNMS.

Contents

This chapter discusses the following topics:

Activate the Alarm Browser

Background

Use this procedure to activate the alarm browser. This allows you to capture alarm, event, and clear messages that are forwarded to network surveillance OSs for NEs in your Target Group, and displays them in the Log Browser window on your workstation screen.

Task

Complete the following steps to activate the alarm browser.

Step	Action
1	Select **Fault** from the main menu bar on the Map window. This displays a pull-down menu.
2	From the pull-down menu, select **Alarm Browser**. This displays the Log Browser window.
3	To save the output from this window to a file, do the following, a. Click on **File** on the menu bar on the Log Browser window and then select **Save As**. A pop-up window is displayed. b. Select the PC drive where the file folder resides in which to store the file output by clicking the down arrow next to the “Look In” field on the window. Select the drive. c. Select and open the file folder for the saved output file by double-clicking on the folder in the scrollable list on the pop-up window. d. Type a name for the output file in the File name field. e. Click the Save button. The output is saved to the named file. **NOTE:** To view the saved output file, use the Wordpad application.
4	When you are finished viewing the log information, access the **File** pull-down menu from the menu bar and select **Close**. **Stop! End of Task.**

Access the Alarm Summary

Background

Use this procedure to access the Alarm Summary window, which contains NE/ aggregate alarm summary information, as well as Trail Alarm summary information. This summary information includes the number of critical, major, and minor alarms for each NE and trail.

Before you begin

Before you begin this task, make sure that you have identified the NE or trail for which you want to obtain alarm information.

Task

Complete the following steps to access the Alarm Summary.

Step	Action
1	Select an NE on the Map pane on the Map window to see an alarm summary for a specific NE. **OR** Select no NEs at this point to see an alarm summary for all NEs in your Target Group.
2	Select **Fault** from the main menu bar on the Map window. This displays a sub-menu.
3	From the sub-menu, select **Alarm Summary**. This displays the Alarm Summary window. The Alarm Summary window contains two sections - the NE/Aggregate Alarm Summary table and the Trail Alarm Summary table. **NE/Aggregate Alarm Summary Table —** Each line in this table provides, for the listed TID, a color code indicating the highest severity alarm for the NE/aggregate, as well as a count of the Critical, Major, and Minor alarms for SONET or Prompt and Deferred alarms for SDH, and count of Standing Condition (SC) events (shown under the “NA” category) for the NE/aggregate. For the NEs listed, you can initiate cut-throughs, access the Alarm List, define the level of alarms to be monitored/displayed, provision the NE system parameters and port,and display equipment. To access these tasks, point to an NE’s summary line with the mouse, click the left mouse button to select it, and then click the menu mouse button. A pop-up menu appears, from which you can select the desired operation. **NOTE:** For specific information about an operation (such as provisioning NE ports), look up the related task in the Task Index. **Trail Alarm Summary Table —** This table lists a count of critical, major, and minor alarms for the AIDs that terminate the trail between two NEs. A color code indicates the highest severity alarm for the trail.
4	When you are finished viewing the alarm summary information, access the **File** pull-down menu from the menu bar and select **Close**. **Stop! End of Task.**

Access the Alarm List

Background

Use this procedure to access the alarm list, which contains a line of information about each active alarm or standing condition (SC) event in an NE or aggregate. An SC event requires a clear command from the NE to indicate that the condition no longer exists. You can sort the list by alarm severity and age, age alone, condition, data/time logged, or acknowledged vs. unacknowledged. You can also use the list to acknowledge and unacknowledge alarms (see Related information below).

Task

Complete the following steps to access the alarm list.

Step	Action
1	Position the mouse pointer over the NE or aggregate for which you want a list of alarms and press the menu (right) mouse button. A sub-menu appears.
2	Select **Alarm List** from the sub-menu. The Alarm List window is displayed. You can also access the Alarm List for a selected piece of equipment on the Equipment View window by selecting the equipment in the Equipment View explorer and clicking the right mouse button to display a pop-up menu. Choose **Alarm List** from the pop-up menu. Or, position the mouse cursor on the graphical representation of the piece of equipment in the Equipment View window and click the right mouse button to display a pop-up menu and choose **Alarm List**. The Alarm List window is displayed. The Alarm List window can also be displayed from the Alarm Summary window by positioning the mouse cursor on the NE's TID on the Alarm Summary window, single-clicking the left mouse button to select the NE/TID, right-clicking the menu mouse button to display a pop-up menu, and the chooseing **Alarm List** from the pop-up menu.)

Step	Action (Contd)	
3	On the Alarm List window, each row on the window represents an alarm in the selected NE. The default sort order is occurrence date and time. TO.... Change the sort order	DO THIS... Click on the column head of the desired sort item. Choose **View** from the menu bar on the Alarm List window, A sub-menu is displayed. Choose **Sort** from the sub-menu. The Sort window is displayed. Select the sort criteria for each level of sort by clicking the down arrow next to each field to display a drop-down list, and then select the field on which to sort, and then choose to sort by the selected field in either Ascending or Descending order. *Continued on next page*

Step	Action (Contd)	
4	TO... Filter the Alarm List	DO THIS... Choose **View** from the menu bar on the Alarm List. A sub-menu is displayed. Choose **Filter Alarms** from the sub-menu. A Filter Alarm window is displayed. Select the criteria for filtering (limiting) the Alarm List. The criteria is: • Check Service Affecting (SA) or Non Service Affecting (NSA) • Modifier: choose All (alarms) or a Modifier. If you choose Modifier, click the Signal Level Affected (SLA) button. A secondary window pops up. Move the SLA categories to the Chosen SLAs list and click the OK button. The Alarm List Filter window is displayed again. • Choose the Alarm Severity Level (All, Critical, Major, Minor, Not Alarmed) • Choose the status: All, Acknowledged, Unacknowleged When you have your choices, click the OK button. To ignore the selections, click the Cancel or Close button. *Continued on next page*

Step	Action (Contd)
You can also filter acknowledged alarms for the list in another way. Choose **View from the menu toolbar. A sub-menu is displayed. Choose Filter Acknowledged Alarms** from the sub-menu. Another sub-menu is displayed. Choose Show All, Acknowledged Only, or Unacknowledged Only.	
The Alarm List window provides the following data for each alarm for the selected NE: • Color—a color code associated with the alarm severity • Alarm ID—an identifying code for the alarm • TID—the TID of the NE that originated the message or target TID that receives a command. • AID—the Access Identifier, or address, of the equipment component or facility. If this is part of an SLC NBS (Narrow Band Shelf), an asterisk (*) appears. • Ack—the user ID of the user that acknowledged the alarm • Severity—Critical, Major, or Minor • SA/NSA—whether the problem is service affecting (SA) or non-service affecting (NSA) • Date/Time of OCC—the date/time the alarm occurred • Date/Time of Log DateTime—the date/time the alarm was logged by the EMS • Condition—a message that indicates the type of failure or status condition • SLA—the Signal Level Affected (category) • Probable Cause—the condition type (code) indicating the probable cause of failure **NOTE:** To display details about a specific alarm or event shown in the Alarm list, position the mouse button on the alarm listing for which you want additional details, and double click the select mouse button. This displays the Alarm Text window, containing specific information about the alarm or event. *Continued on next page*	

Step	Action (Contd)
5	To save the output from this window to a file, do the following, a. Choose **File** on the menu bar on the Alarm List window and then select **Save As**. A pop-up window is displayed. b. Select the PC drive where the file folder resides in which to store the file output by clicking the down arrow next to the "Look In" field on the window. Select the drive. c. Select and open the file folder for the saved output file by double-clicking on the folder in the scrollable list on the pop-up window. d. Type a name for the output file in the File name field. e. Click the Save button. The output is saved to the named file. **NOTE:** To view the saved output file, use the Wordpad application.
6	To print a copy of the Alarm List obtained, choose **File** on the Alarm List window menu bar and use the following options: • **Print Setup** - choose this option from the File sub-menu to choose which field from the Alarm List to print. Click the Landscape or Portrait radio button to print the list in landscape or portrait mode. Use the arrow push buttons to move fields from the total list of fields from the left display column to the "Chosen Fields" display column on the right side of the window. Move fields back and forth between columns as necessary. When you have made your selections, click the OK button. Click the Cancel button to cancel the print setup operation and exit the window. • **Print Preview** - choose this option from the File sub-menu to preview what the Alarm List will look like when printed. If there are no alarms listed, a message is displayed. After you have finished previewing the output online, choose **File** from the Print Preview window menu bar and then choose **Close** to close the window. • **Print** - choose this option to print the Alarm List. When you choose this option, a pop-up Print window is displayed, allowing you to select the printer, number of copies, and other parameters for printing. When you have made your selections on the pop-up Print window, click the OK button and the copy(ies) are printed to the selected printer destination. If there are no alarms on the Alarm List, a message is displayed. *Continued on next page*

Step	Action (Contd)
7	When you are finished viewing the alarm list information, access the **File** pull-down menu from the menu bar and select **Close**. **Stop! End of Task.**

Acknowledge/Unacknowledge Alarms

Background

Use this procedure to acknowledge or unacknowledge single alarms, one at a time.

Before you begin

Before you begin this task, determine the alarm(s) to be acknowledged or unacknowledged.

Task

Complete the following steps to acknowledge or unacknowledge single alarms, one at a time.

Step	Action
1	Position the mouse pointer over the NE or aggregate for which you want a list of alarms and press the menu (right) mouse button. A sub-menu appears. *Continued on next page*

Step	Action (Contd)
2	Select **Alarm List** from the sub-menu. The Alarm List window is displayed. You can also access the Alarm List for a selected piece of equipment on the Equipment View window by selecting the equipment in the Equipment View explorer and clicking the right mouse button to display a pop-up menu. Choose **Alarm List** from the pop-up menu. Or, position the mouse cursor on the graphical representation of the piece of equipment in the Equipment View window and click the right mouse button to display a pop-up menu and choose **Alarm List**. The Alarm List window is displayed. The Alarm List window can also be displayed from the Alarm Summary window by positioning the mouse cursor on the NE's TID on the Alarm Summary window, single-clicking the left mouse button to select the NE/TID, right-clicking the menu mouse button to display a pop-up menu, and the chooseing **Alarm List** from the pop-up menu.)
3	Select Fault from the menu bar near the top of the Alarm List window. This displays a sub-menu.
4	Select **Acknowledge Selected** or **Unacknowledge Selected** from the displayed sub-menu, as appropriate. (If you wish to acknowledge or unacknowledge *all* the alarms in the list, select **Acknowledge All in List** or **Unacknowledge All in List**, as appropriate.) **NOTE:** If an alarm is not yet acknowledged, there is no entry in the Ack field on that line. If it is already acknowledged, the Ack field contains the acknowledger's userid. **Stop! End of Task.**

Acknowledge/Unacknowledge Alarm Groups

Background Use this procedure to select and then acknowledge or unacknowledge a group of alarms.

Before you begin Before you begin this task, determine the alarms to be acknowledged or unacknowledged.

Task Complete the following steps to select and then acknowledge or unacknowledge a group of alarms.

Step	Action
1	Position the mouse pointer over the NE or aggregate for which you want a list of alarms and press the menu (right) mouse button. A sub-menu appears.
2	Select **Alarm List** from the sub-menu. The Alarm List window is displayed. You can also access the Alarm List for a selected piece of equipment on the Equipment View window by selecting the equipment in the Equipment View explorer and clicking the right mouse button to display a pop-up menu. Choose **Alarm List** from the pop-up menu. Or, position the mouse cursor on the graphical representation of the piece of equipment in the Equipment View window and click the right mouse button to display a pop-up menu and choose **Alarm List**. The Alarm List window is displayed. The Alarm List window can also be displayed from the Alarm Summary window by positioning the mouse cursor on the NE's TID on the Alarm Summary window, single-clicking the left mouse button to select the NE/TID, right-clicking the menu mouse button to display a pop-up menu, and the chooseing **Alarm List** from the pop-up menu.)
3	Using the mouse, select each row that contains an alarm you want to include in the group to be acknowledged or unacknowledged. To select multiple continuous rows, hold the Contro key down and drag the mouse pointer over the desired lines. To select multiple non-continuous lines, hold the Shift or Control key down and right click each line to be included. (Unacknowledged alarms contain no entry on their rows in the **Ack** column. Acknowledged alarms contain, in the **Ack** column, the login ID of the person who acknowledged the alarm.) Select as many rows of acknowledged or unacknowledged alarms as desired.
4	Select **Fault** from the menu bar at the top of the Alarm List window. This displays a sub-menu.
5	Choose **Acknowledge Selected** or **Unacknowledge Selected**, as appropriate. (Or to acknowledge or unacknowledge *all* alarms in the list [without having to choose individual alarms], select **Acknowledge All in List** or **Unacknowledge All in List**, as appropriate.) **Stop! End of Task.**

Acknowledge/Unacknowledge All Alarms

Background

Use this procedure to acknowledge all unacknowledged alarms on the Alarm List window or to unacknowledge all acknowledged alarms on the Alarm List window.

Before you begin

Before you begin this task, you should make certain that you do want to acknowledge or unacknowledge these alarms.

Task

Complete the following steps to acknowledge or unacknowledge all alarms.

Step	Action
1	Position the mouse pointer over the NE or aggregate for which you want a list of alarms and press the menu (right) mouse button. **Result:** A sub-menu appears. *Continued on next page*

Step	Action (Contd)
2	Select **Alarm List** from the sub-menu. The Alarm List window is displayed. You can also access the Alarm List for a selected piece of equipment on the Equipment View window by selecting the equipment in the Equipment View explorer and clicking the right mouse button to display a pop-up menu. Choose **Alarm List** from the pop-up menu. Or, position the mouse cursor on the graphical representation of the piece of equipment in the Equipment View window and click the right mouse button to display a pop-up menu and choose **Alarm List**. The Alarm List window is displayed. The Alarm List window can also be displayed from the Alarm Summary window by positioning the mouse cursor on the NE's TID on the Alarm Summary window, single-clicking the left mouse button to select the NE/TID, right-clicking the menu mouse button to display a pop-up menu, and the chooseing **Alarm List** from the pop-up menu.)
3	Select **Fault** from the menu bar at the top of the Alarm List window. This displays a sub-menu.
4	From the sub-menu, choose **Acknowledge All in List** (to acknowledge all unacknowledged alarms in the Alarm List window) or **Unacknowledge All in List** (to unacknowledge all acknowledged alarms in the Alarm List window), as appropriate. (Unacknowledged alarms contain no entry in the Ack field on their rows. Acknowledged alarms contain, in the Ack field, the userid of the alarm acknowledger.) **Stop! End of Task.**

Acknowledge/Unacknowledge All Alarms for an NE

Background

Use this procedure to acknowledge or unacknowledge all alarms for a selected NE or aggregate.

Before you begin

Before you begin this task, you should make certain that you do want to acknowledge or unacknowledge these alarms.

Task

Complete the following steps to acknowledge or unacknowledge all alarms for a selected NE or aggregate.

Step	Action
1	On the Map pane portion of the Map window, use the mouse to select the NE or aggregate for which you want to acknowledge all unacknowledge alarms or unacknowledge all acknowledged alarms. **OR** Select no NE at this point.
2	Select **Fault** from the main menu bar at the top of the Map window. This displays a sub-menu.
3	Select **Alarm Acknowledgement** from the displayed sub-menu. This displays another sub-menu containing the choices **Acknowledge** and **Unacknowledge**.
4	From the displayed sub-menu, select **Acknowledge** to acknowledge all unacknowledged alarms for an NE, or **Unacknowledge** to unacknowledge all acknowledged alarms for an NE. If you did not choose an NE in step 1, the Choose an NE/Aggregate window is displayed. To obtain a listing of just NEs, click the Network Elements radio button. To obtain a listing of aggregates, click the Aggregates button. Double-click the on the item in the list (network element or aggregate) and click the OK button. Alarms are acknowledged or unacknowledged for the selected NE or aggregate or NEs. **Stop! End of Task.**

Monitor Alarms

Background

Use this procedure to limit the amount of autonomous messages and Critical autonomous messages that should be monitored for an NE. See the Related Information below for more information about alarm monitoring.

Before you begin

Before you begin this task, determine what type of alarm monitoring you want to establish for the NE.

Task

Complete the following steps to monitor alarms.

Step	Action	
1	Select an NE in the Map pane portion of the Map window **OR** Select no NE at this point.	
2	IF... You selected an NE in step 1 You did not select an NE in step 1.	THEN... Click the right (menu) mouse button. A pop-up menu is displayed. Select **Alarm Monitoring** from the pop-up menu. A sub-menu is displayed. Select **Fault** from the main menu bar on the Map window. The Fault menu is displayed. Select **Alarm Monitoring** from the Fault menu. A sub-menu is displayed.
3	Choose one of the following options from the displayed sub-menu: • **All Messages**—This option allows all autonomous messages to be accepted from the NE. If the NE's alarms are currently being throttled, choose this option to put the NE back into an unthrottled alarm state. • **Throttled**—This option allows only Critical messages to be accepted from the NE, even if the alarm throttle level set in the Administer NE menu has not been reached or if automatic alarm throttling is displayed. If you did not select an NE in Step 1, the Choose an NE/Aggregate window is displayed. Click the Network Elements radio button to limit the list to NEs. Click the Aggregates radio button to limit the list to aggregates. Double-click on the item (NE or aggregate) in the Choose an NE/Aggegate window to select it and click the OK button. A message is sent to the NE by the system to change the alarm status on the NE. After the change is received by the NE, the Alarm monitoring status of the NE is displayed on the Map pane portion of the Map window. If **Throttled** is selected, the NE icon changes back and forth from grey to the color of the highest severity alarm. If **All Messages** is selected, the NE icon displays only the color of the highest severity alarm. **Stop! End of Task.**	

View Throttled Alarm Statistics

Background

Use this procedure to view throttled alarm statistics for an NE. This window indicates the time of the last alarm message received.

Before you begin

Before you begin this task, determine the NE for which you want to view the throttled alarm statistics.

Task

Complete the following steps to view throttled alarm statistics for NEs.

Step	Action
1	Select an NE on the Map pane portion of the Map window. **OR** Select no NE at this point.
2	Select **Fault** from the main menu bar on the Map window. This displays a sub-menu.
3	Select **Alarm Monitoring** from the displayed sub-menu. This displays another sub-menu.
4	Select **Statistics** from the displayed sub-menu. If you did select an NE in step 1, the Choose an NE/Aggregate window is displayed. To obtain a list of NEs on this window, click the Network Elements radio button To obtain a list of aggregates on this window, click the Aggregates radio button. For this function, click the Network Elements radio button to list NEs. Double-click on the NE in this list to select it and click the OK button. A pop-up window is displayed, showing the number of autonomous messages and alarms that have been generated for the selected NE since the time and date of the last reporting interval. Click the OK button on the pop-up window to close it. **Stop! End of Task.**

Resynchronize Alarms

Background

Whenever any loss of NE communications occurs, use this procedure to update the alarm list and autonomous message log from the network elements in the subnetwork. The system automatically resynchronizes alarms whenever the communications status with an NE changes from *down* to *up*, but this procedure allows you to perform this function any other time, as desired.

NOTE:
Alarm resynchronization does not work unless the NE is in an unthrottled state. Before resynchronizing alarms for an NE, the user should disable the automatic/manual alarm throttling control for the NE.

The alarm resynchronization process does not clear the existing GUI display and alarm tally/list during the resynchronization process, but rather retains the existing alarms until the resynchronization is complete. The system can distinguish between:

- standard alarms that already exist in the GUI and alarm/tally list displays
- new alarms, and
- alarms that are cleared by the NE between resynchronizations.

This allows the system to incrementally update the GUI display and alarm tally/list to accurately indicate the subnetwork status to the user.

Before you begin

Before you begin this task, be aware that alarms cannot be resynchronized on non-communicating NEs.

Task

Complete the following steps to resynchronize alarms on demand.

Step	Action
1	Position the mouse cursor on the NE and click the right (menu) mouse button. A pop-up menu is displayed. **OR** Select no NE at this point.
2	If you selected an NE, click the right mouse button. A pop-up menu is displayed. Select **Resynchronize Alarms** from the pop-up menu. If you did not select an NE on the Map window in step 1, choose **Fault** from the main menu bar on the Map window. The Fault sub-menu is displayed. Choose **Resynchronize Alarms** from the Fault sub-menu. The Choose an NE/Aggregate window is displayed. Click the Network Elements radio button on this window to list NEs. Click the Aggregates radio button on this window to list aggregates. Double-click on the item in the list (network element or aggregate) to select it and click the OK button. The system resynchronizes the alarms for the selected NE/aggregate. **Stop! End of Task.**

Enable/Disable Audible Alarms

Background

Use this procedure to enable and disable the audible alarm feature.

Before you begin

Before you begin this task, be sure that you do want to change the current status of the audible alarm feature.

Turn up the volume on your PC's audio control if you decide to enable the Audible Alarms feature to clearly hear audible alarms or standing condition (SC) events.

Task

Complete the following steps to enable or disable the audible alarm feature.

Step	Action
1	On the Map window, select **Fault** from the main menu bar. This displays a sub-menu.
2	Select **Audible Alarms** from the displayed sub-menu. This displays another sub-menu. • If the audible alarm feature is currently enabled, a mark appears next to the Audible menu item on the displayed sub-menu. If desired, click on Audible to disable audible alarms. • If the audible alarm feature is currently disabled, the mark does *not* appear next to the Audible menu item on the displayed sub-menu. If desired, click on Audible to enable audible alarms. **NOTE:** Another way to enable or disable the Audible Alarm feature is to click on the Audible Alarms button on the Map window toolbar. If the Audible Alarms feature is currently enabled, clicking on it until a red slash appears across this button disables the Audible Alarms feature. Clicking on it again enables the Audible Alarms feature. **Stop! End of Task.**

Quiet the Audible Alarm

Background

Use this procedure to quiet the audible alarm when it is sounding. When the audible alarm is enabled and an alarm occurs, it sounds for a short duration (about five seconds) and repeats every minute. Each time the audible alarm sounds, the sound corresponds to the highest level alarm received. Once the user quiets the alarm, it does not sound again until another alarm is received.

Before you begin

Before you begin this task, be sure that you do want to quiet the audible alarm and that you have noted the latest alarms.

Task

Complete the following steps to quiet the audible alarm.

Step	Action
1	On the Map window, select **Fault** from the main menu bar. This displays a sub-menu.
2	Select **Audible Alarms** from the displayed sub-menu. This displays another sub-menu.
3	Select **Quiet Current Alarms** from the displayed sub-menu. The system quiets the current alarms and does not audibly signal alarms until a new alarm arrives. (The alarms still need to be acknowledged.) **Stop! End of Task.**

Enable/Disable the Alarm Indicator

Background

Use this procedure to enable or disable the system's alarm indicator function. Disabling the alarm indicator causes nodes and aggregates not to flash when alarms are received. Enabling alarm indicators turns this function back on.

Before you begin

Before you begin this task, make sure you do want to enable or disable the alarm indicator function, as appropriate.

Be aware that disabling the alarm indicator function stops alarmed nodes and aggregates from flashing, but it does *not* acknowledge alarms.

Task

Complete the following steps to enable or disable the alarm indicator function for all NEs.

Step	Action
1	On the Map window, select **View** from the main menu bar. This displays a sub-menu.
2	Select **Alarm Indications** from the displayed sub-menu. This displays another sub-menu.
3	On the displayed sub-menu, there will be a bullet mark next to either **All Enabled** or **All Disabled**. The one with the bullet is the current state. You can change the state by clicking with your mouse pointer. For example, if the bullet is currently next to **All Enabled** and you want to disable the alarm indicator function, click **All Disabled**. The system moves the bullet and makes the change to the feature. **Stop! End of Task.**

View an ASAP

Background

Use this procedure to view an existing Alarm Severity Assignment Profile (ASAP) for a Profile Type in an NE.

Before you begin

Before you begin this task, access the Map window.

Task

Complete the following steps to view an existing ASAP.

Step	Action
1	Select an NE from the Map window. **OR** Select no NEs at this point.
2	Select **Fault** from the main menu bar on the Map window. The Fault menu is displayed.
3	Select **Alarm Severity Assignment Profiles** from the Fault menu. If you did not select an NE in Step 1, the Choose an NE/Alarm Severity Profiles is displayed. Select an NE by double-clicking on the item and click the OK button. The Alarm Severity Assignment Profile Management window is displayed. This window consists of an explorer, which allows you to view and select the Profile Type under the selected NE, and six action buttons to the right of the explorer: • Add • Modify • Delete • View • Assignments • Rename
4	Click on the plus (+) sign next to the NE TID in the explorer to expand and view the Profile Types for that NE.

Step	Action (Contd)
5	Click on the plus (+) sign next to the Profile Type in the explorer to expand and view the Profile Names under that Profile Type.
6	Choose a Profile Name under a Profile Type. The chosen Profile Name is highlighted.
7	Click on the View button. The View an Alarm Severity Assignment Profile window is displayed, showing the probable causes (alarm states) for the selected Profile Type and the current alarm severity levels for each probable cause. **Stop! End of Task.**

Add an ASAP

Background

Use this procedure to add a new Alarm Severity Assignment Profile (ASAP) for a Profile Type in the chosen NE. To add a new ASAP, the alarm severity settings of the default ASAP for the selected Profile Type are copied over to a new Profile Name. The newly created ASAP will have the same alarm severity settings as the default ASAP unless they are changed. Once it is created, the new ASAP, which is identified by its Profile Name, can be assigned to an entity (AID) in the NE.

Before you begin

Before you begin this task, be aware that WaveStar SNMS will prevent you from adding a new ASAP for a Profile Type if the maximum number of allowable ASAPs for that Profile Type in the NE has been exceeded.

Be aware that if you want to see the ASAP alarm severity levels in SDH format, you must change the Fault settings to SDH format using the Preferences option. See the Modify User Preferences task in the *WaveStar SNMS Provisioning Guide* for instructions on how to modify the alarm severity level display to SDH format using the Preferences option in the GUI.

Refer to the TL1 documentation for the *ED-ASAP-PROF* command for the allowed alarm severity levels for each condition type.

Task

Complete the following steps to add a new ASAP.

Step	Action
1	Select an NE from the Map window. **OR** Select no NEs at this point.
2	Select **Fault** from the main menu bar on the Map window. The Fault menu is displayed.
3	Select **Alarm Severity Assignment Profiles** from the Fault menu. If you did not select an NE in Step 1, the Choose an NE/Alarm Severity Profiles is displayed. Select an NE by double-clicking on the item and click the OK button. The Alarm Severity Assignment Profile Management window is displayed. This window consists of an explorer, which allows you to view and select the Profile Type under the selected NE, and six action buttons to the right of the explorer: • Add • Modify • Delete • View • Assignments • Rename
4	Click on the Add button. The Add an Alarm Severity Assignment Profile window is displayed.
5	To create an ASAP for a Profile Type, click the down arrow next to the Profile Type field and select a Profile Type.

Continued on next page

Step	Action (Contd)
6	Enter a name for the new ASAP in the Profile Name field. The Profile Name can be 1-24 characters (A-Z, a-z, 0-9,). **NOTE:** The Profile Name entered becomes the suffix of the complete profile name; the system adds a prefix based on the Profile Type chosen (OLS 400G only).
7	If desired, make changes to the alarm severity level settings for the new ASAP. To change a alarm severity level for a probable cause, click the appopriate radio button. For example, if the current alarm severity level is CR (for Critical), and you want to change it to MJ (Major), click the MJ radio button in the row for the probable cause.
8	Click the Apply button activate your choices, or click the OK button to activate your choices and close the window. The new ASAP is created. **Stop! End of Task.**

Modify an ASAP

Background

Use this procedure to modify an existing Alarm Severity Assignment Profile (ASAP) for a Profile Type.

Before you begin

Before you begin this task, access the Map window.

Refer to the TL1 documentation for the *ED-ASAP-PROF* command for the allowed alarm severity levels for each condition type.

Task

Complete the following steps to modify an existing profile.

Step	Action
1	Select an NE from the Map window. **OR** Select no NEs at this point.
2	Select **Fault** from the main menu bar on the Map window. The Fault menu is displayed.
3	Select **Alarm Severity Assignment Profiles** from the Fault menu. If you did not select an NE in Step 1, the Choose an NE/Alarm Severity Profiles is displayed. Select an NE by double-clicking on the item and click the OK button. The Alarm Severity Assignment Profile Management window is displayed. This window consists of an explorer, which allows you to view and select the Profile Type under the selected NE, and five action buttons to the right of the explorer: • Add • Modify • Delete • View • Assignments • Rename
4	Click on the plus (+) sign next to the NE TID in the explorer to expand and view the Profile Types for that NE. *Continued on next page*

Step	Action (Contd)
5	Click on the plus (+) sign next to the Profile Type in the explorer to expand it.
6	Choose a Profile Name for the profile to be modified. The Profile name is highlighted.
7	Click on the Modify button. The Modify an Alarm Severity Assignment Profile window is displayed, showing the the current alarm severity levels for each probable cause in the selected Profile Type and Profile Name.
8	Make changes to the alarm severity level(s) for the probable cause(s), as needed. To change a alarm severity level for a probable cause, click the appropriate radio button. For example, if the current alarm severity level is CR (for Critical), and you want to change it to MJ (Major), click the MJ radio button in the row for the probable cause.
9	Click the OK button. The changes are made to the selected ASAP. **Stop! End of Task.**

Delete an ASAP

Background

Use this procedure to delete an Alarm Severity Assignment Profile (ASAP) for a Profile Type in an NE.

Before you begin

Before you begin this task, make sure that the ASAP to be deleted is not assigned to an AID in an NE. If it is, remove the ASAP assignment from the NE's AID. Also, you cannot delete the default ASAP for a Profile Type in an NE.

Be aware that the deletion of an ASAP is only supported for OLS 400G NEs.

Task

Complete the following steps to delete an ASAP.

Step	Action
1	Select an NE from the Map window. **OR** Select no NEs at this point.
2	Select **Fault** from the main menu bar on the Map window. The Fault menu is displayed.
3	Select **Alarm Severity Assignment Profiles** from the Fault menu. If you did not select an NE in Step 1, the Choose an NE/Alarm Severity Profiles is displayed. Select an NE by double-clicking on the item and click the OK button. The Alarm Severity Assignment Profile Management window is displayed. This window consists of an explorer, which allows you to view and select the Profile Type under the selected NE, and six action buttons to the right of the explorer: • Add • Modify • Delete • View • Assignments • Rename

Step	Action (Contd)
4	Click on the plus (+) sign next to the NE TID in the explorer to expand and view the Profile Types for that NE.
5	Click on the plus (+) sign next to the Profile Type in the explorer to expand it. The explorer shows the list of ASAPs available for that Profile Type.
6	Click on the Profile Name of the ASAP to be deleted. The ASAP is highlighted. The five action buttons to the right of the explorer are enabled.
7	Click the Delete button. A pop-up window is displayed, asking if you really want to delete the selected profile.
8	Choose Yes to delete the profile. **Stop! End of Task.**

Rename an ASAP

Background

Use this procedure to rename an existing inactive Alarm Severity Assignment Profile (ASAP). An inactive ASAP profile is one that is not currently assigned to one or more AIDs of an entity.

Before you begin

Before you begin this task, be aware that you cannot rename a default ASAP or active ASAP. An active ASAP is one that is currently assigned to an AID in an NE.

To perform this task, access the Map window.

Task

Complete the following steps to rename an existing ASAP.

Step	Action
1	Select an NE from the Map window. **OR** Select no NEs at this point.
2	Select **Fault** from the main menu bar on the Map window. The Fault menu is displayed.
3	Select **Alarm Severity Assignment Profiles** from the Fault menu. If you did not select an NE in Step 1, the Choose an NE/Alarm Severity Profiles window is displayed. Select an NE by double-clicking on the item and click the OK button. The Alarm Severity Assignment Profile Management window is displayed. This window consists of an explorer, which allows you to view and select the Profile Type under the selected NE, and six action buttons to the right of the explorer: • Add • Modify • Delete • View • Assignments • Rename
4	Click on the plus (+) sign next to the NE TID in the explorer to expand and view the Profile Types for that NE.

Step	Action (Contd)
5	Click on the plus (+) sign next to the Profile Type in the explorer to expand and view the Profile Names under that Profile Type.
6	Click on the existing profile to be renamed under the selected Profile Type. The selected profile is highlighted.
7	Click on the Rename button. The Rename an Alarm Severity Profile window is displayed. This window has three fields: • Profile Type—shows the related ASAP Profile type. This field is greyed out (cannot be modified here) • Profile Name—shows the current ASAP profile name. This field is greyed out (display-only field; the name is not modified in this field) • New Name—field for entering a new name for the selected ASAP profile
8	Enter the new name for the ASAP profile in the New Name field.
9	Click the Apply button to initiate the change or click the OK button to initiate the change and close the Rename an Alarm Severity Profile window. A message is displayed, “Renaming...”, indicating that the system is processing the ASAP name change. **NOTE:** The ASAP renaming process may take a long time. Do not close the Rename an Alarm Severity Profile window until the “Renaming...” message disappears from the status message bar on the window and the renaming process is complete. If you clicked the Apply button on the Rename an Alarm Severity Profile window, click the Close button to close this window when the renaming process is complete. When the renaming process is complete, the Alarm Severity Profiles window shows the ASAP name change in the explorer portion of the window. **Stop! End of Task.**

Assign ASAP to AID

Background

Use this procedure to associate an Alarm Severity Assignment Profile (ASAP) with one or more AIDs in an NE. You have the option of either assigning the default ASAP or an ASAP that you have created to an NE's AID.

Before you begin

Before you begin this task, add the new ASAP (if it has not already been created) or modify the existing ASAP to be associated with the NE's AID(s). Also, use the Assignments button on the Alarm Severity Assignment Profile Management window to view the NE entity(ies) currently assigned to an ASAP (Profile Name).

Task

Complete the following steps to assign an ASAP to one or more AIDs in an NE.

Step	Action
1	Select **Configuration** from the main menu bar on the Map window. The Configuration menu is displayed.
2	Select **Provision** from the Configuration menu. The Choose an NE window is displayed.
3	Double-click on the NE in the list to select it.
4	Click the OK button. The Provisioning window is displayed. The alternate way to access the Provisioning window is to position the mouse pointer on the NE in the Map window and click the left (select) mouse button to select it. The selected NE is highlighted. Then, click the right (menu) mouse button to display a pop-up menu, and select **Provision** from the pop-up menu.
5	In the Network Element Explorer portion of the Provisioning window, expand the NE equipment hierarchy until the desired AID is displayed.
6	Click on the AID to choose it. The AID is highlighted.
7	Click the Provision button. The Provisioning panel of the window is displayed.
8	Click the down arrow next to the ASAP field in the Provisioning panel to display a drop-down list of available ASAPs for the AID. The default ASAP for the AID is highlighted and displayed, by default.
9	Select the ASAP to be assigned to the AID.

Step	Action (Contd)
10	Click the Apply button. A pop-up message is displayed, advising you that the parameter change may affect service and asks whether you want to proceed with the change. The ASAP is assigned to the chosen AID.
11	Choose Yes. The Status Dialog window is displayed, showing that the ASAP assignment request is being processed. Click the Close button on the Status Dialog window to close it.
12	To make additional ASAP assignments, repeat Steps 6-11. **Stop! End of Task.**

View ASAP Assignments

Background

Use this procedure to view the entities to which the chosen Alarm Severity Assignment Profile (ASAP) is assigned.

Before you begin

Before you begin this task, access the Map window.

Task

Complete the following steps to view the entity assignments (by AID) for the selected Profile Type and ASAP.

Step	Action
1	Select an NE from the Map window. **OR** Select no NEs at this point.
2	Select **Fault** from the main menu bar on the Map window. The Fault menu is displayed.
3	Select **Alarm Severity Assignment Profiles** from the Fault menu. If you did not select an NE in Step 1, the Choose an NE/Alarm Severity Profiles is displayed. Select an NE by double-clicking on the item and click the OK button. The Alarm Severity Assignment Profile Management window is displayed. This window consists of an explorer, which allows you to view and select the Profile Type under the selected NE, and six action buttons to the right of the explorer: • Add • Modify • Delete • View • Assignments • Rename
4	Click on the plus (+) sign next to the NE TID in the explorer to expand and view the Profile Types for that NE.

Step	Action (Contd)
5	Click on the plus (+) sign next to the Profile Type in the explorer to expand it.
6	Choose a Profile Name for the profile to be viewed. The Profile name is highlighted.
7	Click on the Assignments button. The Alarm Severity Assignment Profile Assignments window is displayed, showing the entity(ies), by AID, for the selected Profile Type and profile.
8	Click the Close button to close the window. **Stop! End of Task.**

Provision Environmental Alarms

Background

Use this procedure to assign alarm severity levels for environmental alarms generated by miscellaneous discretes (scan points) on the NE, by choosing an Alarm Severity Assignment Profile (ASAP) and a message to be displayed.

Before you begin

Before you begin this task, create an ASAP for the environmental alarm Profile Type of the NE if you want to use an ASAP other than the NE's default ASAP.

Be aware that this function is only available for OLS 400G NEs.

Task

Complete the following steps to set up severity levels for the chosen NE's environmental alarms and an alarm message to be displayed (if needed).

Step	Action
1	Select **Fault** from the main menu bar on the Map window. The Fault menu is displayed.
2	Select **Alarm Provisioning** from the Fault menu. The Fault Management Administrative Settings window is displayed. This window is divided into three tabbed panels: • Miscellaneous Discretes • Alarm Delays • Office Alarms & Messages
3	Click on the Miscellaneous Discretes panel tab, if this panel of the window is not already displayed.
4	In the Miscellaneous Discretes Explorer portion of the window, click on the NE to select it. The NE's TID is highlighted.
5	Click on the plus (+) sign next to the TID in the explorer to expand and display the environmental "scan points" (discretes) for the NE.

Continued on next page

Step	Action (Contd)
6	Click on a scan point (discrete) in the list to select it. If necessary, use the scroll bar to the right of the displayed items in the explorer to find the desired scan point (discrete). The selected discrete is highlighted.
7	Choose an ASAP by clicking the down arrow next to the Environmental ASAP Name field to display a list of available ASAPs and clicking on an ASAP to select it.
8	If needed, enter alarm message text for the selected scan point in the Alarm Message field. The alarm message can contain 1-26 alphanumeric characters. Spaces and periods are allowed. This step is optional. **Stop! End of Task.**

Provision Alarm Delays

Background

Use this procedure to set alarm generation and clearing delays for NEs. Setting an alarm delay invokes the system to only send an alarm notification when an alarm causing event continues to be present for the specified alarm delay period. Setting a clearing delay invokes the system to only clear an alarm when the alarm causing event has been absent for the specified clearing delay period.

Before you begin

Before you begin this task, be aware that the OLS 400G NE only supports alarm generation and clearing delays for facility alarms.

Task

Complete the following steps to set alarm generation and clearing delays for an NE.

Step	Action
1	Select **Fault** from the main menu bar on the Map window. The Fault menu is displayed.
2	Select **Alarm Provisioning** from the Fault menu. The Fault Management Administrative Settings window is displayed. This window is divided into three tabbed panels: ■ Miscellaneous Discretes ■ Alarm Delays ■ Office Alarms & Messages

Step	Action (Contd)
3	Click on the Alarm Delays panel tab. The Alarm Delays panel is displayed.
4	Choose an NE from the Network Elements list by clicking on the NE's TID. The NE is highlighted.
5	Set values for the following fields, as needed: • Alarm Delay Facility/(for AllMetro NEs only)Incoming Signal —use the spinner buttons next to this field to select an alarm delay period for facility alarms (or incoming signal alarms for AllMetro NEs). The available values are 0 (seconds) or greater than 10 seconds and less than or equal to 60 seconds. The available values for an Alarm Delay for Incoming Signals (AllMetro NEs only) are 0-120 (seconds). The value of this field must be less than or equal to the value of the Clear Delay Facility field. The default value is 0, if no other value is selected. • Clear Delay Facility/(for AllMetro NEs only)Incoming Signal —use the spinner buttons next to this field to select a clear delay period for facility alarms (or incoming signal alarms for AllMetro NEs). The available values are 0-60 (seconds). The available values for a Clear Delay for Incoming Signals (AllMetro NEs only) are 0-120 (seconds). The default value is 0, if no other value is selected. • Alarm Delay Equipment—use the spinner buttons next to this field to select an alarm delay period for equipment alarms. The available values are 0-60 (seconds). The value of this field must be less than or equal to the values of the Clear Delay Facility and the Clear Delay Equipment fields. The default value is 0, if no otther value is selected. • Clear Delay Equipment—use the spinner buttons next to this field to select a clear delay period for equipment alarms. The available values are 0-60 (seconds). The default value is 0, if no other value is selected. **Stop! End of Task.**

Provision Alarm Indicators and Autonomous Messages

Background

Use this procedure to enable or disable audio/visual alarm indicators and allow or inhibit autonomous messages for specific NEs in your network.

Before you begin

Before you begin this task, be sure that the Alarm Indicator and/or Audible Alarm feature(s) is enabled if you want to enable either alarm indicator for an NE.

Be aware that the ability to allow or inhibit autonomous messages is only for the current WaveStar SNMS login session, not for all login sessions for the NE. The ability to allow or inhibit autonomous messages is currently only available for OLS 400G NEs.

Task

Complete the following steps to provision audio/visual indicators and receipt of autonomous messages for an NE.

Step	Action
1	Select **Fault** from the main menu bar on the Map window. The Fault menu is displayed.
2	Select **Alarm Provisioning** from the Fault menu. The Fault Management Administrative Settings window is displayed. This window is divided into three tabbed panels: ■ Miscellaneous Discretes ■ Alarm Delays ■ Office Alarms & Messages

Continued on next page

Step	Action (Contd)	
3	Click on the Office Alarms & Messages panel tab. The Office Alarms & Messages panel is displayed.	
4	Choose an NE from the Network Elements list by clicking on the NE's TID. The NE is highlighted.	
5	TO ...	CLICK ...
	• enable audio/visual alarm indicators for alarms on the chosen NE	• the Enabled radio button in the Office A/V Alarms portion of the panel
	• disable audio/visual alarm indicators for alarms on the chosen NE	• the Disabled radio button in the Office A/V Alarms portion of the panel
	• inhibit the receipt of autonomous messages from the chosen NE	• the Inhibit radio button in the Autonomous Messages portion of the panel
	• allow the receipt of autonomous messages from the chosen NE	• the Allow radio button in the Autonomous Messages portion of the panel
	Stop! End of Task.	

Automatically Throttle Alarms

Background

Use this procedure to set up automatic alarm throttling for an NE. When this feature is enabled, alarms (except for Critical Alarms) will be automatically throttled when the number of alarms exceeds the set alarm threshold.

Before you begin

Before you begin this task, access the Map window.

The following table shows the relationship of automatically throttling alarms using this procedure to manually throttling alarms for an NE and whether alarm throttling is enabled for the NE.

Manual Throttling	Auto Alarm Throttling	Alarm Throttling for the NE is:
ON	ON	ON
ON	OFF	ON
OFF	ON	ON (if threshold exceeded)
OFF	OFF	OFF

Task

Complete the following steps to automatically throttle alarms for an NE.

Step	Action	Action
1	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.	
2	Select **Fault** from the Administration menu. The Fault sub-menu is displayed.	
3	Select **Alarm Throttling** from the Fault sub-menu. The Automatic Alarm Throttling window is displayed.	

Continued on next page

Step	Action (Contd)	Action
4	Click on the NE TID in the explorer portion of the window to select it. If the NE is under an aggregate, click on the plus (+) sign next to the aggregate in the explorer to expand the aggregate and select the NE.	
5	TO ... Enable automatic alarm throttling for the selected NE Disable automatic alarm throttling for the selected NE	DO THIS... Click the Enabled button under the “Set Alarm Throttling to” portion of the window and select a alarm threshold by moving the threshold arrow to the left or right until the desired threshold number is shown in the box. The maximum value is 3600 messages per hour. Click the Disabled button under the “Set Alarm Throttling to” portion of the window.
6	Click the Apply button to activate your choice(s) or click the OK button to activate your choice(s) and close the window. **Stop! End of Task.**	

Filter Alarms

Background

Use this procedure to switch between the filtered and unfiltered view of alarms on the Map window, Alarm List, and alarm tallies (the Alarm Notifcation window). When the alarm filtered state is on (the filtered view), alarms or events that are filtered out by the system's alarm filtering methods (Alarm Aging, Event-Per-Time Filtering for the transient condition (TC) Event Browser, Symptomatic Alarm Filtering) are not shown in the Map window, Alarm List, and alarm tallies. When the alarm filtered state is off (the unfiltered view), all alarms and events, including those that would normally be filtered out by the system's various filtering methods, are shown in the Map window, Alarm List, alarm tallies, and TC Event Browser (for TC events that exceed the to the EPT count parameter set). An unfiltered view of alarms is the default. If the WaveStar SNMS GUI becomes flooded with symptomatic alarms, you can enable this option to filter such alarms out of the Map window, Alarm List, and alarm tallies. When you change this option, you must log out and then log back to reflect the change in the filtered or unfiltered state.

Before you begin

Before you begin this task, determine whether you want a filtered or unfiltered view of alarms and events in the network.

Task

Complete the following steps to choose a filtered or unfiltered view of alarms in the Map window, Alarm List, and alarm tallies.

Step	Action	
1	Select **Fault** from the main menu bar. The Fault menu is displayed.	
2	TO.... Obtain a filtered view of alarms in the network Obtain an unfiltered view of alarms in the network	DO THIS... Select the Filter Alarms option in the Fault menu to place an “x” before the option Select the Filter Alarms option to remove the “x” before the option (if there is an “x” there and the filtered view is activated). When the Filter Alarms option is changed, a pop-up window is displayed with the message “You must first log out and log back into the EMS”. A message is also displayed in the Map window status bar “User Preferences Saved Successfully”. This indicates that the change to the Alarm Filtering state has been saved for when you log out and log back into WaveStar SNMS.
3	Log out of WaveStar SNMS and then log back in to obtain the new view of alarms in the network. **Stop! End of Task.**	

Display the Transient Condition Event Browser

Background

Use this procedure to display a list of transient condition (TC) events. TC events (for example, a protection switch occurs) are generated by one or more NEs in the network and do not require clearing messages to be generated because they do not affect the condition of the NE over an extended period of time.

The following events are shown in the Transient Condition Browser:

- TL1-based messages—REPT-EVT with the "condeff" parameter equals "TC" (BWM/2.5G/25G_10G/OC192-4F/AllMetro)

  Only the TC events that exceed the Event-Per-Time (EPT) alarm filtering count are displayed; in other words, the REPT-EVT with "condeff" = "TC" and passing the EPT filter ("eptexceeded" = "1"). The EPT filter does not apply to other TC events, such as REPT-SW and REPT-PROTSW.

- CMISE-based messages—Report Event message M-EVENT-REPORT with "condeff" (mapped API parameter) equals "TC" (400G).

When a new TC event arrives, it is placed at the top of the TC Browser listing. TC events that exceed the maximum number of TC events that have not been cleared are automatically removed from the list, starting with the oldest TC events.

Task

Complete the following steps to display the Transient Condition browser.

Step	Action
1	Position the mouse cursor on the Transient Condition Event Browser toolbar button on the Map window toolbar and click the button. **NOTE:** The Transient Condition Event Browser toolbar button is located to the right of the Global Unacknowledge toolbar button on the Map window toolbar. Another way to tell if it is the Transient Condition Toolbar button is to move the mouse cursor to each button until the tooltips help or the message in the Map window status bar identifies it as the Transient Condition Event Browser button. **OR** Choose **Fault** from the main menu bar on the Map window, which displays The Fault menu. Choose **Transient Condition Event Browser** from the Fault menu. The Transient Condition Event Browser window is displayed. The window provides a listing of each TC event by date and time of occurrence.
2	To save the output from this window to a file, do the following, a. Click on **File** on the main menu bar on the Map window and then select **Save As**. A pop-up window is displayed. b. Select the PC drive where the file folder resides in which to store the file output by clicking the down arrow next to the “Look In” field on the window. Select the drive. c. Select and open the file folder for the saved output file by double-clicking on the folder in the scrollable list on the pop-up window. d. Type a name for the output file in the File name field. e. Click the Save button. The output is saved to the named file. **NOTE:** To view the saved output file, use the Wordpad application. *Continued on next page*

Step	Action (Contd)
3	When you are finished viewing the transient event information, access the **File** pull-down menu from the menu bar and select **Close** or, to close the window, click the “x” button in the upper-right hand corner of the window border. **Stop! End of Task.**

Display and Use the Network Alarm/ Event Log

Background

Use this procedure to display the Network Alarm/Event Log, and to use this log to view and save important system-compiled alarm and event information.

Task

Complete the following steps to use the Network/Alarm Event Log.

Step	Action
1	Select **Logs** from the main menu bar on the Map window. This displays the sub-menu.
2	Select **Network Alarm/Event** from the displayed sub-menu. This displays the viewing parameters window for the Alarm/Event Log. *Continued on next page*

Step	Action (Contd)
3	On the viewing parameters window, select the parameters for which you want to display Alarm/Event Log data: • Use the up and down arrows on the **Start Date & Time** and **End Date & Time** spinner fields to adjust the entries in these fields. Network Alarm/Event data will be displayed only for data that falls within the selected parameter values. (If you make no adjustments, the start and end dates default to the current date, the start time defaults to 00:00, and the end time defaults to 15 minutes after the time this window was opened.) You can also type the date and time in the **Start Date & Time** and **End Date & Time** fields. The date must be input in dd-mm-yyyy format (for example, July 30, 2000 is entered as 30-07-2000). The year input must be the current year, and the date input cannot be beyond the current date. The time must be input in 24-hour format as hh:mm, in 15 minute increments (for example, 11:15 P.M. is entered as 23:15). If the date or time entered is invalid, the color of the field changes to yellow, and you must re-enter a valid date or time in the proper format. • To choose to view data related only to selected network elements or only to selected Aggregates, select the **Network Elements** or the **Aggregates** radio button (to the right of **Choose from a list of:**), respectively. If you select the **Network Element** radio button, then a list of NEs appears just below and to the left of the radio button. If you select the **Aggregate** radio button, then a list of ag-gregates appears instead of NEs. After selecting one of these two radio buttons, you can use the arrow push buttons between the left and right list areas to move selected NEs or aggregates (whichever of the two applies) into the right side “Chosen” list area. The NEs or aggregates you move into this “Chosen” list will be the NEs or aggregates for which later you will be viewing Alarm/Event Log data. • To sort the data in a particular order, click the **Ascending** or **Descending** radio button. **Descending** is the default. • Use the **Alarms** and **Events** checkboxes near the lower left of the viewing parameters window to request both alarm and event information or just one of the two. Clicking these checkboxes toggles between placing a check (include this data) and removing the check (do *not* include this data). • Select from the **Alarm record options** and/or **Event record options** lists to further specify the type of data you want to display. *Continued on next page*

Step	Action (Contd)
4	After you have finished specifying parameters on the viewing parameters window, click the OK button. This closes the window and displays the Log browser window, containing the information that meets your specified parameters. You can use this window to view the log records or save them to a file. **Stop! End of Task.**

Display and Use the Network Notifications Log

Background

Use this procedure to display the Network Notifications Log, and to use this log to view and save important system-compiled network notifications information, including protection switching history.

Task

Complete the following steps to use the Network Notifications Log.

Step	Action
1	Select **Logs** from the main menu bar on the Map window. This displays a sub-menu.
2	Select **Network Notifications** from the displayed sub-menu. This displays the viewing parameters window for the Network Notifications Log.
3	On the viewing parameters window, select the parameters for which you want to display Network Notifications Log data: • Use the up and down arrows on the **Start Date & Time** and **End Date & Time** spinner fields to adjust the entries in these fields. Network Notifications data will be displayed only for data that falls within the selected parameter values. (If you make no adjustments, the start and end dates default to the current date, the start time defaults to 00:00, and the end time defaults to 15 minutes after the time this window was opened.) You can also type the date and time in the **Start Date & Time** and **End Date & Time** fields. The date must be input in dd-mm-yyyy format (for example, July 30, 2000 is entered as 07-30-2000). The year input must be the current year, and the date input cannot be beyond the current date. The time must be input in 24-hour format in 15 minute increments (for example, 11:15 P.M. is entered as 23:15). If the date or time entered is invalid, the color of the field changes to yellow, and you must re-enter a valid date or time in the proper format. • To choose to view data related only to selected network elements or only to selected Aggregates, select the **Network Elements** or the **Aggregates** radio button (to the right of **Choose from a list of:**), respectively. If you select the **Network Element** radio button, then a list of NEs appears just below and to the left of the radio button. If you select the **Aggregate** radio button, then a list of ag-gregates appears instead of NEs. After selecting one of these two radio buttons, you can use the arrow push buttons between the left and right list areas to move selected NEs or aggregates (whichever of the two applies) into the right side “Chosen” list area. The NEs or aggregates you move into this “Chosen” list will be the NEs or aggregates for which later you will be viewing Network Notifications Log data. • To sort the data in a particular order, click the **Ascending** or **Descending** radio button. **Descending** is the default. • Use the **Show these types of log records: radio buttons and a** field near the lower part of the viewing parameters window to further specify the type of data wanted. *Continued on next page*

Step	Action (Contd)
4	After you have finished specifying parameters on the viewing parameters window, click the OK button. This closes the window and displays the Log browser window, containing the information that meets your specified parameters. You can use this window to view the log records or save them to a file. **Stop! End of Task.**

Display and Use the Network Command/Response Log

Background

Use this procedure to display the Network Command/Response Log, and to use this log to view and save important system-compiled network command/response information.

Task

Complete the following steps to use the Network Command/Response Log.

Step	Action
1	Select **Logs** from the main menu bar on the Map window. This displays a sub-menu.
2	Select **Network Command/Response** from the displayed sub-menu. This displays the viewing parameters window for the Network Command/ Response Log. *Continued on next page*

Step	Action (Contd)
3	On the viewing parameters window, select the parameters for which you want to display Network Command/Response Log data: • Use the up and down arrows on the **Start Date & Time** and **End Date & Time** spinner fields to adjust the entries in these fields. Network Command/Response data will be displayed only for data that falls within the selected parameter values. (If you make no adjustments, the start and end dates default to the current date, the start time defaults to 00:00, and the end time defaults to 15 minutes after the time this window was opened.) You can also type the date and time in the **Start Date & Time** and **End Date & Time** fields. The date must be input in dd-mm-yyyy format (for example, July 30, 2000 is entered as 07-30-2000). The year input must be the current year, and the date input cannot be beyond the current date. The time must be input in 24-hour format as hh:mm in 15 minute increments (for example, 11:15 P.M. is entered as 23:15). If the date or time entered is invalid, the color of the field changes to yellow, and you must re-enter a valid date or time in the proper format. • To choose to view data related only to selected network elements or only to selected Aggregates, select the **Network Elements** or the **Aggregates** radio button (to the right of **Choose from a list of:**), respectively. If you select the **Network Element** radio button, then a list of NEs appears just below and to the left of the radio button. If you select the **Aggregate** radio button, then a list of ag-gregates appears instead of NEs. After selecting one of these two radio buttons, you can use the arrow push buttons between the left and right list areas to move selected NEs or aggregates (whichever of the two applies) into the right side “Chosen” list area. The NEs or aggregates you move into this “Chosen” list will be the NEs or aggregates for which later you will be viewing Network Command/ Response Log data. • To sort the data in a particular order, click the **Ascending** or **Descending** radio button. **Descending** is the default. • If you belong to a command group that allows you to view other user’s command/response log records (check with your system administrator), then you can click on the More Options button to display an additional viewing parameters window. Click More Options, and then use this additional window to select the users and log record sources you want to include in your viewing parameters. In both cases, select the desired parameters by clicking on them in the left list, and using the right arrow symbol button (**>**) to move the selections to the “Chosen” list. (The current user’s username already appears in the “Chosen” list by default.) *Continued on next page*

Step	Action (Contd)
4	After you have finished specifying parameters on one or both of the viewing parameters windows, click the OK button. This displays the Log browser window, containing the information that meets your specified parameters. You can use this window to view the log records or save them to a file. **Stop! End of Task.**

Display and Use the EMS Alarm/Event Log

Background

Use this procedure to display the EMS Alarm/Event Log, and to use this log to view and save important system-compiled alarm information.

Task

Complete the following steps to use the EMS Alarm/Event Log.

Step	Action
1	Select **Logs** from the main menu bar on the Map window. This displays a sub-menu.
2	Select **EMS Alarm/Event** from the displayed sub-menu. This displays the viewing parameters window for the EMS Alarm Log Viewing Parameters.
3	On the viewing parameters window, select the time and date parameters for which you want to display EMS Alarm/Event Log data: ➧ Use the up and down arrows on the **Start Date & Time** and **End Date & Time** spinner fields to adjust the entries in these fields. Alarm data will be displayed only for data that falls within the selected parameter values. (If you make no adjustments, the start and end dates default to the current date, the start time defaults to 00:00, and the end time defaults to 15 minutes after the time this window was opened.) You can also type the date and time in the **Start Date & Time** and **End Date & Time** fields. The date must be input in dd-mm-yyyy format (for example, July 30, 2000 is entered as 07-30-2000). The year input must be the current year, and the date input cannot be beyond the current date. The time must be input in 24-hour format as hh:mm in 15 minute increments (for example, 11:15 P.M. is entered as 23:15). If the date or time entered is invalid, the color of the field changes to yellow, and you must re-enter a valid date or time in the proper format. ➧ To sort the data in a particular order, click the **Ascending** or **Descending** radio button. **Descending** is the default.
4	After you have finished specifying parameters on the viewing parameters window, click the OK button. This closes the window and displays the Log browser window, containing the information that meets your specified parameters. You can use this window to view the log records or save them to a file. **Stop! End of Task.**

Display and Use the EMS Activity Log

Background

Use this procedure to display the EMS Activity Log, and to use this log to view and save important user/system-compiled activity information.

The onset and termination of system overload conditions are also logged in the Activity Log.

Task

Complete the following steps to use the EMS Activity Log.

Step	Action
1	Select **Logs** from the main menu bar on the Map window. This displays a sub-menu.
2	Select **EMS Activity** from the displayed sub-menu. This displays the viewing parameters window for the EMS Activity Log.
3	On the viewing parameters window, select the parameters for which you want to display Activity Log data: • Use the up and down arrows on the **Start Date & Time** and **End Date & Time** spinner fields to adjust the entries in these fields. Activity data will be displayed only for data that falls within the selected parameter values. (If you make no adjustments, the start and end dates default to the current date, the start time defaults to 00:00, and the end time defaults to 15 minutes after the time this window was opened.) You can also type the date and time in the **Start Date & Time** and **End Date & Time** fields. The date must be input in dd-mm-yyyy format (for example, July 30, 2000 is entered as 07-30-2000). The year input must be the current year, and the date input cannot be beyond the current date. The time must be input in 24-hour format as hh:mm in 15 minute increments (for example, 11:15 P.M. is entered as 23:15). If the date or time entered is invalid, the color of the field changes to yellow, and you must re-enter a valid date or time in the proper format. • To choose to view data related only to a selected user(s), you can use the arrow push buttons between the left and right list areas to move a selected user(s) into the right side “Chosen” list area. The user(s) you move into this “Chosen” list will be the user(s) for which you will be viewing Activity data. • You can choose the activity criteria you want to include in your viewing parameters by using the scroll down list to select **All Activities**, **Only Completed Activities**, or **Only Failed Activities**. • Select the desired activities from the **Available Activities** list by clicking to highligh the desired activities in the left list, and using the arrow push buttons to move the selections to the “Chosen” list.
4	After you have finished specifying parameters on the parameters windows, click the OK button. This displays the Log browser window, containing the information that meets your specified parameters. You can use this window to view the log records or save them to a file. **Stop! End of Task.**

Performance Management

2

Introduction

Summary

This chapter describes procedures for collecting and viewing performance monitoring (PM) data for network elements managed by WaveStar SNMS.

Before you begin

Read the Performance Management Concepts chapter to acquire an understanding of the Performance Managment functions provided by WaveStar SNMS.

Contents

This chapter discusses the following topics:

Provision PM Data Collection for an NE

Background

Use this procedure to enable or disable the collection of Path, Far-end or Near-end PM data for a port or tributary by an NE. Provisioning of PM data collection by the NE should be done prior to globally enabling the PM feature in WaveStar SNMS and enabling the collection of PM data from an NE by WaveStar SNMS.

Before you begin

Before you begin this task, access the Map window.

Related tasks

See the following related tasks:

- Enable/Disable the PM Feature
- Enable/Disable PM Data Collection

Task

Complete the following steps to enable or disable the collection of Path, Far-end or Near-end PM data for a port or tributary by an NE.

Step	Action
1	Select **Configuration** from the main menu bar on the Map window. **Result:** The Configuration menu is displayed.
2	Select **Provision** from the Configuration menu. **Result:** The Choose an NE window is displayed.
3	Double-click on the NE in the list to select it.
4	Click the OK button. **Result:** The Provisioning window is displayed. The alternate way to access the Provisioning window is to position the mouse pointer on the NE in the Map window and click the right (menu) mouse button to display a pop-up menu, and select **Provision** from the pop-up menu.

Step	Action (Contd)	
5	In the Network Element Explorer portion of the Provisioning window, expand the NE equipment hierarchy until the desired port or tributary AID is displayed.	
6	Click on the AID to choose it. The AID is highlighted.	
7	Click the Provision button. **Result:** The Provisioning panel of the window is displayed.	
8	Use the scroll bar located to the right of the Provisioning panel of the Provisioning window to scroll down to the “Performance Management” section of the Provisioning panel. The “Performance Management” section of the Provisioning panel contains parameter fields for enabling/disabling collection of Near-end and Far-end PM data for the selected port.	
9	TO... Enable collection of Far-end section PM data for the selected NE port/ Disable collection of Far-end section PM data for the selected NE port	DO THIS... Click the down arrow next to the Far-end PM Section Enable field to display a drop-down list. The choices are: Enable or Disable. Choose Enable. Click the down arrow next to the Far-end PM Section Enable field to display a drop-down list. The choices are: Enable or Disable. Choose Disable (Disable is the default.)

Step	Action (Contd)	
10	TO...	DO THIS...
	Enable collection of Near-end section PM data for the selected NE port	Click the down arrow next to the Near-end PM Section Enable field to display a drop-down list. The choices are: Enable or Disable. Choose Enable. (Enable is the default.)
	Disable collection of Near-end section PM data for the selected NE port	Click the down arrow next to the Near-end PM Section Enable field to display a drop-down list. The choices are: Enable or Disable. Choose Disable.

Step	Action (Contd)	
11	TO... Enable collection of Path PM data for the selected NE tributary Disable collection of Path PM data for the selected NE tributary	DO THIS... Click the down arrow next to the Path PM Section Enable field to display a drop-down list. The choices are: Enable or Disable. Choose Enable. (Enable is the default.) Click the down arrow next to the Near-end PM Section Enable field to display a drop-down list. The choices are: Enable or Disable. Choose Disable.
12	Click the Apply button. A pop-up message is displayed, advising you that the parameter change may affect service and asks whether you want to proceed with the change.	
13	Choose Yes. The Status Dialog window is displayed, showing that the provisioning request is being processed. Click the Close button on the Status Dialog window to close it.	

Enable/Disable the PM Feature

Background

Use this procedure to globally enable or disable the Performance Monitoring (PM) data collection feature for all supported NEs (OLS 400G, BWM, STM64). When the PM data collection feature is turned on, WaveStar SNMS periodically collects PM data from each NE that has PM data collection activated. When the PM feature is globally disabled, PM data is not collected from any NE.

Task

Complete the following steps to globally enable or disable the PM feature.

Step	Action	
1	Select **Performance** from the main menu bar on the Map window. The Performance menu is displayed.	
2	Select **Global PM Management** from the Performance menu. The Global PM Data Administration window is displayed.	
3	IF … you want to enable the PM feature	THEN … click on the Collect PM Data box to place a check there and select the retention period for 15-minute and 1-day PM data reports. To select the retention period, move the slider bar for each report type to the left or right. You can set the retention period from 1 to 30 days for each report type. The number displayed to the right of each slider bar shows the setting selected. **NOTE:** Click the Retrieve button to display the current system default retention periods.
	you want to disable the PM feature	click on the Collect PM Data box to remove the check or leave the box blank.
4	Click the Apply button to activate your choices. **Stop! End of Task.**	

Enable/Disable PM Data Collection

Background

Use this procedure to enable or disable PM data collection for the specified NE and, if PM data collection is enabled, select the PM reporting interval. You can also reset the digital PM data registers and the start time of 1-day PM data collection, if needed (for OLS 400G NEs only).

Before you begin

Before you begin this task, be aware that NE PM data collection will not be performed until the PM feature is globally enabled (see Enable/Disable the PM Feature). Be aware that PM data collection is suspended during an alarm storm. WaveStar SNMS resumes PM data collection after the alarm storm has subsided.

Task

Complete the following steps to enable collection of the selected PM data types or disable PM data collection for the entire NE. You may also reset digital PM data registers (bins) and/or the start time of 1-day PM data collection for OLS 400G NEs, if needed.

Step	Action
1	Select **Performance** from the main menu bar on the Map window. The Performance menu is displayed.
2	Select **NE PM Management** from the Performance menu. The Choose an NE window is displayed.
3	Double-click on the NE in the list to select it and click the OK button. The NE PM Data Administration window is displayed. **OR** Select an NE on the Map or Subnetwork Explorer, right-click on the NE to bring up a pop-up menu, select **Performance Management** from the pop-up menu, and select **NE PM Management** to display the NE PM Data Administration window. If the selected NE is an OLS 400G, the NE PM Data Administration window has a Network Element explorer, that can be expanded to show the equipment hierarchy for provisioning and two panels on the right side of the window: • EMS PM Data Settings • Network Element PM Data Settings **NOTE:** The Network Element PM Data Settings panel is only displayed if the selected NE is an OLS 400G. If the selected NE is not an OLS 400G, only the EMS PM Data Settings panel is displayed. *Continued on next page*

Step	Action (Contd)	
4	In the EMS PM Data Settings panel: IF ... • you want to collect PM data for the selected PM data type in 15-minute intervals • you want to collect PM data for the selected PM data type in 1-day intervals • you want to collect both 15-minute and daily PM data for the PM data type • collect no PM data (disable PM data collection for the NE)	 THEN ... • check the Enable 15 Minute PM data collection for this NE box. • check the Enable 1-Day PM data collection for this NE box. • check both boxes. • click both boxes to remove the checks, or leave both boxes blank.
5	IF ... • you want to collect PM data from all data types • you want to collect PM data from one or more types **NOTE:** Use the Retrieve button to retrieve the previous settings.	THEN ... • click the All Facility Types in This NE radio button. • click the Only these facility types radio button and then check the data types for PM data.
6	IF ... • you only want to enable/disable PM data collection for the NE • you also want to reset the digital PM data registers and/or the start time of 1-day PM data collection for an OLS 400G NE	THEN ... • click the Apply button to activate your choices. Stop at this point. • go to Step 7.
7	Click on the Network Element PM Data Settings panel tab. The Network Element PM Data Settings panel is displayed (if the selected NE is an OLS 400G). *Continued on next page*	

Step	Action (Contd)	
8	In the Network Element Explorer portion of the panel: Click on the NE's TID to select the NE level of the equipment hierarchy **OR** Click the plus (+) sign next to the NE's TID and click the plus (+) sign to expand the equipment hierarchy until the specific level and unit of equipment that you want to provision is shown in the explorer (bay, shelf, slot, circuit pack, or optical port).	
9	Click the Provision button below the explorer portion of the panel. The NE-level PM Data Settings fields are displayed.	
10	IF... You selected the NE level of the equipment hierarchy for provisioning in step 8	THEN... Select to reset the digital PM registers for: • All SUPV Channels • All OTUs • All SUPV Channels and ALL OTUs by clicking the associated radio button in the Reset NE's Digital PM Registers (Bins) portion of the Network Element PM Settings panel. Go to Step 11 to choose which digital PM registers to reset.
	You selected a bay, shelf, or slot for provisioning in step 8	Click on the Reset Digital PM Registers (Bin) panel tab. Go to Step 11 to choose which digital PM registers to reset

Continued on next page

Step	Action (Contd)	
11	For the entire NE or the selected unit of equipment (bay, shelf, or slot):	
	TO ...	CLICK ...
	• reset the current 15-minute digital PM data registers	• the Reset 15 Minute Bins Only button
	• reset the current 1-day digital PM data registers	• the Reset 1 Day Bins Only button
	• reset both digital PM data registers	• the Reset Both Bins button
12	If you selected the NE level for provisioning in Step 8, and you enabled collection of 1-day PM data on the EMS Data Settings panel, the NE's 1 Day PM Data Collection Start Time portion of the panel displays the current start time (hour) for collection of 1-day PM data. To change the start time, click the up/down spinner buttons to change the time (hour). The hour counter uses a 24-hour time format. For example, to change the start of 1-day PM data collection to 1:00 PM, click the up/down spinner buttons until the number **13** is displayed in the hour field. **NOTE:** Use the Retrieve button to retrieve the current settings.	
13	Click the Apply button to activate your choices. A pop-up question dialog window is displayed, informing you that changing the PM parameter values may affect service, and asks if you want to modify the values. Choose Yes to initiate the PM data parameter changes. **Stop! End of Task.**	

Administer PM Data

Background

Use this procedure to display and provision analog and/or digital PM data parameters for the selected NE interface. For the OLS 400G, this option allows you to provision PM threshold values for the:

- Supervisory Channel
- Optical Line
- Optical Channel
- Optical Translator Unit (OTPS)

Before you begin

Be aware that the PM feature must be globally enabled and the selected NE must have PM data collection activated for one or more PM data types.

PM threshold values can only be provisioned for an OLS 400G NE with this procedure. For other NE types, PM threshold values must be set by issuing TL1 commands via the Cut-Through window.

Task

Complete the following steps to display and provision PM parameters for the selected NE interface.

Step	Action
1	Select **Performance** from the main menu bar on the Map window. The Performance menu is displayed.
2	Select **NE PM Management** from the Performance menu. The Choose an NE window is displayed.
3	Double-click on the NE in the list to select it and click the OK button. The NE PM Data Administration window is displayed. **OR** Select an NE on the Map or Subnetwork Explorer, right-click on the NE to bring up a pop-up menu, select **Performance Management** from the pop-up menu, and select **NE PM Management** to display the NE PM Data Administration window. The NE PM Data Administration window is divided into two parts. The left side of the window contains an NE explorer tree. Depending on the NE type chosen, the NE explorer may contain just a TID at the top part of the hierarchy, or can be expanded to show equipment entities and AIDs for facilities below the NE (TID) level. The right side of the window consists of two panels: • EMS PM Data Settings • Network Element PM Data Settings **NOTE:** The Network Element PM Data Settings panel is only displayed if the NE is an OLS 400G. The remaining steps in this procedure only apply to an OLS 400G NE. When the PM Data Administration window is first displayed, the NE TID is selected in the explorer tree, the explorer tree is unexpanded (if it is expandable), and the current EMS PM Data settings for the entire NE are shown in the EMS PM Data Settings panel.
4	Click on the Network Element PM Data Settings tab.
5	In the explorer portion of the window, single-click on the plus (+) sign next to the TID of the selected NE to expand the tree and display the equipment entities of the NE. Continue to click and expand levels of the equipment hierarchy until you locate the AID of a PM facility for which you want to display and provision PM parameters. Double-click on the AID of the PM facility in the explorer tree to select it. *Continued on next page*

Step	Action (Contd)
6	Click on the Provision button below the explorer tree portion of the window. The PM Data Admin Panel for the selected NE facility is displayed in the right side of the window.
7	Depending on the NE PM facility selected, the PM Data Admin Panel displays some or all the following parameter fields and buttons: • Digital PM Threshold Settings—this portion of the panel allows you to set the 15-minute and/or 1 day threshold values for digital PM data collection for the specific parameter. Click on the Get NE Defaults button to retrieve the current defaults from the NE for these parameters. Modify the value(s) as needed. • Analog PM Threshold Settings—this portion of the panel allows you to display and change the low and high threshold values for analog PM data for the selected PM facility. Click the Retrieve button to obtain the current settings from the NE. Modify the value(s) as needed. • Recalculate Baseline—this portion of the panel allows you to recalculate (set) the baseline value for an analog PM data parameter. First, click the down arrow next to the Reason Code field to display a valid list of reason codes for the recalculation (for example, Add a New NE), and select a reason code. Depending on the NE PM facility selected, one or more of the following buttons to recalculate the signal power baseline value is displayed and enabled: — Recalulate Xmit: click this button to recalculate the signal power transmitted baseline value — Recalculate Receive: click this button to recalculate the signal power received baseline value — Recalculate Both: click this button to recalculate the baseline value for signal power in both directions **NOTE:** To obtain the current values from the NE for these fields, click the Retrieve button.
8	Click the Apply button to activate your choices. A pop-up question dialog window is displayed, informing you that changing the PM parameter values may affect service, and asks if you want to modify the values. Choose Yes to initiate the PM data parameter changes. **Stop! End of Task.**

View PM Data (Facility)

Background

Use this procedure to view the PM data from an NE facility collected by WaveStar SNMS. You can choose to view either current data from the NE(s) or historical data stored in the WaveStar SNMS database, as well as for what facility type, and whether to show 15-minute or 1-day PM data. The data selected for viewing is shown in table format, sorted and filtered according to your choices.

Before you begin

Before you begin this task, the PM feature must be globally enabled, the selected NE must have PM data collection activated for one or more PM data types, and the Facility option under the View PM Report Settings section of the Global PM Data Administration window must be selected.

Task

Complete the following steps to view PM data for a specified NE.

Step	Action
1	Select **Performance** from the main menu bar on the Map window. The Performance menu is displayed.
2	Select **View PM Data** from the Performance menu. The Choose an NE window is displayed.
3	Select an NE and click the OK button. The View PM Data window is displayed. **OR** Select an NE on the Map or Subnetwork Explorer, right-click on the NE to bring up a pop-up menu, select **Performance Management** from the pop-up menu, and select **View PM Data** to display the View PM Data window.

Step	Action (Contd)
4	Choose to show either current data or historical data by clicking on the appropriate radio button. If you choose current 1-day data, the PM data that is displayed is from 12:00 AM of the current day through the current time. If you choose historical 1-day data, the PM data that is displayed is from 12:00 AM of the date entered through the current date and time. If you chose historical data, choose the date and time of the data by using the date and time (if you choose 15-minute data, in hours) spinner fields. **NOTE:** If you configured the data retention period on the Global PM Data Administration window for less than 30 days, you can only view the data files that fall within the selected data retention period.
5	Choose one of the NE facility types for viewing by clicking on the appropriate radio button.
6	Choose to show 15-minute or 1-day PM data by clicking on the appropriate radio button.
7	Click the OK button. The PM Data window is displayed, showing the selected PM data in table format. To save the contents of table data to a file on the local system, click the Save button on the PM Data window. **Stop! End of Task.**

View PM Data (AID)

Background

Use this procedure to view the PM data collected by WaveStar SNMS. You can choose to view either current data from the NE(s) or historical data stored in the WaveStar SNMS database, as well as for what facility type, and whether to show 15-minute or 1-day PM data. The data selected for viewing is shown in table format, sorted and filtered according to your choices.

Before you begin

Before you begin this task, the PM feature must be globally enabled, the selected NE must have PM data collection activated for one or more PM data types. and the AID option under the View PM Report Settings section of the Global PM Data Administration window must be selected.

Task

Complete the following steps to view PM data for a specified NE and AID.

Step	Action
1	Select **Performance** from the main menu bar on the Map window. The Performance menu is displayed.
2	Select **View PM Data** from the Performance menu. The Choose an NE window is displayed.
3	Select an NE and click the OK button. The View PM Data window is displayed. **OR** Select an NE on the Map or Subnetwork Explorer, right-click on the NE to bring up a pop-up menu, select **Performance Management** from the pop-up menu, and select **View PM Data** to display the View PM Data window.
4	Choose to show 15-minute or 1-day PM data by clicking on the appropriate radio button.

Step	Action (Contd)
5	Choose to show either current data or historical data by clicking on the appropriate radio button. If you choose current 1-day data, the PM data that is displayed is from 12:00 AM of the current day through the current time. If you choose historical 1-day data, the PM data that is displayed is from 12:00 AM of the date entered through the current date and time. If you chose historical data, choose the date and time of the data by using the date and time (if you choose 15-minute data, in hours) spinner fields. **NOTE:** If you configured the data retention period on the Global PM Data Administration window for less than 30 days, you can only view the data files that fall within the selected data retention period.
6	Enter the starting date/time (From:) and ending date/time (To:) in the Choose Date & Time section of the window. For each date, enter the month, in mm format, in the first box (for example, January is entered as “01”). Enter the day, in dd format, in the second box (for example, the 15th day is entered as “15”). Enter the year, in yyyy format (for example, the year 2000 is entered as “2000”). For each time, the hour is entered in the first box, in 24-hour, hh format, and the minutes are entered in the second box, in mm format (for example, 1:15 PM is entered as “13:15”).

Step	Action (Contd)
7	Choose one of the NE facility types for viewing by clicking on the appropriate radio button.
8	Choose an AID for viewing PM data for a specific NE entity by clicking the Choose AID button. A pop-up window is displayed, showing the AIDs available for selection. Select an AID from the list. The selected AID is shown in the field next to the “Choose AID to View PM Data on:” label on the window.
9	Click the OK button. The PM Data window is displayed, showing the selected PM data in table format. To save the contents of table data to a file on the local system, click the Save button on the PM Data window. **Stop! End of Task.**

View a PM Profile

Background

Use this procedure to view an existing PM profile for a Profile Type in an NE.

Before you begin

Be aware that is GUI function is not available for OLS 400G NEs. Before you begin this task, access the Map window.

Task

Complete the following steps to view an existing PM profile.

Step	Action
1	Select an NE from the Map window. **OR** Select no NEs at this point.
2	Select **Performance** from the main menu bar on the Map window. The Performance menu is displayed.
3	Select **PM Profiles** from the Performance menu. If you did not select an NE in Step 1, the Choose an NE window is displayed. Select an NE by double-clicking on the item and click the OK button. The Manage PM Profiles window is displayed. This window consists of an explorer, which allows you to view and select the Profile Type under the selected NE, and five action buttons to the right of the explorer: • Add • Modify • Delete • View • Assignments
4	Click on the plus (+) sign next to the NE TID in the explorer to expand and view the Profile Types for that NE. *Continued on next page*

Step	Action (Contd)
5	Click on the plus (+) sign next to the Profile Type in the explorer to expand and view the Profile Names under that Profile Type.
6	Choose a Profile Name under a Profile Type. The chosen Profile Name is highlighted.
7	Click on the View button. The View a PM Profile window is displayed, showing the PM parameter threshold values for the selected Profile Type. **Stop! End of Task.**

Add a PM Profile

Background

Use this procedure to add a new PM profile for a Profile Type in the chosen NE. To add a new PM profile, the PM parameter threshold values of the default profile for the selected Profile Type are copied over to a new Profile Name. The newly created PM profile will have the same threshold values as the default PM profile unless they are changed. Once it is created, the new PM profile, which is identified by its Profile Name, can be assigned to an entity (AID) in the NE.

Before you begin

Before you begin this task, be aware that WaveStar SNMS will prevent you from adding a new PM profile for a Profile Type if the maximum number of allowable profile for that Profile Type in the NE has been exceeded. Also, this GUI function is not available for OLS 400G NEs.

Task

Complete the following steps to add a new PM profile.

Step	Action
1	Select an NE from the Map window. **OR** Select no NEs at this point.
2	Select **Performance** from the main menu bar on the Map window. The Performance menu is displayed.
3	Select **PM Profiles** from the Performance menu. If you did not select an NE in Step 1, the Choose an NE/Alarm Severity Profiles is displayed. Select an NE by double-clicking on the item and click the OK button. The Manage PM Profiles window is displayed. This window consists of an explorer, which allows you to view and select the Profile Type under the selected NE, and five action buttons to the right of the explorer: • Add • Modify • Delete • View • Assignments
4	Click on the plus (+) sign next to the NE TID in the explorer to expand and view the Profile Types for that NE.
5	Select the desired Profile Type in the explorer by single-clicking on it.

Step	Action (Contd)
6	Click the Add button. The Add a Performance Management Profile window is displayed, showing the default PM parameter threshold values in the default profile for the Profile Type chosen.
7	To create a profile for a Profile Type other than the one originally chosen, go back to the Manage PM Profiles window, select a different Profile Type in the explorer, and then click the Add button to return to the Add a Performance Management Profile window.
8	Enter a name for the new profile in the Profile Name field. The Profile Name can be 1-24 characters (A-Z, a-z, 0-9). **NOTE:** The new Profile Name cannot be Default. Also, you cannot use a name that has already been used under the selected Profile Type.
9	If desired, make changes to the threshold values for the new profile.
10	Click the Apply button activate your choices, or click the OK button to activate your choices and close the window. The new profile is created. **Stop! End of Task.**

Modify a PM Profile

Background

Use this procedure to modify an existing PM profile for a Profile Type. You can modify the PM thresholds in an existing profile, the Profile Name, or both.

Before you begin

Be aware that this GUI function is not available for OLS 400G NEs. Before you begin this task, access the Map window.

Task

Complete the following steps to modify an existing profile.

Step	Action
1	Select an NE from the Map window. **OR** Select no NEs at this point.
2	Select **Performance** from the main menu bar on the Map window. The Performance menu is displayed.
3	Select **PM Profiles** from the Performance menu. If you did not select an NE in Step 1, the Choose an NE window is displayed. Select an NE by double-clicking on the item and click the OK button. The Manage PM Profiles window is displayed. This window consists of an explorer, which allows you to view and select the Profile Type under the selected NE, and five action buttons to the right of the explorer: • Add • Modify • Delete • View • Assignments
4	Click on the plus (+) sign next to the NE TID in the explorer to expand and view the Profile Types for that NE.
5	Click on the plus (+) sign next to the Profile Type in the explorer to expand it.
6	Choose a Profile Name for the profile to be modified. The Profile name is highlighted.

Step	Action (Contd)
7	Click on the Modify button. The Modify a PM Profile window is displayed, showing the the current PM parameter threshold values in the selected Profile Type and Profile Name.
8	Make changes to the PM parameter threshold values, as needed. You can also change the Profile Name if desired. **NOTE:** The new Profile Name cannot be Default. Also, you cannot use a name that has already been used under the selected Profile Type.
9	Click the OK button. The changes are made to the selected profile. **Stop! End of Task.**

Delete a PM Profile

Background

Use this procedure to delete a PM profile for a Profile Type in an NE.

Before you begin

Be aware that this GUI function is not available for OLS 400G NEs. Before you begin this task, make sure that the PM profile to be deleted is not assigned to an AID in an NE. If it is, remove the PM profile assignment from the NE's AID. Also, you cannot delete the default profile for a Profile Type in an NE.

To perform this task, access the Map window.

Task

Complete the following steps to delete a PM profile.

Step	Action
1	Select an NE from the Map window. **OR** Select no NEs at this point.
2	Select **Performance** from the main menu bar on the Map window. The Performance menu is displayed.
3	Select **PM Profiles** from the Performance menu. If you did not select an NE in Step 1, the Choose an NE window is displayed. Select an NE by double-clicking on the item and click the OK button. The Manage PM Profiles window is displayed. This window consists of an explorer, which allows you to view and select the Profile Type under the selected NE, and five action buttons to the right of the explorer: • Add • Modify • Delete • View • Assignments
4	Click on the plus (+) sign next to the NE TID in the explorer to expand and view the Profile Types for that NE.

Step	Action (Contd)
5	Click on the plus (+) sign next to the Profile Type in the explorer to expand it. The explorer shows the list of profiles available for that Profile Type.
6	Click on the Profile Name of the profile to be deleted. The profile is highlighted.
7	Click the Delete button. A pop-up window is displayed, asking if you really want to delete the selected profile.
8	Choose Yes to delete the profile. **Stop! End of Task.**

Assign PM Profile to AID

Background

Use this procedure to associate a PM profile with one or more AIDs in an NE. You have the option of either assigning the default PM profile or a PM profile that you have created to an NE's AID.

Before you begin

Be aware that this GUI function is not available for OLS 400G NEs. Before you begin this task, add the new profile (if it has not already been created) or modify the existing profile to be associated with the NE's AID(s). Also, use the Assignments button on the Manage PM Profiles window to view the NE entity(ies) currently assigned to a Profile Name.

Task

Complete the following steps to assign an ASAP to one or more AIDs in an NE.

Step	Action
1	Select **Configuration** from the main menu bar on the Map window. The Configuration menu is displayed.
2	Select **Provision** from the Configuration menu. The Choose an NE window is displayed.
3	Double-click on the NE in the list to select it.
4	Click the OK button. The Provisioning window is displayed. The alternate way to access the Provisioning window is to position the mouse pointer on the NE in the Map window and click the right (menu) mouse button to display a pop-up menu, and select **Provision** from the pop-up menu.
5	In the Network Element Explorer portion of the Provisioning window, expand the NE equipment hierarchy until the desired AID is displayed.
6	Click on the AID to choose it. The AID is highlighted.
7	Click the Provision button. The Provisioning panel of the window is displayed.

Continued on next page

Step	Action (Contd)
8	Click the down arrow next to the appopriate Profile pointer field in the Provisioning panel to display a drop-down list of available profiles for the AID. The currently assigned PM Profile for the AID is highlighted and displayed, by default. **NOTE:** There may be more than one profile displayed, depending on the AID selected. For example, there may be both Physical and Section-Line profile fields available for provisioning. The types of PM profiles that can be assigned depend on the rate of the AID selected.
9	Select the PM profile to be assigned to the AID.
10	Click the Apply button. A pop-up message is displayed, advising you that the parameter change may affect service and asks whether you want to proceed with the change.
11	Choose Yes. The Status Dialog window is displayed, showing that the profile assignment request is being processed. Click the Close button on the Status Dialog window to close it.
12	To make additional profile assignments, repeat Steps 6-11. **Stop! End of Task.**

View PM Profile Assignments

Background

Use this procedure to view the entities to which the chosen PM profile is assigned.

Task

Complete the following steps to view the entity assignments (by AID) for the selected Profile Type and Profile Name.

Step	Action
1	Select an NE from the Map window. **OR** Select no NEs at this point.
2	Select **Performance** from the main menu bar on the Map window. The Performance menu is displayed.
3	Select **PM Profiles** from the Performance menu. If you did not select an NE in Step 1, the Choose an NE window is displayed. Select an NE by double-clicking on the item and click the OK button. The Manage PM Profiles window is displayed. This window consists of an explorer, which allows you to view and select the Profile Type under the selected NE, and five action buttons to the right of the explorer: • Add • Modify • Delete • View • Assignments
4	Click on the plus (+) sign next to the NE TID in the explorer to expand and view the Profile Types for that NE.
5	Click on the plus (+) sign next to the Profile Type in the explorer to expand it.
6	Choose a Profile Name for the profile to be viewed. The Profile name is highlighted.
7	Click on the Assignments button. ThePM Profile Assignments window is displayed.

Step	Action (Contd)
8	At the top of the window is a drop-down list for selecting the shelf. Select the desired shelf and click the View Assignments button. The panel is updated and shows the entity(ies), by AID, for the selected Profile Type, profile name, and shelf.
9	To view assignments on a different shelf, select another shelf from the drop-down list and click the View Assignment button.
10	After you are finished viewing assignments, click the Close button to close the window. **Stop! End of Task.**

System Introduction

3

Introduction

Purpose

This chapter provides a general system overview of WaveStar SNMS.

Objectives

This chapter explains how to do the following:

- List the features available on WaveStar SNMS and briefly describe each feature
- Identify the basic hardware components of WaveStar SNMS
- Identify the basic software components of WaveStar SNMS
- Identify the network element types and releases supported by WaveStar SNMS
- Identify the system interfaces of WaveStar SNMS

Contents

This chapter discusses the following topics:

System Overview

Description

The Lucent Technologies' WaveStar™ SubNetwork Management System (SNMS) is an Element Management System (EMS) that supports the new generation of Lucent Technologies' transmission products: the Lucent Technologies' WaveStar product family. The WaveStar products are intelligent Network Elements (NEs) which can discover and report their configuration (including physical equipage) and connectivity within the network.

WaveStar SNMS operates as an enhanced graphical tool and as a general configuration management aid. It is designed to take advantage of the capabilities of the WaveStar NEs, and to optimize the role of the NEs in management functions to create an intelligent operations environment.

Just as the WaveStar network elements are the solution to your transport network needs, WaveStar SNMS is the answer to the corresponding operations needs to efficiently manage the network. The following details some of the ways WaveStar SNMS achieves this:

- WaveStar SNMS provides centralized, secure, remote administration of Synchronous Optical Networks (SONET) and Dense Wavelength Division Multiplexing (DWDM) subnetworks. From a single work center, a WaveStar SNMS user can remotely manage SONET and DWDM NEs. Lucent Technologies patented Dynamic Network Operations (DNO) process gathers network configuration information from the NEs, providing accurate, hands-off population of the WaveStar SNMS database, and ensures that the WaveStar SNMS management functions operate using the actual network configuration.
- WaveStar SNMS provides fault, performance, configuration, security, and log management functions via the GUI.
- WaveStar SNMS supports 7-layer OSI as well as OSI over Transmission Control Protocol/Internet Protocol (TCP/IP) communication protocols over LAN physical interfaces.
- WaveStar SNMS supports X.25-based protocol layer for Lucent Technologies' Large Capacity Terminal (LCT).
- WaveStar SNMS supports CMISE and TL1 application protocols.
- WaveStar SNMS supports communication multiplexing or concentration to provide network security and to record all database changes.
- WaveStar SNMS provides a TL1 cut-through capability, allowing the user to access an NE through a native command set.

Graphical user interface

WaveStar SNMS incorporates a platform independent, Java-based Graphical User Interface (GUI) that allows for the use of PCs running Windows NT as the user's terminals. The WaveStar SNMS GUI is a common interface to all NEs, regardless of type, and provides a powerful, flexible, and user friendly interface to execute the most frequently used actions. The GUI also supports numerous customization options so that users may tailor the displays in accordance with their own preferences.

The GUI provides graphical features such as multilevel displays of the network, an automatically generated map of the overall managed domain, hierarchically arranged equipment displays down to the shelf level, a graphical representation of the cross connection configuration with point and click provisioning, and form and menu-based provisioning for viewing and setting provisional parameters. The GUI also provides the ability to initiate a cut-through session to directly send TL1 commands to NEs.

Year 2000 compliance

WaveStar SNMS and the underlying software platforms are designed to comply with the Year-2000[1] initiative to ensure correct date representation and date/time calculation for the year 2000 and beyond. This includes data that is received by WaveStar SNMS from the supported NEs.

1 WaveStar SNMS Release 4.2 and UNIX Release 11.0 are Year-2000 compliant only when the required Year-2000 patch set (Y2K-1020S800) is installed.

Features

Overview

WaveStar SNMS provides a set of standard and value-added features used to administer the WaveStar NEs. These are grouped into the following categories:

- Fault Management
- Performance Management
- Configuration Management
- Security Management
- Log Management
- NE Event Handler
- Cut-Through Capability

Fault management

Fault Management monitors alarms and conditions in the subnetwork. WaveStar SNMS receives autonomous alarm messages from NEs when alarm states are set or cleared. These alarm messages are processed and made available to the user through the GUI, or to other network surveillance systems. WaveStar SNMS supports the following Fault Management tasks:

- Alarm status indication on the network map for equipment, facility failures, and updates
- Hierarchical alarm status indication at NE, bay, shelf, and circuit pack levels
- Textual alarm summary report
- Alarm provisioning at the NE level (via TL1 cut-through)
- Alarm provisioning at the EMS level
- Alarm synchronization
- Autonomous alarm handling
- Alarm correlation
- Alarm aging

Performance management

WaveStar SNMS collects Performance Monitoring (PM) data from NEs that have PM data collection activated. It stores collected PM data for a retention period set by the user (up to 30 days). WaveStar SNMS allows the user to view unprocessed PM data, or the data can be exported to an off-line system for more sophisticated analysis and reporting purposes.

Configuration management

WaveStar SNMS has a Dynamic Network Operations (DNO) feature that retrieves the internal configurations of NEs and external connectivity relationships. This feature enables the system to discover, without manual intervention, the topology of subnetworks consisting of Lucent Technologies' NEs.

The GUI supports the following configuration management tasks:

Subnetwork configuration management

- Network Element/trail discovery/update/display
- Aggregate management/display

NE configuration management

- Equipage discovery/update/display
- Equipment provisioning and pre-provisioning
- Cross-connection provisioning/display
- Tributary reservation
- Manual path provisioning
- Protection switch management
- Port provisioning

Software management

- Software download to NEs
- Software copy from one NE to another
- Software install (activate) on NE
- NE data backup and restore

Security management

WaveStar SNMS maintains a set of connections to the NEs that are shared by all users. Administration of individual user logins and passwords is centralized on WaveStar SNMS rather than distributed across the large number of managed NEs.

All users are required to have a login and password to communicate with the system. The system administrator assigns users to the NEs they can use (Target Groups) and the actions they can perform (Command Groups). Target Groups and Command Groups can be set up according to the type of tasks users are performing, such as maintenance, provisioning, or monitoring.

WaveStar SNMS provides two levels of security management:

- EMS security management
  - — defines EMS users (user id and password)
  - — partitions the network into user-defined target groups
  - — defines command groups
  - — assigns EMS user to target groups and command groups
- NE security management
  - — provides services to manage NE user id and password

Log management

Log Management provides services to various system modules including:

- Writing log messages to database tables
- Retrieving log messages from database tables
- Displaying information on selected activities

These log messages are helpful for keeping track of information regarding system performance and actions. The information can be filtered to suit the user's needs.

NE event handler

The NE Event Handler process is a passive distributor of non-alarm autonomous messages emitted by the NEs. It registers with the Southbound interface for database change messages from TL1 NEs and with Q3 gateway for CMISE NEs.

The main functions of the NE Event Handler (NEH) are the following:

- Receive non-alarm autonomous messages (TL1 from Southbound and CMISE from Q3 gateway)
- Distribute the received messages to the user
- Log by invoking the Log Manager

Cut-through capability

In order for the user to execute NE TL1 commands that may not be explicitly supported, a cut-through capability is available. WaveStar SNMS allows the user access only to the NEs and associated commands defined by the Target and Command Groups for which the user is assigned.

Hardware Architecture

Overview

WaveStar SNMS consists of a Hewlett-Packard (HP) host processor, and GUI workstations (PC/Sun) connected via an Ethernet LAN, with the option to interface via a Wide Area Network (WAN).

A WAN/PSN is recommended for large, geographically dispersed configurations to concentrate access from SNMS to the managed subnetworks. The same WAN/PSN can also be used to access other network management systems or other hosts. Every SNMS installation requires data connections to each managed subnetwork.The southbound WAN from SNMS to the NEs must support an OSI/LAN interface and/or an IP/LAN interface. If FT-2000 LCT NEs are to be managed an X.25 PSN is required.

Host platform

The system hardware architecture consists of two main components:

- HP K-class or N-class server running HP-UX version 11.0 (Nov. 1999) with associated peripherals (console, terminals, and printers)
- PC running Windows NT® 4.0 (Service Pack 4) or
- Sun Solaris workstation Version 2.6 or 2.7.

GUI workstation

The recommended platform for the Java GUI client is a personal computer running Windows NT 4.0 with Service Pack 4. The Java GUI software is installed on the PC as a standalone application. Transaction requests are issued by the GUI software to the EMS host. The host returns responses associated with these transactions back to the PC. The interface to the PC is via an 802.3 LAN link. The GUI application messages and GUI cut-through data traffic are transported using this interface.

System redundancy options

The EMS system redundancy option provides multiple levels of application and host redundancy for backup support and disaster recovery in the event of failure. The local and geographic redundancy configurations require two similarly equipped hosts that operate in an active/standby arrangement. The two host computers are linked via a TCP/IP WAN segment and employ data replication to provide near real-time database synchronization of the standby host with the currently active host.

Under normal operating conditions, the SNMS application is running on the active host, with that host actively monitoring all network elements in the management

domain. The backup host is in a hot-standby state, maintaining data connections to the network, and using data replication from the active host to keep its database current. In the event of a primary host failure, there is automatic switch-over with the local redundancy configuration, while a manual command is needed to initiate the switch-over with the geographical redundancy configuration. Upon switch-over, the standby host assumes active control of the network.

The SNMS redundancy options include:

- host redundancy
- local redundancy
- geographic redundancy
- dual redundancy

Host redundancy

Host redundancy provides component redundancy within a single host where there is no backup host available (Figure 3-1). Recovery relies on switching control to another resource on the same host such as a backup LAN card or mirrored disk.

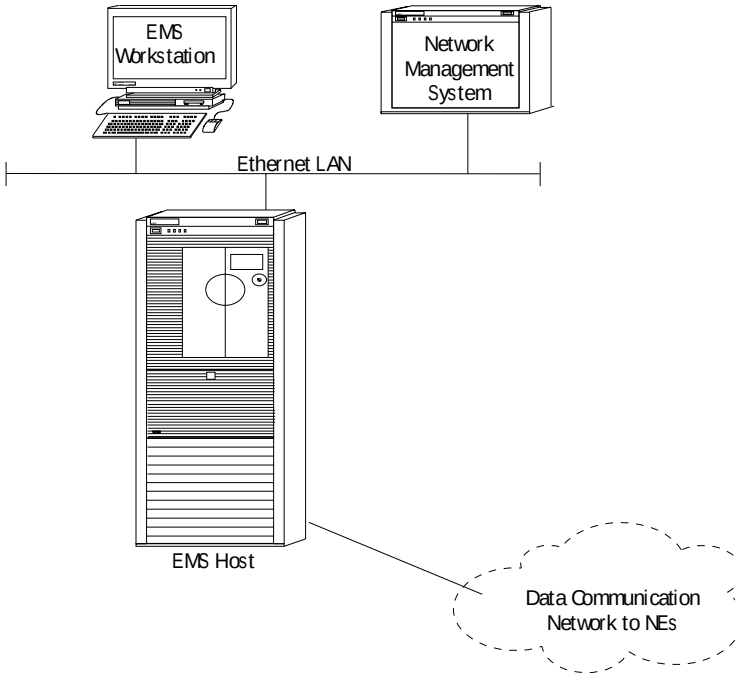

Figure 3-1. EMS Basic Host Redundancy Configuration

Local redundancy

Local redundancy employs two similarly equipped hosts located in the same building (Figure 3-2). Each host is configured with redundant hardware components. Should the primary host fail, the backup host is activated automatically without user intervention.

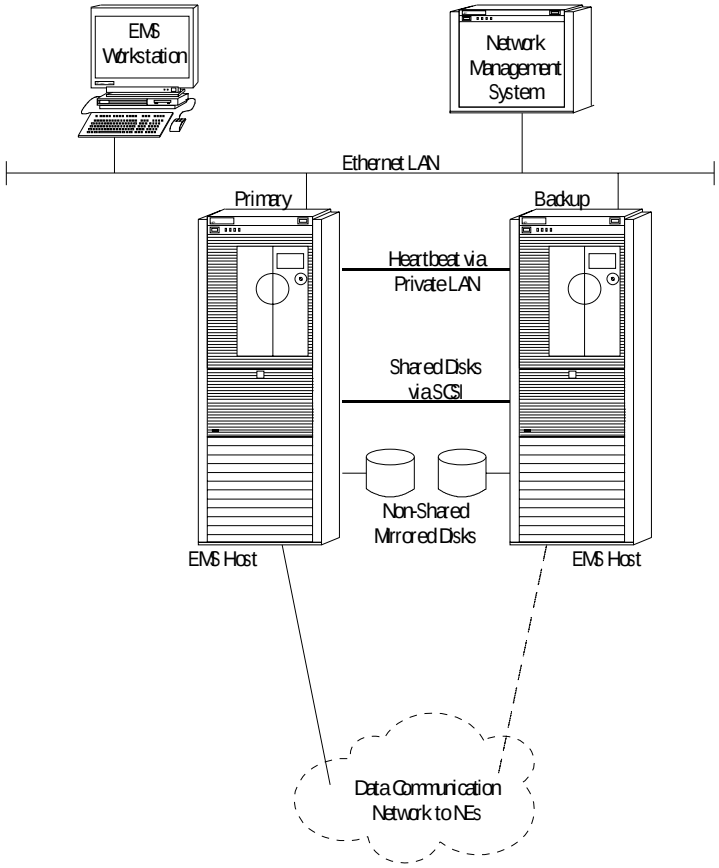

Figure 3-2. EMS Local Redundancy Configuration

Under normal operating conditions, the WaveStar SNMS Host is in service (or “active”) on the primary host monitoring all network elements in the database. The backup host exists in a passive (or “standby”) mode with the WaveStar SNMS application running in a “read only” mode. Although the “standby” host is logged into all network elements, it does not initiate any event to the network or react to any notifications from the network. Database synchronization is handled using Informix Enterprise Replication, FTP file transfer, and event forwarding from the “active” host. In the event of a primary host failure, control is automatically

switched from the primary to the backup host, changing the WaveStar SNMS application from “standby” to “active” service without user intervention. Once the primary host failure is repaired, manual intervention is required to synchronize the database and switch control back to the primary host.

Geographic redundancy

Geographic redundancy employs two similarly equipped hosts located in different geographical locations (like Atlanta, GA, and Denver, CO (Figure 3-3). Each host is configured with redundant hardware components, and resides on a TCP/IP WAN segment. Data replication and event forwarding via WAN are used to maintain EMS database and UNIX file system synchronization.

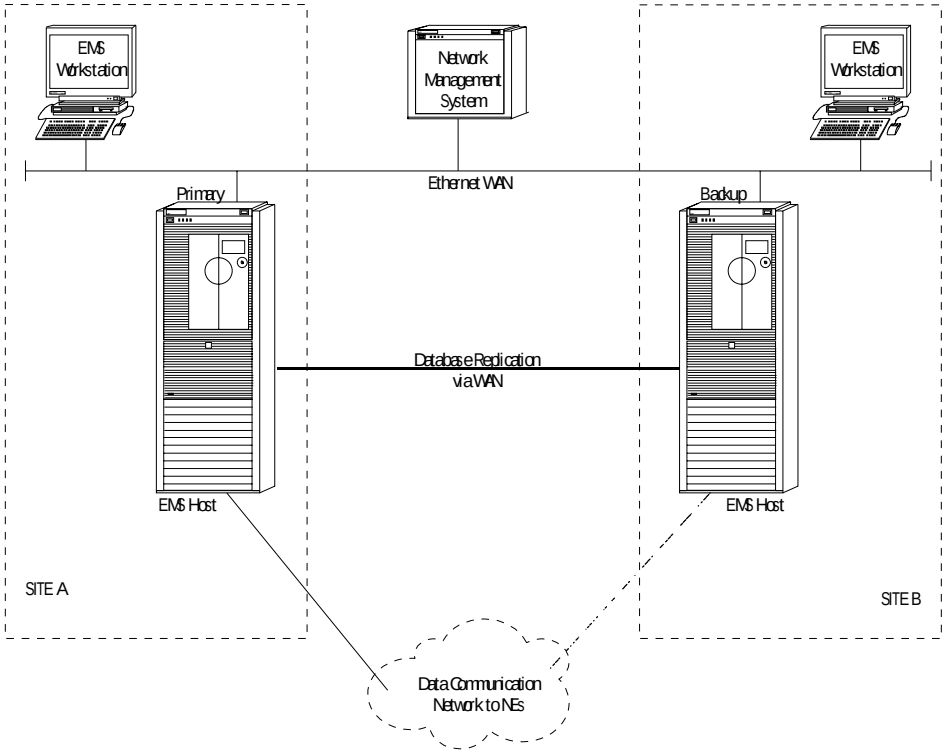

Figure 3-3. EMS Geographic Redundancy Configuration

Under normal operating conditions, the WaveStar SNMS application is in service (or “active”) on the primary host monitoring all network elements in the database. The backup host exists in a passive (or “standby”) mode with the WaveStar SNMS application running in a “read only” mode. Although the “standby” host is logged

into all networks, it does not initiate any event to the network or react to any notification from the network. Database synchronization is handled using Informix Enterprise Replication, FTP file transfer, and event forwarding from the “active” host. In the event of a primary host failure, control can be manually switched from the primary to the backup host changing the WaveStar SNMS application from “standby” to “active” service.

Unlike local redundancy, which is automated, geographic redundancy requires an external command to invoke a switch over. This external command can be issued via a UNIX command line by the WaveStar SNMS system administrator, or by association from a Network Management System. Once the primary host failure is repaired, manual intervention is required to synchronize the database and switch control back to the primary host

Dual redundancy

In dual redundancy, both local and geographic strategies are combined to provide an additional level of reliability. As shown in Figure 3-4, both Site A and B have two hosts that can be employed to monitor the network.

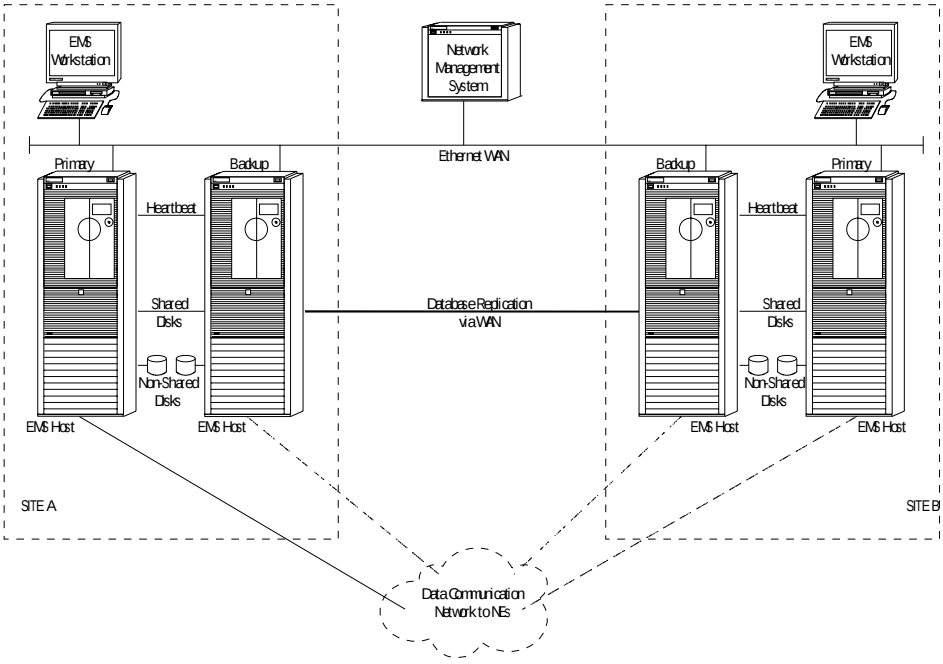

Figure 3-4. EMS Dual Redundancy Configuration

The following redundancies are implemented using the architecture shown in Figure 1-4.

- Local redundancy is implemented at Site A identifying a primary and backup host. Both hosts are brought on-line (one active, one standby) as described in local redundancy.
- Local redundancy is implemented at Site B identifying a primary and backup host. Both hosts are initially left in a “down” state, however, with neither running the WaveStar SNMS application.
- Geographic redundancy is implemented to designate the primary host at Site B as the backup host to the primary host at Site A. The primary host at Site B is then brought on-line in “standby” mode as described in geographic redundancy. Thus, the primary host at Site A replicates it’s database to both the backup host at Site A and the primary host at Site B, keeping all three synchronized.

In the event of a primary host failure at Site A, control automatically switches to the backup host at Site A (for example, local redundancy). In addition, the backup host at Site A now begins replicating its database to the primary host in Site B to maintain synchronization (e.g., geographic redundancy). At this point, the user has two options:

1. If the expected time to repair the failed host at Site A is short, the system can be run in geographic redundancy mode until the failed host is repaired.
2. If the expected time to repair the failed host at Site A is lengthy, the backup host at Site B can be brought on-line in “standby” mode and synchronized with the active host at Site A.

In the event there is a complete failure of Site A (both primary and backup hosts), the primary host at Site B can be “activated” and a local redundancy configuration at Site B can be used.

Once the affected site is repaired, a manual procedure must be used to synchronize the primary host at Site A. Only then can database replication be enabled at Site B to fully synchronize the primary host at Site A. Once fully synchronized, a manual switchover must be initiated to switch control back to the primary host at Site A and re-enable dual redundancy.

Software Architecture

Overview

The software architecture can be divided into the following major subsystems:

- Configuration Management
- Fault Management
- NE Event Handler
- EMS Security Management
- Southbound Management Interface
  - X.25-based protocol layer
  - OSI-based protocol layer
  - OSI over TCP/IP-based protocol layer
  - TL1 Manager
  - Connection Manager
  - Gateway process
  - QA process (CMISE only)
  - SONET Directory Service (SDS)
- Log Management
- Operation, Administration, and Maintenance
  - Log and trace
  - Scheduler
- JAVA-based GUI

Supported Network Elements

Overview

WaveStar SNMS R4.2 provides element management support for the following NEs and their software releases. The information is the best available at the time of publication of this document and is subject to change based on the availability of the NE releases.

Table 3-1. Network Elements Supported by WaveStar SNMS R4.2

Managed NEs	Supported Releases
WaveStar BWM	R1.2, R1.3, R2.0, R3.0
WaveStar OLS 400G	R2.0, R3.0, R4.0
WaveStar NCC	R3.0, R3.1, R3.2, R4.0
WaveStar 2.5G/10G	R2.0, R3.0, R4.0 (10G shelf option available beginning in R3.0)
WaveStar OC-192 4-Fiber	R1.0, R1.1, R2.0
STM-64	R1.0, R1.1, R2.0, R2.1
FT-2000 LCT	R4.0
LambdaRouter	R1.0

System Interfaces

Overview

The WaveStar SNMS southbound communication interface connects with NEs, and supports OSI and OSI over TCP/IP communications with the NEs.

- OLS 400G supports both an OSI and OSI over TCP/IP interface.
- BWM and 2.5G only support an OSI interface. However, since the NCC acts as a transport bridge, WaveStar SNMS also supports an OSI over TCP/IP interface to BWM and 2.5G NEs via a transport bridge.
- NCCs support both OSI and OSI over TCP/IP interfaces, much like the 400G.

Southbound interface

The WaveStar SNMS Southbound interface contains the required functionality to connect to the NEs, to manage these connections, and to forward and receive the messages between the NEs and WaveStar SNMS, for all supported communication protocols.

Connection Manager Process

The Connection Manager (CM) process centralizes the functions of sending, receiving, routing, and processing the connections needed for responses and autonomous messages going in, and coming from, the CMISE and TL1 Southbound subsystems. CM handles the following functions:

- At start-up, load external configurative parameters from a configuration file.
- Create and terminate associations to all NEs.
- Perform association requests in a staggered manner to minimize the impact of the connection processes on the network.
- Implement association recovery mechanisms.
- Receive connection-related indication messages from TL1 and CMISE Southbound subsystems, update association status in memory, and forward notifications to WaveStar SNMS.
- Create/modify/delete NEs, store and forward related information.
- Send notification to WaveStar SNMS for any incorrect NE types.

CMISE Southbound

The CMISE Southbound subsystem is made of two processes for the support of Lucent Technologies' WaveStar 400G NEs.

- Gateway (GW) process
  - — serves as a bridge process between the Management Functional Area (MFA) and the Q3 Manager
  - — receives requests from MFA and the Connection Manager, and sends them down to the Q3 Manager through a socket interface
  - — receives responses and autonomous notifications coming from NE via socket. Sends them to MFA or the Connection Manager as required.
  - — logs Command and Responses, via the Log Server and Log library.
- Q3 Adaptor process

  The Q-Adaptor maintains a representation of the manged object instances of the managed object classes defined in the information model and converts Common Management Information Service Element (CMISE) requests into the non-TMN format of the underlying OS or NE. It also converts the non-TMN notifications received from a non-TMN OS or NE and converts them to CMISE notifications.

TL1 Southbound

TL1 Southbound is supported by the TL1-Manager process, which is responsible for command/response handling.

SONET Directory Services

The SONET Directory Services (SDS) subsystem resides in the Southbound of the system. All system applications access the shared memory contained in SDS to retrieve information. The shared memory contains the status, last update time, and various directory information. WaveStar SNMS employs two agents to manage this information: the Directory Services Agent (DSA) and the Directory User Agent (DUA). The DSA maintains the Directory Information Base and the DUA retrieves and gives information to and from it.

The DSA organizes network elements into a structure known as the Directory Information Base (DIB). The DUA accesses the DSA for any new NEs registered in the MIT and notifies other WaveStar SNMS processes of the existence of the new NE. WaveStar SNMS then logs into the new NE and via the Dynamic Network Operations (DNO) process gathers the internal configuration and external connectivity relationships from the NE. This ensures that the WaveStar SNMS management functions operate using the actual network configuration.

Northbound interface to WaveStar NMS

WaveStar SNMS supports a northbound interface to the WaveStar Network Management System (WaveStar NMS). WaveStar NMS is a part of a telecommunications management network that provides comprehensive and integrated management of an entire transport network. WaveStar NMS manages network elements through an interface with WaveStar SNMS. WaveStar SNMS exchanges NE alarm information, configuration information, and performance monitoring data with WaveStar NMS, through a standard CORBA interface.

There are two WaveStar NMS interfaces supported by WaveStar SNMS. The first interface is a server to server interface and the other interface is a GUI to GUI interface.

The server to server interface is responsible for passing NE information from SNMS to WaveStar NMS. The interface is called the northbound TL1 interface in SNMS jargon and the southbound interface in NM terminology. The interface takes place over a socket connecting the WaveStar NMS server to the WaveStar SNMS server.

The GUI to GUI cut-through allows WaveStar NMS to invoke WaveStar SNMS GUI screens from the WaveStar NMS GUI. This feature is called the F-interface in both WaveStar NMS and WaveStar SNMS terminology. Both GUIs must be installed on an NT Terminal Server and be properly configured to talk to one another. The interface supports a one-to-many configuration where one WaveStar NMS GUI can talk to many WaveStar SNMS GUIs of different versions.

Alarm Management Concepts

4

Introduction

Purpose

This chapter provides general information about monitoring alarms and conditions in a subnetwork of network elements managed by WaveStar SNMS. It also provides general information about the Log Management features provided by WaveStar SNMS for displaying and viewing alarm data, NE commands/ responses, and other messages generated by WaveStar SNMS and managed network elements.

Objectives

This chapter explains how to do the following:

- Use the Alarm Notification window to identify the number and type of alarms currently in the subnetwork
- Display the Alarm Summary, Alarm List, and Alarm Details windows to identify various information about current alarms
- Initiate resynchronization of alarms
- Limit the amount of autonomous messages to be monitored for an NE using the Alarm Throttling feature
- Administer audible alarms
- Manage alarm severity assignment profiles (ASAPs) for an NE
- Use the Network Alarm/Event Log to obtain a history of all alarms and events generated by NEs as a result of unexpected behaviors

- Use the Network Notification Log to obtain information on database changes, protection switching, and other NE-related activities
- Use the Network Command/Response Log to review all commands and responses that originate from or received by WaveStar SNMS
- Use the EMS Alarm Log to obtain information on all system hardware-related and/or software-related alarms
- Use the EMS Activity Log to obtain information about all user and system-related acitivities

Contents

This chapter discusses the following topics:

Fault Management

Overview

Fault Management monitors alarms and conditions in the subnetwork. Users can access Fault Management functions from the Main Menu, or by accessing the pop-up menu on an NE or Aggregate icon in the Map window, or on the items listed in tables or other screens. Some important Fault Management features include the alarm summary and alarm list, viewing autonomous alarms as they are received, alarm throttling, and visible alarm indicators.

Features

WaveStar SNMS receives autonomous alarm messages from NEs when alarm states are set or cleared. These alarm messages are processed and made available to the user through the GUI. Following is a complete list of Fault Management features, all of which are available to the user via the GUI:

- Alarm notification (tallies)
- Alarm Summary
- Alarm List
- Alarm Indication and Acknowledgement
- Alarm Details
- Trail Alarms
- Alarm Resynchronization
- Alarm Throttling
- Audible Alarms
- Alarm Browser
- Alarm Filtering
- Alarm Severity Assignment Profile Management
- Transient Event Condition Browser
- Alarm Provisioning—office alarm and messages, alarm delays, miscellaneous discretes

In addition to the above alarm windows and reports, the Map window indicates which NEs and aggregates have alarms and their severity level. Also, the EMS host icon indicates the alarm status of the host. Furthermore, the Map window indicates which NEs have unacknowledged alarms (by flashing those nodes), and which NEs have exceeded the alarm throttling threshold (with the color gray).

Alarm notification

Another way WaveStar SNMS keeps you informed about current alarms is via the Alarm Notification window. This window contains information on the type and number of current alarms in the subnetwork. It remains open on your screen, and comes to the front each time another alarm is tallied.

The Alarm Notification window contains five buttons for SONET, labeled Critical, Major, Minor, Not Alarmed (for SONET), or, for SDH, four buttons labeled Prompt, Deferred, Informational, and EMS Communications, corresponding to the types of alarms that may appear. The “Not Alarmed” (for SONET) or “Informational” (for SDH) represents the number of Standing Condition (SC) events that have been received which require clearing. Below each of these buttons is a number that indicates the current number of alarms/events for each category.

When the color of an NE is white on the Map window (the default color), this indicates that the NE is in a “Not Alarmed” state, or has received one or more Standing Condition (SC) events which require clearing by the NE. When the SC event has been cleared by the NE, the color of the NE returns to green, indicating that there are no active alarms present and the NE is communicating.

To see more information about a specific alarm severity level or the event, just point to the desired severity button on the Alarm Notification window and click. The system then displays the Alarm List window, filtered by the severity type of the clicked button.

Alarm summary

The Alarm Summary feature provides a single-line overview of alarm information for each node and trail in an aggregate. This information is provided via the Alarm Summary window on the GUI. This window lists the NEs in your Target Group and displays the number of Critical, Major, Minor and Not Alarmed (standing condition) alarms/events (for SONET) or Prompt, Deferred, and Informational (standing condition) alarms/events (for SDH) for each NE. The alarms can be listed by severity or TID.

Alarm list

The Alarm List contains a line of various information about each active alarm in an NE. You can sort the list using various critieria, such as alarm severity and age, age alone, condition, date/time logged, and acknowledged vs. unacknowledged. You can also acknowledge or unacknowledge the alarms listed here.

Alarm indication and acknowledgement

The Alarm Indicator feature graphically indicates the arrival of new alarms by flashing the impacted nodes and aggregates. If there are one or more alarms against an NE and alarm indication is enabled, that node will flash (in the color of the highest severity alarm). Likewise, if there are one of more alarms against one or more NEs in an aggregate and alarm indication is enabled, that aggregate will

flash. (When all the alarms against an NE or aggregate are acknowledged it no longer flashes.) Users should acknowledge alarms for which they are responsible. (The system tags the acknowledgment so that other users will not attempt to troubleshoot the same problem.)

Alarm details

Alarm Details are available to the user via the Alarm List window. This window contains a line of information about each active alarm in an NE or aggregate. Before acknowledging an alarm, it is a good practice to display it on the Alarm List window to check the details and make sure you want to acknowledge it. You can then perform the acknowledgement right from the Alarm List window.

Trail alarms

Trails are physical links between NEs. The system monitors all existing trails for alarm conditions.

NEs can only automatically discover and report to WaveStar SNMS trails over which there is an active DCC. Users can, however, add trails between any pair of termination points on NEs.

The following Information about trail alarms that have occurred can either be displayed on the Alarm Summary window or by selecting the trail:

- Trail Alarm Summary Window—this lists a count of critical, major, and minor alarms for the AIDs that terminate the trail between two NEs.
- Trail Alarm List—this contains a line of information about each active alarm for the trails between two NEs. This information includes alarm severity, occurrence date/time, condition, and date/time logged.

Alarm resynchronization

Alarm Resynchronization provides the ability for the system to update its alarm list, autonomous message log, and command/response log from network elements in the subnetwork whenever any outage of NE communications occurs. The system automatically resynchronizes alarms whenever the communications status with an NE changes from “down” to “up.”

Before resynchronizing alarms for an NE, the user should disable the automatic/manual alarm throttling control for the NE. Alarm resynchronization does not work unless the NE is in an unthrottled state.

The alarm resynchronization process does not clear the existing GUI display and alarm notification/list displays during the resynchronization process, but rather retains the existing alarms until the resynchronization is completed. The system can distinguish between:

- standing alarms that already exist in the GUI and alarm/notification list displays
- new alarms
- alarms that are cleared by the NE between resynchronizations.

This allows the system to incrementally update the GUI display and alarm notification/list displays to accurately indicate the subnetwork status to the user.

Alarm throttling

The Alarm Throttling feature enables you to limit the amount of autonomous messages and Critical autonomous messages that should be monitored for an NE.

Alarm throttling can be done on demand for an NE through the Alarm Throttling option on the NE's pop-up menu or be set up to occur automatically when the number of alarms exceed a specified threshold. An alarm throttle level between zero and 3,600 per hour can be specified in the Automatic Alarm Throttling window. The recommended initial level is 100 messages per hour (and this is the default). If an NE has been enabled for alarm throttling and the number of alarms in the NE exceeds the set level, the NE is automatically put on throttled, or partial, alarm monitoring.

The Alarm Throttling feature is useful during events, such as an initial network turn-up (or maintenance activity), where large numbers of messages are generated by an NE. Throttling alarm only allows alarms of a Critical priority to be displayed on the GUI, sent upstream to an OS, or retrieved via alarm queries. (Non-maintenance-related messages are not affected by alarm throttling and continue to be logged in the normal manner.)

Audible alarms/ events

The audible alarm provides an alternative way to alert the user to existing alarms or standing condition (SC) events. The following list provides an overview of audible alarm specifications:

- Audible alarms are generated at each system interface screen.
- To eliminate possible confusion, the characteristics of the audible alarm (that is, sound, duration, and interval between sounds) is common to all users of the host.
- Individual user interface users can enable or disable the audible alarm feature for their respective system user interface screens.
- The Map window contains the audible alarm symbol near the upper middle of the screen. The symbol is a speaker if the audible alarm is enabled, or a speaker with a slash through it if disabled.
- When the audible alarm is enabled, an audible alarm is initiated at the onset of each new alarm or SC event, with sound characteristics that correspond to the severity level of the most severe alarm/SC event. When there are multiple concurrent alarms or SC events of different severity levels, the sound emitted corresponds to the most severe unacknowledged prevailing alarm or SC event.
- Audible alarms last for a short duration and are repeated after a set time interval, until quieted by the user.

When you log off WaveStar SNMS and then log in again, the Audible Alarm feature is enabled. You can disable it The audible alarm sounds are initially loaded

with system default settings. These settings can be adjusted by the system administrator.

Alarm browser

The Alarm Browser lets you view alarms and clear messages for the NEs in your Target Group as they occur. Specifically, it captures *alarm*, *event*, and *clear* messages that are received from NEs in your Target Group and displays them in the Browsing Alarm Audit Log window on your workstation screen.

Alarm filtering

Alarm filtering is the selective removal of alarm messages from being forwarded to the GUI. Alarm filtering can be applied to reduce the number of alarms forwarded to the GUI caused by intermittent failure, or to filter symptomatic alarms associated with a reported signal failure, such as those that occur during a fiber cut. All alarms that are filtered out are logged in WaveStar SNMS and can be viewed through the Alarm Browser.

Types of Alarm Filtering

WaveStar SNMS uses three basic methods to reduce the number of alarms to be displayed:

- Aging—waiting for a pre-set time period to eliminate alarms that are caused by temporary failures (and are cleared within a time period shorter than the aging interval)
- Event-per-Time (EPT) Filtering—EPT, which is primarily an alarm reduction technique, filters transient condition (TC) events such as PM Threshold Crossing Alerts (TCAs). To forward all TC events, set the EPT count to zero. Both the time and number of TEs can be adjusted to only log TCs that exceed the expected normal level.
- Symptomatic Alarm Filtering—Symptomatic Alarm Filtering (SAF) filters out a set of pre-defined symptomatic NE alarms and standing condition (SC) events. The filtering is based on the Probable Cause (Condition Type) of the alarms and SC events received from all NEs, including the EMS-based alarms. The list of Probable Causes for SAF filtering is specified in the SAF filter parameter file, which is a UNIX flat file that can be edited using standard UNIX editing tools such as *vi*. Any alarm (including NE and EMS alarms) that match a Probable Cause specified in the SAF filter parameter file is filtered out. Alarms and events that are filtered out are not shown in the Map window or alarm lists. The SAF filter does not differentiate between NE types for the source of the alarms/events.

WaveStar SNMS provides a default set of pre-defined Probable Causes for alarms only in the SAF filter parameter file as follows:

SONET

- AIS-P (SONET Path Alarm Indication Signal Detected)
- AIS-L (SONET Line Alarm Indication Signal Detected)
- AIS (SONET Alarm Indication Signal Detected)
- RFI-P (SONET Remote Failure Indication-STS path)
- RFI-L (SONET Remote Failure Indication-line)
- PDI-P (SONET Remote Failure Indication-VT path)

SDH

- MSAIS (SDH MSect Alarm Indication Signal Detected)
- AUAIS (SDH AU Alarm Indication Signal Detected)
- MSRDI (SDH MSect Remote Failure Indication)
- HPRDI (SDH HP Remote Failure Indication)
- TRIBSDH (SDH Communications Failure)

The set of Probable Causes in the SAF filter parameter file can be modified by editing the file using standard UNIX editing tools.

The SAF filter is enabled by default and cannot be turned off by the user via the GUI. The WaveStar SNMS administrator enables or disables SAF filtering by changing the value of the *SNC_FM_SAF_FLAG* parameter in the */snc/etc/FM_rc* file (see the Adjusting Fault Management Parameters section in this chapter). WaveStar SNMS updates its SAF filtering based on the current Probable Causes specified in the SAF filter parameters file after the system administrator executes the **alarm_filter_update** command.

The Map window displays an “unfiltered view” of alarms, including symptomatic alarms filtered out by the SAF filter, by default. You can choose a “filtered view” of alarms, where the symptomatic alarms listed above in the explanation of the SAF feature are not displayed or counted in the alarm tallies, Map window view, and Alarm List.

Adjusting Aging and EPT Filtering Parameters

WaveStar SNMS provides several adjustable parameters for processing, collecting, and filtering alarm and event messages. These messages are grouped into three categories, as shown in the following table:

Table 4-1. Alarm and Event Categories

Message Type	Condition Status
Active alarms/ events	These alarms/events have not been cleared.
Standing condition alarms/ events	The alarm originator (for example, the NE) send a clear message when the condition no longer exists.
Transient condition events	The alarm originator (for example, the NE) do not send a clear message because the event does not change an NE's condition for an extended period of time.

The WaveStar SNMS fault management parameters are adjustable for each type of supported NE. The following parameters for alarm aging and EPT filtering can be adjusted.

- **Age Time—**This parameter is the number of seconds that an alarm or standing condition event is held while waiting for a clear message. Enabling this filter suppresses repeated alarm/clear message pairs, such as those that are generated by intermittent failures.

  Alarms that do not clear within the specified time are forwarded to the Map window and other windows that list alarm information, such as the Alarm Summary and Alarm List windows.

  Held alarms do not appear on the alarm windows and are not forwarded to a network surveillance system. These alarm messages are, however, available through the WaveStar SNMS Logs.

  The default value for all NE types and Probable Causes is 0 seconds (in effect, aging is "disabled."). The maximum value is 3600 seconds.

  However, the value of the Aging Filter flag, SNC_FM_AGING_FLAG, in the file */snc/etc/FM_rc*, which enables or disables the Aging Filtering feature itself, is 1 (enabled). See the Adjusting Fault Management Parameters section in this chapter.

- **Event-Per-Time (EPT) Count—**This parameter is the number of occurrences of a transient condition event that must be generated within the specified EPT Time before the event is flagged in the WaveStar SNMS event log and passed to an external operations system. The events that are counted must have matching condition codes, TIDs, and AIDs. The default count for all NE types and Probable Causes is 0. The maximum count is 3600.

- **EPT Time—**This parameter is the number of seconds that the system maintains an EPT count parameter for a recurring transient event. The default value for all NE types and Probable Causes is 0 seconds. The maximum value is 3600 seconds.

  Transient events that occur in the network can be viewed through the Transient Condition (TC) Event Browser available through a toolbar button on the Map window in the WaveStar SNMS GUI.

  The following events are shown in the Transient Condition Browser:

  - TL1-based messages—REPT-EVT with the "condeff" parameter equals "TC" (BWM/2.5G/25G_10G/OC192-4F/AllMetro)

    Only the TC events that exceed the Event-Per-Time (EPT) alarm filtering count are displayed; in other words, the REPT-EVT with "condeff" = "TC" and passing the EPT filter ("eptexceeded" = "1"). The EPT filter does not apply to other TC events, such as REPT-SW and REPT-PROTSW.

  - CMISE-based messages—Report Event message M-EVENT-REPORT with "condeff" (mapped API parameter) equals "TC" (400G).

The above alarm filtering parameters are maintained in a UNIX file that the WaveStar SNMS system administrator can edit (see Adjusting Fault Management Parameters).

Adjusting Fault Management Parameters

Certain parameter settings for alarm filtering are maintained in an editable UNIX file under */snc/etc/FM_rc*. The following table shows the environment variables for the filtering parameters, their default value, and their allowed values.

Table 4-2. Alarm Filtering Environment Parameters

Parameter	Environment Variable	Allowed Value	Default Value
Aging Filtering flag (to turn filtering by aging method on/off)	SNC_FM_AGING_FLAG	1=enabled 0=disabled	0 (disabled)
Symptomatic Alarm Filtering (SAF) flag to turn SAF filtering on/ off	SNC_FM_SAF_FLAG	1=enabled 0=disabled	1 (enabled)
Age Time	SNC_FM_DEF_AGE_TIME	0 to 3600 seconds	10 seconds
EPT Flag	SNC_FM_EPT_FLAG	1=enabled 2=disabled	2 (disabled)
EPT Count	SNC_FM_EPT_COUNT	0 to 3600	0 seconds
EPT Time	SNC_FM_DEF_STAT_TIME	0 to 3600 seconds	0 seconds
Auto Throttle Flag	SNC_FM_AUTO_THROTTLE_ FLAG	1=enabled 0=disabled	1 (enabled)
Manual Throttle Flag	SNC_FM_MANUAL_THROTTLE_ FLAG	1=enabled 0=disabled	0 (disabled)
Status Time	SNC_DEF_STAT_TIME	0 to 3600 seconds	3600 seconds
Throttle Level	SNC_FM_DEF_THROTTLE_LEVEL	0 to 3600 seconds	100 seconds

Turning the Age/Time and EPT filters on or off

To turn the Age/Time and EPT filters on or off in the file *FM_rc*, do the following:

1. Go to the directory */ems/etc* (for SNMS R. 4.0 or later releases) or the directory */snc/etc* (for SNMS releases before R. 4.0).

2. Edit (using the UNIX *vi* editor) the file *FM_rc* and change the following values:

   Change the value of the variable *SNC_FM_AGING_FLAG* to zero (0) to turn the Aging filter off (the default) or 1 to turn the Aging filter on.

   Search for and change the value of the variable *SNC_FM_EPT_FLAG* to zero (0) to turn the EPT filter off (the default) or 1 to turn the EPT filter on.

3. After modifying the *FM_rc* file, run the *alarm_filter_update* script to execute the update.

Changing Age/Time and EPT filter values

To change other Age/Time and EPT filter parameter values, do the following:

1. Go to the directory */ems/config/FM* (for SNMS R. 4.0 or later releases) or the directory */snc/config/FM* (for SNMS releases before R. 4.0).
2. Edit (using the UNIX *vi* editor) the file *FM.cfg* and change the following values:

   The first column is the Condition Type (the first row contains the default values for all Condition Types that are not in the first column).

   The second column is the timer value of the Age/Time filter for a Condition Type (the first row value is the default).

   The sixth column is the value for the count of the EPT filter.

   The seventh column is the value for the time period of the EPT filter.

3. After modifying the *FM.cfg* file, run the *alarm_filter_update* script to execute the update.

Changing the SAF filter parameter values

To change the SAF filter parameter values, do the following:

1. Go to the directory */ems/config/FM* (for SNMS R. 4.0 or later releases) or the directory */snc/config/FM* (for SNMS releases before R. 4.0).
2. Edit (using the UNIX *vi* editor) the file *FM_Conditions* and change the following values:

   The file lists the Condition Types that are to be filtered out. Modify as needed.

3. After modifying the *FM_Conditions* file, run the *alarm_filter_update* script to execute the update.

Tunring the SAF filter on or off

To turn the SAF filter on or off, do the following:

1. Go to the directory */ems/etc* (for SNMS R. 4.0 or later releases) or the directory */snc/etc* (for SNMS releases before R. 4.0).

2. Edit (using the UNIX *vi* editor) the file *FM_rc* and change the following values:

   Search and change the value of the variable *SNC_FM_SAF_FLAG* to 1 to turn the SAF filter on (the default) or to zero (0) to turn the SAF filter off.

3. After modifying the *FM_rc* file, run the *alarm_filter_update* script to execute the update.

Overload conditions and fault management

When WaveStar SNMS receives a large number of alarms and Threshold Crossing Alerts (TCAs), as during an alarm storm, and the volume of alarms/ messages exceeds a certain pre-set limit, the system is in an overload condition.

WaveStar SNMS is in overload mode when the number of outstanding (unprocessed) messages in the Fault Management Input Queue (buffer) exceeds the Overload Set Limit of 800 messages (the pre-set default value).

The Map window in the GUI has an Overload Indicator box that alerts the user to the overload condition.

When WaveStar SNMS is in an overload condition, it suspends processing of TCAs and other transient condition events, the collection of PM data and display of PM historical data, and certain on-demand and scheduled user activities (such as NE data backups, software downloads, and DNOs) until the overload condition ends.

When the number of messages in the Fault Management Input Queue drops below 200 messages, the system is no longer in overload and the system resumes processing of alarms/events, collection of PM data, and user-initiated transactions in the following order:

1. All transactions requested by users in “ad hoc” (on demand) mode.
2. All scheduled NE data backups.
3. All other scheduled tasks.

Alarm severity assignment profile management

An Alarm Severity Assignment Profile (ASAP) is used to assign an alarm severity level to a given entity within an NE, based on the probable cause of the alarm and the NE type.

Each entity can be assigned to a specific ASAP. Each ASAP consists of a set of probable causes with specified alarm severity levels. By default, entities of the same type are assigned to a default ASAP for that type.

The following table shows which ASAP capabilities are currently available through the GUI-based ASAP management functions, based on the NE type and the earliest NE release to which it applies, if available. In the table, “NA” means “Not Available”.

	BWM	2.5G	2.5G_10G	10G (STM64)	10G OC192-4F	400G
View an ASAP	1.2	2.0	3.0	1.0	1.0	2.0
Add an ASAP	1.3	NA	3.0	2.0	1.0	2.0
Modify an ASAP	1.2	2.0	3.0	1.0	1.0	2.0
Delete an ASAP	NA	NA	4.0	NA	NA	2.0
Rename an ASAP	1.3	NA	3.0	1.0	1.0	NA
Assign ASAP to AID	1.2	2.0	3.0	1.0	1.0	2.0
View ASAP Assign-ment for an AID	1.2	2.0	3.0	1.0	1.0	2.0
View all AIDs assigned to a profile	NA	NA	NA	NA	NA	2.0

NOTE:
For OLS 400G R. 2.0 NEs, ASAP provisioning only affects the alarms sent to WaveStar SNMS, not alarms sent to other OSs, including the Craft

Interface Terminal (CIT). ASAP provisioning for OLS 400G R. 3.0 NEs affects all alarms generated by the NE and sent to all OSs.

Alarm severity assignment for AllMetro NEs

AllMetro NEs do not support the ASAP feature. Alarm severity assignment is done by direct assignment of the alarm severity for an AID or group of AIDs. Alarm severity provisioning on an AllMetro NE can be done for the following entities:

- Supervisory channels
- Incoming port (OTU IN)
- Environment ports

Alarm severity provisioning for AllMetro environmental points can be done at the port level through the GUI or by issuing TL1 commands in Cut-Through mode. The TL1 commands *RTRV-ATTR-ENV {TID}{AID}* and *SET-ATTR-ENV{TID}{AID}* allow you to retrieve and set the alarm message and notification code for the AID for the specified AID.

For details about use of TL1 commands to provision alarm severity assignment in the AllMetro NE, consult the AllMetro documentation.

Example of an ASAP entry

A Loss of Signal (LOS), which can be a probable cause of an alarm on an Incoming DS3 Port (the entity) of a BWM NE, may be assigned an alarm severity level of Critical in the ASAP associated with the DS3 port entity type.

NOTE:
For an explanation of specific probable causes for an NE type, refer to the related NE documentation.

Types of ASAPs

There are different types of ASAPs associated with different types of equipment entities. An ASAP can only be assigned to each entity of the same type. Each ASAP/entity type has a specific list of applicable probable alarm causes associated with it.

Example of a profile type

In the OLS 400G, a shelf is a specific entity in an NE that generates its own set of alarms for which there are probable causes. Therefore, a shelf can be a Profile Type for which an ASAP exists or can be created.

Parts of an ASAP

Each Profile Type for an entity in an NE contains:

- A list of probable causes (condition types)
- The service affecting state of each probable cause
  - Service Affecting (SA)
  - Non-Service Affecting (NSA)
  - Service Interrupting (SI)
- The assigned alarm level values for each probable cause
  - Critical (CR) for SONET or Prompt (PR) for SDH
  - Major (MJ) for SONET or Deferred (DF) for SDH
  - Minor (MN) for SONET or Deferred (DF) for SDH
  - No Alarm (NA) for SONET and SDH
  - No Report (NR) for SONET and SDH

The display of alarm level values when adding a new ASAP depends on user selection of SONET or SDH alarm severity levels through the Fault panel of the Preferences option through the GUI.

Refer to the TL1 documentation for the *ED-ASAP-PROF* command for the allowed alarm severity levels for each condition type.

ASAP options

WaveStar SNMS allows you to:

- Retrieve and view ASAPs for an NE
- Add a new ASAP for an NE
- Modify an existing ASAP
- Delete an ASAP
- Rename an existing ASAP (except for default ASAPs)
- View ASAP assignments for NE entities

Adding an ASAP

Each entity/AID (Profile Type) has a default ASAP. When it is first created, a new ASAP inherits the same alarm severity levels as those set up in the default ASAP for a Profile Type. The alarm severity levels for each item in the new ASAP can remain the same as the default ASAP, or be modified as needed. The new ASAP is given a new Profile Name. The newly created ASAP can be assigned to a specific AID (entity) in an NE.

NOTE:
When adding a new ASAP for an NE, the Profile Names “Default” or “default” cannot be used.

Modifying an ASAP

Any ASAP can be modified, including the default ASAP for a Profile Type in an NE, by changing the alarm severity assignments for probable causes in the ASAP.

Deleting an ASAP

Once created, you can delete an ASAP. However, you cannot delete an ASAP that is currently assigned to an entity (AID) in an NE, until you remove the assignment from the AID. You cannot delete the default ASAP for a Profile Type in an NE.

Renaming an ASAP

Once created, you can change the profile name of an inactive ASAP that is not a default ASAP.

Assigning an ASAP to an NE’s AID

Each AID in an NE may generate specific types of alarms. The severity of the alarms with different probable causes generated by each NE’s AID depends on the ASAP assigned to the AID. Each NE’s AID is assigned to a default ASAP. You can assign an ASAP that you created to an AID. Each AID in an NE can be associated with a different ASAP.

Viewing ASAP assignments for NE entities

Each AID may generate specific types of alarms. The alarm severity level of each probable cause for an NE entity depends on the ASAP assigned to the AID. You can select an ASAP for a Profile Type in an NE and see which entities are assigned to the ASAP.

Transient event condition browser

WaveStar SNMS provides a GUI-based browser that allows you to display a list of ransient condition (TC) events that occur in the host’s NE network. Transient events do not require a clear message by the NE because they do not change the NE’s condition over an extended period of time.

Administering fault management functions

WaveStar SNMS allows you to set up or modify several aspects of alarm reporting for the NEs in your network at the same time, using a single GUI window that can be accessed from the Fault menu option on the Map window toolbar. This GUI window allows you to:

- assign severity levels to environmental alarms generated by miscellaneous discretes on the NE (such as “door open” alarms). Severity levels for these types of alarms are set up by assigning an Alarm Severity Assignment Profile (ASAP) to the miscellaneous discrete AID and selecting the alarm severity level
- provision facility and equipment alarm delays
- provision facility and equipment alarm clearing delays
- enable or disable audio/visual alarm indicators
- allow or inhibit the receipt of autonomous messages (**Note:** this option is currently available only for OLS 400G and BWM R. 3.0 NEs)

Related tasks

See the Alarm Management chapter for related tasks.

WaveStar SNMS Logs

Overview

WaveStar SNMS keeps track of certain information regarding system performance and actions. This information is stored in logs, and may be filtered and viewed by the user. The process of collecting, storing, and displaying this information is called Log Management. The following logs are maintained:

- **Network Alarm/Event Log—**This log stores a history of all the alarms and events received from the network elements as a result of unexpected behaviors by an NE.
- **Network Notifications Log—**This log stores notifications from NEs on database changes, protection switching, and other NE-related activities.
- **Network Command/Response Log—**This log stores all commands and responses, except retrieval commands and responses (for example, RTRV-rr) that are originated from and received by SNMS. The user ID information and user interface information (GUI, cut-through, TCP/IP, or dial-up) are also logged.
- **EMS Alarm/Event Log—**This log stores alarms originated by system on all system hardware and/or software-related unexpected behaviors detected by WaveStar SNMS itself.
- **EMS Activity Log—**This log displays information on selected WaveStar SNMS activities for one or more users.

Log Management provides the following four functions:

- **Logging—**logs messages and data into the WaveStar SNMS database or a flat file.
- **Browsing—**provides GUI functionality for the user to browse the messages and data.
- **Filtering—**filters log data to provide only desired data.
- **Purging—**purges old log messages from the WaveStar SNMS database or temporal log files generated by system modules.

Network alarm/ event log

Use the Network Alarm/Event Log to view, save, and print important alarm and event information. WaveStar SNMS logs and stores various alarms and non-alarm events as listed in the appropriate NE documentation.

Clear messages for an OLS 400G NE are always shown as alarms in the log.

The user can filter the Network Alarm/Event Log on certain parameters, including start date/time, end date/time, TID, aggregate, EPT, alarm/event type, and severity. The maximum number of days for which alarm/event data can be displayed is 45.

Network notifications log

WaveStar SNMS logs the following notifications/events in the Network Notifications Log:

- The completion (or noncompletion) of an automatic database backup (from primary NVM to secondary)
- Any change in the WaveStar SNMS database
- The autonomous removal from service of an administrative or data link
- Automatic and manual (user-initiated) equipment protection switches, synchronization mode switches, and system timing reference switches.

The user can filter the Network Notification Log on certain parameters, including start date/time, end date/time, TID, aggregate, and notification type. The maximum number of days for which network notification data can be displayed is 45.

Network command/ response log

All commands that are formulated by internal subsystems as a result of a user operation from the GUI are logged to the Command/Response Log. (The one exception is retrieval commands, which are left out for performance reasons.) WaveStar SNMS provides a user interface parameter for each logged command from all interface types. The possible values for the parameter are GUI, cut-through, TCP/IP, and dial-up.

The system administrator is allowed access to all commands/responses, while users are able to view self-originated commands and responses. The commands are displayed in the order they were received by WaveStar SNMS, each command followed by its response. (If a command did not receive a response, the display indicates this with the entry “time out.”)

The user can filter the Network Command/Response Log on certain parameters, including start date/time, end date/time, TID, and aggregate. The system administrator can filter on these same parameters, plus two more - command interface and user login ID. The maximum number of days for which network command/response data can be displayed is 7.

EMS alarm/event log

WaveStar SNMS logs the following system failures to the WaveStar SNMS Alarm Log:

- 802.3 LAN interface failure
- Disk I/O failure
- Informix EDR agent failure
- File system filling to over 85%
- File system full (over 97%)

- Database space filling to over 85%
- Database space full (over 97%)

The following table shows the system failure information logged by WaveStar SNMS to the Alarm/Event Log.

Table 4-3. System Failure Information in WaveStar SNMS Alarm Log

Parameter	Values	Description
Alarm/Event Type	Alarm	for alarms only
Alarm ID	1 - 999999	WaveStar SNMS assigned alarm identification number
Date of Occurrence	YYYY-MM-DD (month-day)	
Time of Occurrence	HH:MM:SS (hours:minutes:seconds)	
Category	Equipment/ Processing Error	
Alarm Issue Point	<=20 characters	LAN/Disk IO/File System/Database
Effect on Service	NSA	
Severity	CR/MJ/CL	
Probable Cause	Text String (see WaveStar SNMS alarm list)	condition type
Description	Text String (see WaveStar SNMS alarm list)	description of the failure conditions

The user can filter the WaveStar SNMS Alarm Log on the start date/time and end date/time parameters. The maximum number of days for which alarm log data can be displayed is 45.

EMS activity log

All user activities that are executed through the GUI as well as system activities are stored in the EMS database and logged in the EMS Activity Log. By using the Log Management feature, the Activity Log can be browsed by the user and the information saved and printed.

The user can filter the Activity Log on certain parameters including start date/time, user, activity type, and selected activity. The maximum number of days for which activity can be displayed is seven.

The activities are listed in the order they were received by WaveStar SNMS with the requested information.

The onset and termination of system overload conditions are also logged in the Activity Log.

Related tasks

See the Alarm Management chapter for related tasks.

Performance Management Concepts

5

Introduction

Purpose

This chapter provides general information about the Performance Management features of WaveStar SNMS.

Objectives

This chapter provides information to perform the following:

- Enable the Performance Monitoring (PM) feature for PM data collection
- Set the threshold PM parameters for data collection
- Administer storing of PM data
- View PM data
- Generate PM data reports
- Administer PM parameters
- Add, modify, and delete PM profiles
- View PM profile assignments
- Assign a PM profile to an entity (AID) in an NE

Contents

This chapter discusses the following topics:

Background

Overview

The Performance Management features of the system allows users to collect Performance Monitoring (PM) data from certain NE types. Users can specify the NEs and reporting of PM data from either a facility or specific entity (AID) from which PM data is collected. The collected PM data can be viewed online through the GUI or exported to external systems for analysis and report generation.

Performance Monitoring Capabilities

Overview

The Performance Management feature allows the system to retrieve, store, and export Performance Monitoring (PM) data from OLS 400G R.2.0 (and later), BWM R.1.3 (and later) SDH interfaces, TDM 10G (STM-64) SDH interfaces, 2.5G_10G R. 3.0 (and later), AllMetro R. 1.0, and TDM 10G (OC-192) 4-Fiber R. 1.0 (or later) NEs. The system retrieves intermediate and terminal path SONET/SDH bin and line PM data from BWM R. 2.0 (and later) NEs. This feature also allows you to retrieve, store, and export PM data from FT-2000 LCT R. 4.0 NEs. The PM feature, which is enabled or disabled through the GUI, allows you to initiate performance monitoring of managed NEs. PM data can be collected from none, some, or all NEs in the network. You can specify, on a per-NE basis, the type(s) of interfaces from which to collect PM data for analysis. PM data can be turned on or off for each NE and can be collected in 15-minute and/or 1-day time intervals. PM data can be viewed online through the GUI or exported to an external reports system for more sophisticated reports and analysis.

The system also supports remote administration of performance parameters and thresholds through the Cut-Through feature. For the OLS 400G CMISE protocol, the system provides GUI windows to configure OLS 400G performance parameters and thresholds. Performance exceptions are logged from the NEs as Threshold Crossing Alerts (TCAs) each time the administered threshold for these events is exceeded.

Enabling the PM feature

The PM feature must be globally enabled before PM data can be collected from NEs. If the PM feature is not enabled globally, PM data cannot be collected even if PM data collection is turned on for an NE. When the PM feature is globally enabled, you have the option of choosing PM data reports for later viewing from an NE's facility or specific entity (AID). The default is reporting of PM data by facility.

When the PM feature is globally enabled, the system periodically polls each NE that has PM data collection enabled for PM data.

PM data collection

PM data collection can be enabled or disabled for an NE. You can also select the type of PM data to be collected (15-minute, 1-day, or both) for each port type on the NE, or disable PM data collection for a port type.

NEs are normally polled every two hours. Data polling is done by the system in such a way as to avoid overwhelming the network with PM data traffic.

Loss of communications

If connectivity is lost to an NE during PM data polling, upon re-establishing the connection, the system resumes data collection, and polls for the oldest PM data not yet collected, based on the value of the *OLDEST_TO_POLL* variable, *.pm_global* file, found in the */snc/.pm* directory, which can be changed by the system administrator.

For example, if the value of the *OLDEST_TO_POLL* variable is set to four hours and connectivity between an NE and the system is lost for three hours, the system resumes polling for PM data that is up to four hours old if it has not already been collected.

Suspension of PM data collection

PM data collection is suspended during an alarm storm. WaveStar SNMS resumes PM data collection after the alarm storm has subsided.

Initialization of PM data registers

For the selected NE, the PM feature allows you to reset (initialize) the digital PM registers for:

- All current 15-minute digital PM data (Bin A)
- All current 1-day digital PM data (Bin B)
- Both 15-minute and 1-day current PM data

At the NE level, the PM feature allows you to reset (initialize) the digital PM registers for:

- All Supervisory channels in the Optical Line
- All Optical Translator Units (OTUs) in the Optical Line
- Both (All Supervisory Channels and All OTUs in the Optical Line

On an Optical Line basis, the PM feature allows you to reset (initialize) the digital PM registers for:

- All Supervisory channel digital PM bins
- All associated Optical Translator Port Signals (OTPSs)
- Both (All Supervisory channel and all associated OTPSs)

At the Bay level, the PM feature allows you to reset (initialize) the digital PM registers for:

- All OTPSs on all OTUs' digital PM bins (15-minute, 1-day, or both)

On an OTU level, the PM feature allows you to reset (initialize) the digital PM registers for:

- Both OTPSs' digital PM bins (15-minute, 1-day, or both)

On an OTPS level, the PM feature allows you to reset (initialize) the digital PM registers for:

- The OTPS' digital PM bins (15-minute, 1-day, or both)

Setting the start time for 1-day PM data collection

For the selected NE, the PM feature allows you to view and then reset (if necessary) the hour of the start time for collection of 1-day PM data.

Storing PM data

The system stores collected PM data in the WaveStar SNMS database. Each PM database record contains a:

- TID and AID of the NE from which the PM data was collected
- 15-minute or 1-day PM data indicator
- NE interface type from which PM data was collected
- time/date of PM data collection
- validity of PM data
- type of PM data
- value of PM data
- PM threshold exceeded indicator (in other words, whether the PM data collection exceeded the established threshold during PM data collection). **Note:** this variable is not applicable to OLS 400G NEs.

The PM data collected can be invalid if the NE date/time was reset during PM data collection or if the NE PM data register overflowed during the collection interval.

PM data can be stored in the system for 1 to 30 days. The default retention period for 15-minute data is 30 days. The default retention period for 1-day data is 30 days. The data retention period for both 15-minute and 1-day PM data can be specified through the Global PM Management option on the GUI.

PM files are kept for the set retention period, unless the files have to be overwritten due to insufficient data storage space. The system automatically deletes any PM data file when it is older than the retention period or there is a lack of storage space. If there is a lack of data storage space, the system deletes PM data files, starting with the oldest file first, until the storage problem is resolved.

When PM data is deleted, WaveStar SNMS puts an entry into the Alarm Log indicating that PM data has been deleted.

Deleting an NE from WaveStar SNMS

Any PM data associated with an NE is removed from the WaveStar SNMS database when that NE is deleted from WaveStar SNMS.

Viewing PM data

The system allows you to view the "raw" PM data which is either stored in the WaveStar SNMS database or not yet collected from the NE. You can specify which PM data to view using selection criteria such as:

- Current or historical PM data
- Date/time of historical PM data
- The type of PM data (15-minute or 1-day)
- The NE interface type

The date is specified for 1-day data. The date and time of day is specified for 15-minute data.

Generating PM data reports

PM data collected by the system can be automatically downloaded by Lucent Technologies' Integrated Transport Management Dynamic Network Analyzer (ITM-DNA), an external PC-based system which can produce various types of user-defined reports. The downloaded PM data that is stored in the ITM-DNA database can be used to generate reports in a variety of formats, including tabular reports, line graphs, and bar graphs.

Types of PM data

The system can be set up to collect PM data from specific NE interfaces and the Optical Translator Unit (OTU).

The following table shows the interfaces (facility types) by NE type from which PM data can be collected.

NE Types	Applicable Facility Types
OLS 400G	Optical Channels, Optical Lines, Supervisory Channels, Optical Translator Port Signals (OTPS)
BWM R1.3	STM16, STM4, STM1, T3
BWM R2.0	STM64, STM16, STM4, STM1, VC3[1] , VC4[2] , VC44c[2] , VC416c[2] , OC192 , OC48 , OC12, OC3 , T3
BWM R2.1	STM64, STM16, STM4, STM1, VC3[1] , VC4[2] , VC44c[2] , VC416c[2] , OC192 , OC48 , OC12, OC3 , EC1, T3
BWM R3.0-R3.1	STM64, STM16, STM4, STM1, VC3[1], VC4[2], VC44c[2] , VC416c[2] , OC192, OC48, OC-12, OC3, EC1, STS1, STS3c, STS12c, STS48c, T3
STM-64 R1.0-R1.1	STM64, STM16, STM1, STM1E
STM-64 R2.0	STM64, STM16, STM4, STM1, STM1E
STM-64 R2.1	STM64, STM16, STM4, STM1, STM1E, VC3[1], VC4[1], VC44c[1], VC416c[1]
FT-2000 LCT R4.0	OC48, OC12, OC3, EC1, STS1[1] , T3
2.5G_10G R3.0	OC192, OC48, OC12, OC3, EC1, T3, STS48c[2] , STS12c[2], ST3c[2], STS1[2]
2.5G_10G R4.0	OC192, OC48, OC12, OC3, EC1, T3, STS48c[1] , STS12c[1] , ST3c[1] , STS1[1]
AllMetro OLS R1.0	Optical Channels, Optical Lines, Supervisory Channels, Optical Translator Port Signals (OTPS)

[1] Both Terminating Path and Mid-Path PM data are supported.

[2] Only Mid-Path PM data is supported.

Refer to the respective NE hardware documentation for details about the types of PM data that can be generated from each of these interfaces.

NE PM data administration

The PM Data Administration window on the GUI allows you to administer three categories of NE PM data related to the OLS 400G:

- digital PM threshold settings
- analog PM threshold settings
- baseline value calculations

PM threshold values can only be provisioned for an OLS 400G NE through the PM Data Administration window. For other NE types, PM threshold values must be set by issuing TL1 commands via the Cut-Through window.

Digital PM data threshold settings

For the selected NE, the PM data administration feature allows you to retrieve and set the 15-minute and/or 1-day threshold values for PM data collection for the specific parameters listed on the GUI window.

Analog PM data threshold data settings

For the selected NE, the PM data administration feature allows you to display and change the high and low threshold values for signal power received and/or transmitted for the various interfaces.

Recalculation of baseline signal power

The PM data administration feature allows you to set, in the NE, the current baseline value of NE facilities associated with analog PM parameters. To establish the reference point for the high and low threshold values for signal power, the PM feature allows you to recalculate (set) the current baseline value for the signal power received, transmitted, or both. This may be required, for example, when a new NE is brought into service.

Administering PM parameters

Some of the parameters that are used by the system to manage the PM feature, such as the data retention period or the age of the data collected during polling, can be manually changed by the system administrator by editing the value of the corresponding variable in the *.pm_global* file, which is found under */snc/.pm*.

The following table shows the PM variables that can be edited, with their default values.

Table 5-1. PM Feature Variables

Variable	Description	Default Value
PM_COLLECT_STATUS	The current global setting of the PM feature. Value is On or Off.	Off
RETENTION_FOR_PM	The global data retention period for 15-minute PM data.	2 (days)
RETENTION_FOR_DAY	The global data retention period for 1-day PM data.	30 (days)
PM_POLLING_FREQ	The frequency that the system polls the NEs for PM data in a session. Allowed value is 2 to 6 (hours).	2 (hours)
PM_OLDEST_TO_POLL	The age of the oldest PM data that can be collected by the system from the NEs.	4 (hours)
PM_MAX_FILE_POLL	The maximum number of PM data reports for which the system can poll NEs in one session.	user-defined
TOTAL_FILE_SYSTEM	The total number of system host machines for which PM data is being collected.	1

Exception reporting

The system provides exceptions by logging Threshold Crossing Alerts (TCAs) received from the NEs. TCAs, in the form of report events, are generated every time an administered performance threshold is exceeded in the NE. In addition, the system EPT Threshold capability flags the TCA rate when it exceeds the system threshold.

TCAs and alarms are stored in the WaveStar SNMS database and are available for online queries through the Network Alarm/Event Log.

PM profile management

A Performance Management (PM) profile is used to assign a threshold value for the various types of PM data that can be generated by an NE, to a given entity within the NE to establish, for example, threshold limits for TCAs to be generated by an NE.

By default, each entity is assigned to one default PM profile of more than one PM profile type.

The following table shows which PM profile capabilities are currently available through the GUI-based PM profile management functions, based on the NE type and the earliest NE release to which it applies, if available. In the following table, “NA” means “Not Available”.

	BWM	2.5G	25G_10G	STM64	OC192-4F	400G
View an PM/TCA Profile	1.3	2.0	3.0	2.0	NA	2.0
Add an PM/TCA Profile	2.0	NA	3.0	2.0	NA	NA
Modify an PM/TCA Profile	1.3	NA	3.0	2.0	NA	2.0
Delete an PM/TCA Profile	2.0	NA	3.0	2.0	NA	NA
Assign PM/TCA Profile to AID	1.3	NA	3.0	2.0	NA	NA
View PM/TCA Profile Assignment for an AID	1.3	2.0	3.0	2.0	NA	2.0
View all AIDs assigned to a PM/TCA profile	2.0	NA	3.0	2.0	NA	NA

PM profile types

There are different types of PM profiles associated with different types of equipment entities. Each PM Profile Type has an associated set of PM parameters with related threshold values.

The following table lists the available PM Profile Types and the earliest NE releases supported for each profile type. In the table, a plus (+) sign indicates that the Profile Type is supported for releases following the earliest release supported.

PM Profile Types	NE Rels
PHYSICAL	BWM R1.3, 25G_10G R3.0-, OC192-4F R2.0-
SECTION-LINE	BWM R1.3, 25G_10G R3.0-, OC192-4F R2.0-
PATH	BWM R1.3, 25G_10G R3.0-, OC192-4F R2.0-
DS3.	BWM R1.3, 25G_10G R3.0-, OC192-4F R2.0-
SDH RS-MS (Regenerator Section - Multiplex Section)	BWM R1.3
SDH HOVC. (High Order Virtual Container path)	BWM R1.3

PM profile options

WaveStar SNMS allows you to:

- Retrieve and view PM profiles for an NE
- Add a new PM profile for an NE
- Modify an existing PM profile
- Delete a PM profile
- View PM profile assignments for NE entities

Adding a PM profile

Each PM Profile Type has a default profile. When it is first created, a new PM profile inherits the same threshold values as those set up in the default profile for a Profile Type. The threshold values for each item in the new profile can remain the same as the default one for the Profile Type, or be modified as needed. The

new profile is given a new Profile Name. The newly created profile can be assigned to a specific AID (entity) in an NE.

WaveStar SNMS allows a maximum number of profiles (default and newly created). If you attempt to add a new profile and it exceeds the maximum number of profiles allowed for a given profile type, the request is denied by WaveStar SNMS.

The maximum number of profiles allowed for each Profile Type of an NE (applicable to the BWM and 2.5G_10G NE types) are as follows:

- The system supports up to 10 Physical profiles.
- The system supports up to 30 port level profiles (a total of section-line and SDH RS-MS profiles cannot exceed 30).
- The system supports up to 80 path level profiles (in other words, the number of path profiles, SDH HOVC paths, and number of DS3 profiles cannot exceed 80).

The total number of profiles defined above apply to both the system default profiles and the profiles created by the user.

Modifying a PM profile

WaveStar SNMS allows you to modify the threshold values for parameters in the default profile of each Profile Type. You can also modify the PM Profile Name of an inactive profile (one that is not currently assigned to an NE's AID). You cannot modify the name of the default profile for a given Profile Type.

If you modify a PM profile, it erases all of the PM profile threshold values provisioned for individual threshold parameters.

Deleting a PM profile

Once created, you can delete a PM profile. However, you cannot delete a PM profile that is currently active (assigned to an entity (AID) in an NE), until you remove the assignment from the AID. You cannot delete the default profile for a Profile Type in an NE.

Assigning a PM profile to an NE's AID

The default PM/TCA profile or one that you have created can be assigned by selecting the PM Profile Name of the profile when provisioning port parameters for a specific port AID (entity) via the Provisioning function in the GUI, if this parameter is provisionable for a given NE type and port type/interface. The field parameter name is usually "TCA Profile". Each AID in an NE can be associated with a different PM/TCA profile.

Viewing PM profile assignments for NE entities

WaveStar SNMS allows you, through a GUI-based function, to see which entities (AIDs) in a given shelf of an NE are assigned to a specific profile.

Related tasks

See the Performance Management chapter for related tasks.

Glossary

6

Introduction

Purpose

This chapter provides a glossary of terms and a list of acronyms related to WaveStar SNMS.

Contents

This chapter contains the following:

Glossary

Overview

The following is a glossary of terms that are related to WaveStar SNMS.

Numerics

0×1 Line Operation
: 0×1 means unprotected operation. The connection between network elements has one bidirectional line (no protection line).

1+1 Line Protection
: A protection architecture in which the transmitting equipment transmits a valid signal on both the working and protection lines. The receiving equipment monitors both lines. Based on performance criteria and OS control, the receiving equipment chooses one line as the active line and designates the other as the standby line.

1×N Equipment Protection
: 1×N protection pertains to N number of circuit pack/port units protected by one circuit pack or port unit. When a protection switch occurs, the working signals are routed from the failed pack to the protection pack. When the fault clears, the signals revert to the working port unit.

1xN Multi-Cast Cross-Connection
: Consists of N one-way cross-connections from an input tributary to N output tributaries. 1:N Multi-cast (for N>2) is most commonly associated with providing video services.

A

Absent (ABS)
: Used to indicate that a given circuit pack is not installed.

Access Identifier (AID)
: A technical specification for explicitly naming entities (both physical and logical) of an NE using a grammar comprised of ascii text, keywords, and grammar rules.

Active (ACT)
: Used to indicate that a circuit pack or module is in-service and currently providing service functions.

Active Path
: The path that is currently carrying the service in a circuit that is protected at the path level.

Add/Drop Multiplexer (ADM)
The term for a synchronous network element capable of combining signals of different rates and having those signals added to or dropped from the stream.

Aggregate
A user-defined grouping of NEs. It most commonly consists of NEs located in a central office (CO) and the subnetworks to which they belong.

Alarm
Visible or audible signal indicating that an equipment failure or significant event/condition has occurred.

Alarm Correlation
The search for a directly-reported alarm that can account for a given symptomatic condition.

Alarm Cut-Off (ACO)
A button on the user panel used to silence audible alarms.

Alarm Cut-Off and Test (ACO/TST)
The name of a pushbutton on the user panel used to silence audible alarms.

Alarm Indication Signal (AIS)
A code transmitted downstream in a digital network that indicates that an upstream failure has been detected and alarmed if the upstream alarm has not been suppressed.

Alarm Severity
An attribute defining the priority of the alarm message. The way alarms are processed depends on the severity.

Alarm Suppression
Selective removal of alarm messages from being forwarded to the GUI or to network management layer OSs.

Alarm Throttling
A feature that automatically or manually suppresses autonomous messages that are not priority alarms.

Alternate Mark Inversion (AMI)
A line code that employs a ternary signal to convert binary digits, in which successive binary ones are represented by signal elements that are normally of alternative positive and negative polarity but equal in amplitude and in which binary zeros are represented by signal elements that have zero amplitude.

American Standard Code for Information Interchange (ASCII)
A standard 7-bit code that represents letters, numbers, punctuation marks, and special characters in the interchange of data among computing and communications equipment.

Association
A logical connection between manager and agent through which management information can be exchanged.

Asynchronous
The essential characteristic of time-scales or signals such that their corresponding significant instants do not necessarily occur at the same average rate.

Asynchronous Transfer Mode (ATM)
A high-speed transmission technology characterized by high bandwidth and low delay. It utilizes a packet switching and multiplexing technique which allocates bandwidth on demand.

Attribute
Alarm indication level: critical, major, minor, or no alarm.

Autolock
Action taken by the system in the event of circuit pack failure/trouble. System switches to protection and prevents a return to the working circuit pack even if the trouble clears. Multiple protection switches on a circuit pack during a short period of time cause the system to autolock the pack.

Automatic (AUTO)
One possible state of a port or slot. When a port is in the AUTO state and a good signal is detected, the port automatically enters the IS (in-service) state. When a slot is in the AUTO state and a circuit pack is detected, the slot automatically enters the EQ (equipped) state.

Automatic Protection Switch
A protection switch that occurs automatically in response to an automatically detected fault condition.

Autonomous Message
A message transmitted from the controlled Network Element to the ITM-SC which was not a response to an ITM-SC originated command.

B

Backup
The backup and restoration features provide the capability to recover from loss of NE data because of such factors as human error, power failure, NE design flaws, and software bugs.

Bandwidth
The difference in Hz between the highest and lowest frequencies in a transmission channel. The data rate that can be carried by a given communications circuit.

Baud Rate
Transmission rate of data (bits per second) on a network link.

Bidirectional Line
A transmission path consisting of two fibers that handle traffic in both the transmit and receive directions.

Bidirectional Line-Switched Ring (BLSR)
A bidirectional ring in which protection switching is accomplished by switching working traffic into protection time slots in the line going in the opposite direction around the ring.

Bidirectional Ring
A ring in which both directions of traffic between any two nodes travel through the same network elements (although in opposite directions).

Bidirectional Switch
Protection switching performed in both the transmit and receive directions.

Bipolar 3-Zero Substitution (B3ZS)
A line coding technique that replaces three consecutive zeros with a bit sequence having special characteristics accomplishing two objectives: First, this bit sequence accommodates the ones density requirements for digital T3 carrier; Second, the sequence is recognizable at the destination (due to deliberate bipolar violations) and is removed to produce the original signal.

Bipolar 8-Zero Substitution (B8ZS)
A line coding technique that replaces eight consecutive zeros with a bit sequence having special characteristics accomplishing two objectives: First, this bit sequence accommodates the ones density requirements for digital T1 carrier; Second, the sequence is recognizable at the destination (due to deliberate bipolar violations) and is removed to produce the original signal.

Bit
The smallest unit of information in a computer, with a value of either 0 or 1.

Bit Error Rate (BER)
The ratio of error bits received to the total number of bits transmitted.

Bit Error Rate Threshold
The point at which an alarm is issued for bit errors.

Bit Interleaved Parity-N(BIP-N)
A method of error monitoring over a specified number of bits (BIP-3 or BIP-8).

Blank (BLK)
The status of a circuit pack slot that contains a bus extender (blank) circuit pack.

Board Controller Local Area Network (BCLAN)
: The internal local area network that provides communications between the line and board controllers on the circuit packs associated with a high-speed line.

Bridge Cross-Connection
: The setting up of a cross-connection leg with the same input tributary as that of an existing cross-connection leg. This forms a 1:2 bridge from an input tributary to two output tributaries.

Broadband Communications
: Voice, data, and/or video communications at greater than 2 Mb/s rates.

Building Integrated Timing Supply (BITS)
: A single clock that provides all the DS1 and/or composite clock timing reference to all other clocks in that building.

Byte
: Refers to a group of eight consecutive binary digits.

C

C-Bit
: A framing format used for DS3 signals produced by multiplexing 28 DS1s into a DS3. This format provides for enhanced performance monitoring of both near-end and far-end entities.

Cell Relay
: Fixed length cells. For example, ATM with 53 octets.

Central Office (CO)
: A building where common carriers terminate customer circuits.

Channel
: A sub-unit of transmission capacity within a defined higher level of transmission capacity.

Channel State Provisioning
: A feature that allows a user to suppress reporting of alarms and events during provisioning by supporting multiple states (automatic, in-service, and not monitored) for VT1.5 and STS-1 channels.

Circuit
: A set of transmission channels through one or more network elements that provides transmission of signals between two points, to support a single communications path.

Clear Channel (CC)
: A digital circuit where no framing or control bits are required, thus making the full bandwidth available for communications.

Closed Ring Network
A network formed of a ring-shaped configuration of network elements. Each network element connects to two others, one on each side.

Coding Violation (CV)
A performance monitoring parameter indicating bipolar violations of the signal have occurred.

Collocated
System elements that are located in the same location.

Command Group
An administrator-defined group that defines commands to which a user has access.

Concatenation
A procedure whereby multiple virtual containers are associated one with each other, resulting in a combined capacity that can be used as a single container across which bit sequence integrity is maintained.

Consultative Committee for the International Telephone and Telegraph (CCITT)
International Telephone and Telegraph Consultative Committee — An international advisory committee under United Nations' sponsorship that has composed and recommended for adoption worldwide standards for international communications. Recently changed to the International Telecommunications Union Telecommunications Standards Sector (ITU-TSS).

Co-Resident
A hardware configuration where two applications can be active at the same time independently on the same hardware and software platform without interfering with each others functioning.

Correlation
A process where related hard failure alarms are identified.

Craft Interface Terminal (CIT)
The user interface terminal used by craft personnel to communicate with a network element.

Critical (CR)
Alarm that indicates a severe, service-affecting condition.

Cross-Connection
Path-level connections between input and output tributaries or specific ports within a single NE. Cross-connections are made in a consistent way even though there are various types of ports and various types of port protection. Cross-Connections are reconfigurable interconnections between tributaries of transmission interfaces.

Crosstalk
An unwanted signal introduced into one transmission line from another.

Current Value
The value currently assigned to a provisionable parameter.

Cut-Through
A capability that allows a user to utilize a network element's native command set (CIT or TL1 as appropriate) to communicate with network elements in the ITM SNC domain.

D

Data
A collection of system parameters and their associated values.

Database Administrator
A user who administers the database of the application.

Data Communications Channel (DCC)
The embedded overhead communications channel in the synchronous line, used for end-to-end communications and maintenance. The DCC carries alarm, control, and status information between network elements in a synchronous network.

Data Communications Equipment (DCE)
The equipment that provides signal conversion and coding between the data terminating equipment (DTE) and the line. The DCE may be separate equipment or an integral part of the DTE or of intermediate equipment. A DCE may perform other functions usually performed at the network end of the line.

Data Terminating Equipment (DTE)
The equipment that originates data for transmission and accepts transmitted data.

DDM-1000
Lucent Technologies' Dual DS3 Multiplexer — A digital multiplexer that multiplexes DS1, DS1C, or DS2 signals into a DS3 signal or a 90 Mb/s or 180 Mb/s optical signal.

DDM-2000
Lucent Technologies SONET-ready network multiplexer that can function as a lightwave terminal. It is designed primarily for loop feeder and interoffice applications that work in existing asynchronous as well as the emerging SONET networks. This equipment multiplexes DS1, DS3, or EC-1 inputs into EC-1, OC-1, OC-3, or OC-12 outputs.

Default
An operation or value that the system or application assumes, unless a user makes an explicit choice.

Default Provisioning
The parameter values that are preprogrammed as shipped from the factory.

Defect
A limited interruption of the ability of an item to perform a required function. It may or may not lead to maintenance action depending on the results of additional analysis.

Demultiplexer
A device that splits a combined signal into individual signals at the receiver end of transmission.

Demultiplexing
A process applied to a multiplexed signal for recovering signals combined within it and for restoring the distinct individual channels of these signals.

Dense Wavelength Division Multiplexing (DWDM)
Transmitting two or more signals of different wavelengths simultaneously over a single fiber.

Deprovisioning
The inverse order of provisioning. To manually remove/delete a parameter that has (or parameters that have) previously been provisioned.

Digital Cross-Connect Panel (DSX)
A panel designed to interconnect equipment that operates at a designated rate. For example, a DSX-3 interconnects equipment operating at the DS3 rate.

Digital Multiplexer
Equipment that combines by time-division multiplexing several digital signals into a single composite digital signal.

Digital Signal Levels 0, 1, 3 (DS0, DS1, DS3)
An ANSI-defined signal or service level corresponding to the following: DS0 is 64 Kb/s, DS1 is 1.544 Mb/s (equivalent to T1), and DS3 is 44.736 Mb/s (equivalent to 28 T1 channels or T3).

Directory Service Network Element (DSNE)
A designated network element that is responsible for administering a database that maps network element names (TIDs) to addresses [NSAPs (network service access points)] in an OSI subnetwork. There can be one DSNE per ring. A DSNE can also be a GNE.

Dispersion
Time-broadening of a transmitted light pulse.

Dispersion Shifted Optical Fiber
1330/1550 nm minimum dispersion wavelength.

Divergence
When there is unequal amplification of incoming wavelengths, the result is a power divergence between wavelengths.

Doping
The addition of impurities to a substance in order to attain desired properties.

Downstream
At or towards the destination of the considered transmission stream, for example, looking in the same direction of transmission.

Drop and Continue
A circuit configuration that provides redundant signal appearances at the outputs of two network elements in a ring. Can be used for Dual Ring Interworking (DRI) and for video distribution applications.

Drop-Down Menu
A menu that is displayed from a menu bar.

DS1 Signal
Signal with a data rate of 1.544 Mb/s.

DS3 Format
Specifies the line format of a DS3 interface port, such as M13 or C-bit parity.

DS3 Idle Signal
A signal that can be applied to any output port that is not cross-connected to an input port. This signal lets downstream network elements know that the facility is operating normally even though it is not sending a normal DS3 signal.

DS3 Signal
A logical or electrical B3ZS signal with a data rate of 44.736 Mb/s.

DSX-1, 2, 3
Digital cross-connect used to interconnect equipment, provide patch capability, and provide test access at the DS1, DS2, or DS3 level.

Dual Ring Interworking (DRI)
A topology in which two rings are interconnected at two nodes on each ring and operate so that inter-ring traffic is not lost in the event of a node or link failure at an interconnecting point.

E

Electrical Carrier, Level 1 (EC-1)
An electrical interface signal at the SONET rate of STS-1.

Electromagnetic Compatibility (EMC)
A measure of equipment tolerance to external electromagnetic fields.

Electromagnetic Interference (EMI)
High-energy, electrically induced magnetic fields that cause data corruption in cables passing through the fields.

Electronic Industries Association (EIA)
A trade association of the electronic industry that establishes electrical and functional standards.

Electrostatic Discharge (ESD)
Static electrical energy potentially harmful to circuit packs and humans.

Entity
A specific piece of hardware (usually a circuit pack, slot, or module) that has been assigned a name recognized by the system.

Entity Identifier
The name used by the system to refer to a circuit pack, memory device, or communications link.

Equipped (EQ)
Status of a circuit pack or interface module that is in the system database and physically in the frame, but not yet provisioned.

Erbium
A soft rare earth element used in metallurgy and nuclear research.

Erbium Doped Fiber Amplifier (EDFA)
An amplifier that performs by having a light signal pass through a section of erbium-doped fiber and using the laser pump diode to amplify the signal.

Errored Seconds (ES)
A performance monitoring parameter. ES “type A” is a second with exactly one error; ES “type B” is a second with more than one and less than the number of errors in a severely errored second for the given signal. ES by itself means the sum of the type A and type B ESs.

Establish
A user initiated command, at the WaveStar CIT, to create an entity and its associated attributes in the absence of certain hardware.

Event
A significant change. Events in controlled Network Elements include signal failures, equipment failures, signals exceeding thresholds, and protection switch activity. When an event occurs in a controlled Network Element, the controlled Network Element will generate an alarm or status message and send it to the management system.

Event Driven
A required characteristic of network element software system: NEs are reactive systems, primarily viewed as systems that wait for and then handle events. Events are provided by the external interface packages, the hardware resource packages, and also by the software itself.

Externally Timed
An operating condition of a clock in which it is locked to an external reference and is using time constants that are altered to quickly bring the local oscillator's frequency into approximate agreement with the synchronization reference frequency.

Extra traffic
Unprotected traffic that is carried over protection channels when their capacity is not used for the protection of working traffic.

F

Facility
A one- or two-way circuit that carries a transmission signal.

Failures in Time (FIT)
Circuit pack failure rates per 10^9 hours as calculated using the method described in *Reliability Prediction Procedure for Electronic Equipment*, BellCore Method I, Issue 5, September 1995.

Far End (FE)
Any other network element in a maintenance subnetwork other than the one the user is at or working on. Also called remote.

Far-End Block Error (FEBE)
An indication returned to the transmitting node that an errored block has been detected at the receiving node. A block is a specified grouping of bits.

Far-End Receive Failure (FERF)
An indication returned to a transmitting Network Element that the receiving Network Element has detected an incoming section failure. Also known as RDI.

Fault
Term used when a circuit pack has a hard (not temporary) fault and cannot perform its normal function.

Fault Management
Collecting, processing, and forwarding of autonomous messages from network elements.

Fiber Distributed Data Interface (FDDI)
Fiber interface that connects computers and distributes data among them.

Flash EPROM
A technology that combines the nonvolatility of EPROM with the in-circuit reprogrammability of EEPROM (electrically-erasable PROM).

Folded Rings
: Folded (collapsed) rings are rings without fiber diversity. The terminology derives from the image of folding a ring into a linear segment.

Forced
: Term used when a circuit pack (either working or protection) has been locked into a service-providing state by user command.

Frame
: The smallest block of digital data being transmitted.

Frame Relay (FR)
: A form of packet switching that relies on high-quality phone lines to minimize errors. It is very good at handling high-speed, bursty data over wide area networks. The frames are variable lengths and error checking is done at the end points.

Framework
: An assembly of equipment units capable of housing shelves, such as a bay framework.

Free Running
: An operating condition of a clock in which its local oscillator is not locked to an internal synchronization reference and is using no storage techniques to sustain its accuracy.

FT-2000 ADR
: Lucent Technologies' OC-48 rate Add/Drop Rings lightwave Terminal for 2-fiber BLSRs. It is designed primarily for interoffice applications. It supports adds, drop, and through connections for DS3/EC-1, OC-3, IS-3, and OC-12.

G

Gateway Network Element (GNE)
: A network element that passes information between other network elements and management systems through a data communication network.

Gateway Network Element (GNE)
A Network Element that provides a means of communication between an OS and remote Network Elements over the SONET DCC.

In a primary/secondary GNE pair:

The active GNE is the GNE (primary or secondary) that is currently serving as the GNE for the subnetwork.

The primary GNE is the first GNE associated with a subnetwork that initially serves as the GNE for the subnetwork.

The secondary GNE is the second GNE that is associated with the primary GNE for a subnetwork, and can take over communications in the event there is a failure in the communications via the primary GNE.

The standby GNE is the GNE (primary or secondary) that is currently serving as the backup GNE for the subnetwork in the event there is a failure in communications via the active GNE.

H

Hard Failure
An unrecoverable nonsymptomatic (primary) failure that causes signal impairment or interferes with critical network functions, such as DCC operation.

High Level Data Link Control (HDLC)
OSI reference model datalink layer protocol.

Holdover
An operating condition of a clock in which its local oscillator is not locked to an external reference but is using storage techniques to maintain its accuracy with respect to the last known frequency comparison with a synchronization reference.

Host
The host is an HP 9000/800 series platform running HP-UX.

Hot Standby
A circuit pack ready for fast, automatic placement into operation to replace an active circuit pack. It has the same signal as the service going through it, so that choice is all that is required.

Human Machine Language (MML)
A standard language developed by the ITU for describing the interaction between humans and dumb terminals.

I

Idle
An output port not cross-connected to an input port.

Idle Code
A signal transmitted downstream automatically from an idle output port. It can also be transmitted downstream by a manual command from a cross-connected output port.

Insert
To physically insert a circuit pack into a slot, thus causing a system initiated restoral of an entity into service and/or creation of an entity and associated attributes.

In-Service (IS)
A memory administrative state for ports. IS refers to a port that is fully monitored and alarmed.

Integrated Transport Management Network Module (ITM NM)
Lucent Technologies' integrated network management system that provides a broad end-to-end view of the SONET network.

Integrated Transport Management SubNetwork Controller (ITM SNC)
Lucent Technologies' SONET element management layer system that provides fault, configuration, and security functions through the use of a GUI.

Intelligent Alarm Filtering
The filtering of symptomatic alarms and events that are associated with a reported root-cause or symptomatic condition.

Interconnect Signal-3 (IS-3)
The logical equivalent to an OC-3 signal that uses a proprietary interface that allows short-range operation at a lower cost than an OC-3.

Interface Capacity
The total number of STS-1 equivalents (bidirectional) tributaries in all transmission interfaces with which a given transmission interface shelf can be equipped at one time. The interface capacity varies with equipage.

InterLATA
Circuits that cross outside the LATA and to an interexchange carrier.

IntraLATA
Circuits with both end-points within the LATA.

J

Jitter
: Short term variations of amplitude and frequency components of a digital signal from their ideal position in time.

L

Lead Time
: The time interval between placement of a product order and receipt of the product.

Lightguide Build-Out (LBO)
: An attenuating (signal-reducing) element used to keep an optical output signal strength within desired limits.

Line
: A transmission medium, together with the associated equipment, required to provide the means of transporting information between two consecutive network elements. One network element originates the line signal; the other terminates it.

Line Build Out (LBO)
: An equalizer network that guarantees the proper signal level and shape at the DSX panel.

Line Controller Local Area Network (LCLAN)
: The internal local area network that provides communications between the controlled circuit packs.

Line Protection
: The optical interfaces can be protected by line protection. Line protection switching protects against failures of line facilities, including the interfaces at both ends of a line, the optical fibers, and any equipment between the two ends. Line protection includes protection of equipment failures.

Line Timing
: Refers to a network element that derives its timing from an incoming OC-N signal.

Link
: The mapping between in-ports and out-ports. It specifies how components are connected to one another.

Literal Character
: A letter, digit, or symbol that is entered in a command. The first hyphen in UNIT-{1-64} is a literal character; the braces and the second hyphen are not literal characters.

Local Area Network (LAN)
A communications network that covers a limited geographic area, is privately owned and user administered, is mostly used for internal transfer of information within a business, is normally contained within a single building or adjacent group of buildings, and transmits data at a very rapid speed.

Location
An identifier for a specific circuit pack, interface module, interface port, or communications link.

Lockout of Protection
The WaveStar CIT command that prevents the system from switching traffic to the protection line from a working line. If the protection line is active when a "Lockout of Protection" is entered – this command causes the working line to be selected. The protection line is then locked from any Automatic, Manual, or Forced protection switches.

Lockout State
The Lockout State shall be defined for each working or protection circuit pack. The two permitted states are: None – meaning no lockout is set for the circuit pack, set meaning the circuit pack has been locked out. The values (None & Set) shall be taken independently for each working or protection circuit pack.

Loopback
Type of diagnostic test used to compare an original transmitted signal with the resulting received signal. A loopback is established when the received optical or electrical external transmission signal is sent from a port or tributary input directly back toward the output.

Loop Timing
A special case of line timing. It applies to network elements that have only one OC-N/STM-N interface. For example, terminating nodes in a linear network are loop timed.

Loss Budget
Loss (in dB) of optical power due to the span transmission medium (includes fiber loss and splice losses).

Loss of Frame (LOF)
A failure to synchronize to an incoming signal.

Loss of Pointer (LOP)
A failure to extract good data from a signal payload.

Loss of Signal (LOS)
The complete absence of an incoming signal.

M

M23-Format
A standard framing format used for DS3 signals produced by multiplexing 28 DS1s into a DS3 (sometimes referred to as M13 format, without C-bit parity).

Management Functional Area (MFA)

A category of service provided by the Network Management system, such as Fault Management, Configuration Management, Performance Management, or Security Management.

Major
Indicates a service-affecting failure, main or unit controller failure, or power supply failure.

Maintenance Condition
An equipment state in which some normal service functions are suspended, either because of a problem or to perform special functions (copy memory) that cannot be performed while normal service is being provided.

Manual Switch State
A protection group shall enter the Manual Switch State upon the initiation and successful completion of the Manual Switch command. The protection group leaves the Manual Switch state by means of the Clear or Forced Switch commands. While in the Manual Switch state the system may switch the active unit automatically if required for protection switching.

Mapping
The logical association of one set of values, such as addresses on one network, with quantities or values of another set, such as devices or addresses on another network.

Mediation Device (MD)
Allows for exchange of management information between Operations System and Network Elements.

Mid-Span Meet
The capability to interface between two lightwave network elements of different vendors. This applies to high-speed optical interfaces.

Minor (MN)
Indicates a non-service-affecting failure of equipment or facility.

Miscellaneous Discrete Interface
Allows an operations system to control and monitor equipment collocated within a set of input and output contact closures.

Multiplexer
A device (circuit pack) that combines two or more transmission signals into a combined signal on a shared medium.

Multiplexing
The process of combining multiple signals into a larger signal at the transmitter by a multiplexer. The large signal is then split into the original smaller signals at the receiver by a demultiplexer.

N

Network Element (NE)
A node in a telecommunication network that supports network transport services and is directly manageable by a management system.

Network Monitoring and Analysis (NMA)
An operations system designed by Bellcore which is used to monitor network facilities.

Network Service Access Point (NSAP) Address
Network Service Access Point Address (used in the OSI network layer 3). An automatically assigned number that uniquely identifies a Network Element for the purposes of routing DCC messages.

Node
A network element in a ring or, more generally, in any type of network. In a network element supporting interfaces to more than one ring, node refers to an interface that is in a particular ring. Node is also defined as all equipment that is controlled by one system controller. A node is not always directly manageable by a management system.

Non-Preemptible Protection Access (NPPA)
Non-preemptible protection access increases the available span capacity for traffic which does not require protection by a ring, but which cannot be preempted.

Non-Revertive Switching
In non-revertive switching, an active and stand-by line exist on the network. When a protection switch occurs, the standby line is selected to support traffic, thereby becoming the active line. The original active line then becomes the stand-by line. This status remains in effect even when the fault clears. That is, there is no automatic switch back to the original status.

Non-Volatile Memory (NVM)
Memory that retains its stored data after power has been removed. An example of NVM would be a hard disk.

No Request State
This is the routine-operation quiet state in which no external command activities are occurring.

Not Monitored (NMON)
A provisioning state for equipment that is not monitored or alarmed.

O

Open Ring Network
A network formed of a linear chain-shaped configuration of network elements. Each network element connects to two others, one on each side, except for two network elements at the ends which are connected on only one side. A closed ring can be formed by adding a connection between the two end nodes.

Open Systems Interconnection (OSI)
Referring to the OSI reference model, a logical structure for network operations standardized by the International Standards Organization (ISO).

Operations Interface
Any interface providing you with information on the system behavior or control. These include the equipment LEDs, user panel, WaveStar CIT, office alarms, and all telemetry interfaces.

Operations Interworking (OI)
The capability to access, operate, provision, and administer remote systems through craft interface access from any site in a SONET network or from a centralized operations system.

Operations System (OS)
A central computer-based system used to provide operations, administration, and maintenance functions.

Operations System for Intelligent Network Elements (OPS/INE)
A Bellcore configuration management operations system.

Operator
A user of the system with operator-level user privileges.

Optical Carrier N (OC-N)
An optical carrier signal at the SONET rate of N, where n equals 1, 3, 12, 48, or 192. The basic rate of an OC-1 signal is 51.84 Mb/s, equivalent to an STS-1, with other values of N direct multiples of this basic rate.

Optical Channel
A OC-N wavelength within an optical line signal. Multiple channels, differing by 1.5µ in wavelength, are multiplexed into one signal.

Optical Demultiplexer Unit (ODU)
A circuit pack responsible for receiving the optical line signal and separating it into the original number of OC-N/STM-Nsignals.

Optical Line Signal
A multiplexed optical signal containing multiple wavelengths or channels.

Optical Multiplexer Unit (OMU)
A circuit pack responsible for combining multiple signals into one signal. The combined signal is called the Optical Line Signal.

Optical Translator (OT)
A system feature used in conjunction with WaveStar OLS that concatenates multiple OLS terminals, regenerates signals in the 1.3 and 1.5 μ ranges, prevents wavelength blocking via wavelength interchange, provides wavelength add/drop (WAD) capabilities, and establishes open interfaces with multi-vendor signal compatibility.

Optical Translator Port Module (OTPM)
A circuit pack that can electrically regenerate incoming OC-12/STM-4 and OC-3/STM-1 signals into specific outgoing signals of the same type.

Optical Translator Unit (OTU)
A circuit pack that can electrically regenerate incoming OC-N/STM-N signals (1.3 or 1.5 μ ranges) into specific outgoing signals of the same type.

Orderwire (OW)
A dedicated voice-grade line for communications between maintenance and repair personnel.

Original Value Provisioning
Preprogramming of a system's original values at the factory. These values can be overridden using local or remote provisioning.

Outage
A disruption of service that lasts for more than one second.

Out-of-Service
The circuit pack is not providing its normal service function (removed from either the working or protection state) either because of a system problem or because the pack has been removed from service.

P

Packet Assembler/Disassembler (PAD)
An interface between a device and an X.25 packet-switched network. The PAD converts the protocol used by the device and the X.25 protocol used by the network, allowing terminals to exchange data with other packet mode terminals and hosts.

Packet-Switched Network (PSN)
An X.25 network that transmits groups of bits as a unit through the network. Packets usually include data and control information such as addressing, identification, and error-control fields.

Parameter
A variable that is given a value for a specified application. A constant, variable, or expression that is used to pass values between components.

Parity Check
: Tests whether the number of ones (or zeros) in an array of binary bits is odd or even; used to determine that the received signal is the same as the transmitted signal.

Pass-Through
: Paths that are cross-connected directly across an intermediate node in a network.

Path
: A logical connection between the point at which a standard frame format for the signal at the given rate is assembled, and the point at which the standard frame format for the signal is disassembled.

Path Overhead (POH)
: Informational bytes assigned to, and transported with the payload until the payload is demultiplexed. It provides for integrity of communication between the point of assembly of a virtual container and its point of disassembly.

Path Terminating Equipment
: Network elements in which the path overhead is terminated.

Performance Monitoring (PM)
: Measures the quality of service and identifies degrading or marginally operating systems (before an alarm would be generated).

Peripheral Control and Timing Facility Interface (PCTFI)
: A proprietary physical link interface supporting the transport of 21×2 Mb/s signals.

Platform
: A family of equipment and software configurations designed to support a particular application.

Plesiochronous Network
: A network that contains multiple subnetworks, each internally synchronous and all operating at the same nominal frequency, but whose timing may be slightly different at any particular instant.

Polarization Mode Dispersion (PMD)
: Output pulse broadening due to random coupling of the two polarization modes in an optical fiber.

Port (also called Line)
: The physical interface, consisting of both an input and output, where an electrical or optical transmission interface is connected to the system and may be used to carry traffic between network elements. The words “port” and “line” may often be used synonymously. “Port” emphasizes the physical interface, and “line” emphasizes the interconnection. Either may be used to identify the signal being carried.

Port State Provisioning
: A feature that allows a user to suppress alarm reporting and performance monitoring during provisioning by supporting multiple states (automatic, in-service, and not monitored) for low-speed ports.

Preprovisioning
: The process by which the user specifies parameter values for an entity in advance of some of the equipment being present. These parameters are maintained only in NVM. These modifications are initiated locally or remotely by either a CIT or an OS. Preprovisioning provides for the decoupling of manual intervention tasks (for example, install circuit packs) from those tasks associated with configuring the node to provide services (for example, specifying the entities to be cross-connected).

Proactive Maintenance
: Refers to the process of detecting degrading conditions not severe enough to initiate protection switching or alarming, but indicative of an impending signal fail or signal degrade defect.

Protection
: Extra capacity (channels, circuit packs) in transmission equipment that is not intended to be used for service, but rather to serve as backup against equipment failures.

Protection Access
: To provision traffic to be carried by protection tributaries when the port tributaries are not being used to carry the protected working traffic.

Protection Group Configuration
: The members of a group and their roles, for example, working protection, line number, etc.

Protection Path
: One of two signals entering a path selector used for path protection switching or dual ring interworking. The other is the working path. The designations working and protection are provisioned by the user, whereas the terms active path and standby path indicate the current protection state.

Protection State
: When the working unit is currently considered active by the system and that it is carrying traffic. The “active unit state” specifically refers to the receive direction of operation — since protection switching is unidirectional.

Provisioned (PROV)
: Indicating that a circuit pack is ready to perform its intended function. A provisioned circuit pack can be active (ACT), in-service (IS), standby (STBY), provisioned out-of-service (POS), or out-of-service (OOS).

Provisioning
The modification of certain programmable parameters that define how the node functions with various installed entities. These modifications are initiated locally or remotely by either a CIT or an OS. They may arrive at the node via the IAOLAN, CIT port, or any DCC channel. The provisioned data is maintained in NVM and/or hardware registers.

Q

Quad Optical Translator Unit (QOTU)
A unit that provides functions similar to an Optical Translator Unit (OTU), except that an QOTU provides the equivalent functionality of four OTUs in a package that is only twice the size of an OTU.

R

Reactive Maintenance
Refers to detecting defects/failures and clearing them.

Receive-Direction
The direction towards the Network Element.

Regeneration
The process of reconstructing a digital signal to eliminate the effects of noise and distortion.

Reliability
The ability of a software system performing its required functions under stated conditions for a stated period of time. The probability for an equipment to fulfill its function. Some of the ways in which reliability is measured are: MTBF (Mean Time Between Failures) expressed in hours; Availability = (MTBF)/(MTBF+MTTR)(%) [where MTTR = mean time to restore]; outage in minutes per year; failures per hour; percentage of failures per 1,000 hours.

Remote Defect Indication (RDI)
An indication returned to a transmitting terminal that the receiving terminal has detected an incoming section failure. [Previously called far-end-receive failure (FERF).]

Remote Failure Indication (RFI)
A signal that alerts upstream STS-1 path terminating equipment that a downstream failure has been alarmed along the STS-1 path. This action prevents multiple alarms from being activated for the same failure and ensures that a technician is dispatched to correct the failure. (Previously called yellow signals.)

Remote Network Element
: Any Network Element that is connected to the referenced Network Element through either an electrical or optical link. It may be the adjacent node on a ring, or N nodes away from the reference. It also may be at the same physical location but is usually at another (remote) site.

Return to Zero
: A code form having two information states (termed zero and one) and having a third state or an at-rest condition to which the signal returns during each period.

Revertive
: A protection switching mode in which, after a protection switch occurs, the equipment returns to the nominal configuration (that is, the working equipment is active, and the protection equipment is standby) after any failure conditions that caused a protection switch to occur, clear, or after any external switch commands are reset. (See “Non-Revertive Switching.”)

Revertive Switching
: In revertive switching, there is a working and protection high-speed line, circuit pack, etc. When a protection switch occurs, the protection line, circuit pack, etc. is selected. When the fault clears, service “reverts” to the working line.

Ring
: A configuration of nodes comprised of network elements connected in a circular fashion. Under normal conditions, each node is interconnected with its neighbor and includes capacity for transmission in either direction between adjacent nodes. Path switched rings use a head-end bridge and tail-end switch. Line switched rings actively reroute traffic over the protection capacity.

Router
: An interface between two networks. While routers are like bridges, they work differently. Routers provide more functionality than bridges. For example, they can find the best route between any two networks, even if there are several different networks in between. Routers also provide network management capabilities such as load balancing, partitioning of the network, and trouble-shooting.

S

Section
: The portion of a transmission facility, including terminating points, between a terminal network element and a line-terminating network element, or two line-terminating network elements.

Section Layer
: The second of the four levels in a standard SONET signal, used to transport an STS frame across a physical medium. This layer uses the photonic layer to form the physical transport.

Self-Healing
A network's ability to automatically recover from the failure of one or more of its components.

Server
Computer in a computer network that performs dedicated main tasks which generally require sufficient performance.

Serving Area
A user-defined grouping of Network Elements. It most commonly consists of Network Elements located in a central office (CO) and the subnetworks to which they belong.

Severely Errored Seconds (SES)
This performance monitoring parameter is a second in which a signal failure occurs, or more than a preset amount of coding violations (dependent on the type of signal) occurs.

Service
The operational mode of a physical entity that indicates that the entity is providing service. This designation will change with each switch action.

Signal-to-Noise Ratio (SNR)
The relative strength of signal compared to noise.

Signal Rate
An attribute that defines the bit-rate and format of the signal. The signal rate is defined by the STS-N path-level signal bit-rate and format including the presence or absence of concatenation.

Single-Ended Operations
Provides operations support from a single location to remote Network Elements in the same SONET subnetwork. With this capability you can perform operations, administration, maintenance, and provisioning on a centralized basis. The remote Network Elements can be those that are specified for the current release.

Single-Mode Fiber (SM)
An 8-µ diameter low-loss, long-span optical fiber typically operating at either 1310 nm, 1550 nm, or both.

Site Address
The unique address for a Network Element.

Slot
A physical position in a shelf designed for holding a circuit pack and connecting it to the backplane. This term is also used loosely to refer to the collection of ports or tributaries connected to a physical circuit pack placed in a slot.

Software Backup
: The process of saving an image of the current network element's databases, which are contained in its NVM, to a remote location. The remote location could be the WaveStar CIT or an OS.

Software Download
: The process of transferring a generic (full or partial) or provisioned database from a remote entity to the target network element's memory. The remote entity may be the WaveStar CIT or an OS. The download procedure uses bulk transfer to move an uninterpreted binary file into the network element.

Software ID
: Number that provides the software version information for the system.

Span
: An uninterrupted bidirectional fiber section between two network elements.

Span Growth
: A type of growth in which one wavelength is added to all lines before the next wavelength is added.

Squelch Map
: This map contains information for each cross-connection in a ring and indicates the source and destination nodes for the low-speed circuit that is part of the cross-connection. This information is used to prevent traffic misconnection in rings with isolated nodes or segments.

Standby
: The circuit pack is in service but is not providing service functions. It is ready to be used to replace a similar circuit pack either by protection or by duplex switching.

Standby Path
: One of two signals entering a constituent path selector, the standby path is the path not currently being selected.

State
: The state of a circuit pack indicates whether it is defective or normal (ready for normal use).

Status
: The indication of a short-term change in the system.

STS-1E
: Now referred to as EC-1. A signal typically carried by coaxial cables from one equipment location to another. The term EC-1 refers to the organization and data rate of the signal and also to the voltage template the signal must conform to and the impedances for which the voltage template is valid.

STS-1
The basic building block logical signal in the SONET standard with a data rate of 51.84 Mb/s.

Subnetwork
A group of interconnected/interrelated Network Elements. The most common connotation is a synchronous network in which the Network Elements have Data Communications Channel (DCC) connectivity.

Supervisory Signal
An optical signal originating with the telemetry circuit pack that is used to communicate maintenance information.

Suppression
A process where service-affecting alarms that have been identified as an "effect" are not displayed to a user.

Symptomatic Alarm
An alarm that is not indicative of an actual failure itself, but rather of a secondary manifestation.

Synchronization Messaging
Synchronization messaging is used to communicate the quality of network timing, internal timing status, and timing states throughout a subnetwork.

Synchronous
The essential characteristic of time scales or signals such that their corresponding significant instances occur at precisely the same average rate, generally traceable to a single Stratum-1 source.

Synchronous Digital Hierarchy (SDH)
A hierarchical set of digital transport structures, standardized for the transport of suitable adapted payloads over transmission networks.

Synchronous Network
The synchronization of transmission systems with synchronous payloads to a master (network) clock that can be traced to a reference clock.

Synchronous Optical Network (SONET)
The North American standard for the rates and formats that defines optical signals and their constituents.

Synchronous Payload
Payloads that can be derived from a network transmission signal by removing integral numbers of bits from every frame. Therefore, no variable bit-stuffing rate adjustments are required to fit the payload in the transmission signal.

Synchronous Payload Envelope (SPE)
The combined payload and path overhead of an STS-1, STS-3c, STS-12c or STS-48c signal.

Synchronous Transport Signal (STS, STS-N)
The basic logical building block signal for SONET with a rate of 51.84 Mb/s for an STS-1 signal and a rate of N times 51.84 Mb/s for an STS-N signal.

Synchronous Transport Signal, Level N, Concatenated (STS-Nc)
A concatenated SONET payload signal at the STS-N rate, where N equals 3, 12, or 48. For example, an STS-3c signal is constructed by concatenating three STS-1 signals into a signal that uses a single path overhead, rather than three.

T

T1
A carrier system that transmits at the rate of 1.544 Mb/s (a DS1 signal).

T2
A carrier system that transmits at the rate of 6.312 Mbps (a DS2 signal).

T3
A carrier system that transmits at the rate of 44.736 Mbps (a DS3 signal).

Target Group
An administrator-defined group that defines to which Network Elements a user has access.

Target Identifier (TID)
A provisionable parameter that is used to identify a particular Network Element within a network. It is a character string of up 20 characters where the characters are letters, digits, or hyphens (-).

Telemetry Feed-Through
Operations capability for 4-fiber applications which allows the DCC to go from one OLS End Terminal (one subnetwork) through to the other collocated end terminal (separate subnetwork), thereby extending the OLS operations domain.

Through (or Continue) Cross-Connection
A cross-connection within a ring, where the input and output tributaries have the same tributary number but are in lines opposite each other.

Threshold-Crossing Alert (TCA)
A message type sent from a Network Element that indicates that a certain performance monitoring parameter has exceeded a specified threshold.

Through Timing
Refers to a network element that derives its transmit timing in the east direction from a received line signal in the east direction and its transmit timing in the west direction from a received line signal in the west direction.

Time Division Multiplexing (TDM)
A technique for transmitting a number of separate data, voice, and/or video signals simultaneously over one communications medium by interleaving a portion of each signal one after another.

Time Slot Assignment (TSA)
A capability that allows any tributary in a ring to be cross-connected to any tributary in any lower-rate, non-ring interface or to the same-numbered tributary in the opposite side of the ring.

Time Slot Interchange (TSI)
The ability of the user to assign cross-connections between any tributaries of any lines within a Network Element. Three types of TSI can be defined: Hairpin TSI, Interring TSI (between rings), and Intraring TSI (within rings).

Transaction Language One (TL1)
A machine-to-machine communications language that is a subset of ITU's human-machine language.

Transmit-Direction
The direction outwards from the Network Element.

Tributary
A path-level unit of bandwidth within a port, or the constituent signal(s) being carried in this unit of bandwidth, for example, an STS-1 tributary within an OC-N port.

True Wave™ Optical Fiber
Lucent Technologies' fiber generally called non-zero dispersion-shift fiber, with a controlled amount of chromatic dispersion designed for amplified systems in the 1550/1310 nm range.

Two-Way Point-to-Point Cross-Connection
A two-legged interconnection, that supports two-way transmission, between two and only two tributaries.

Two-Way Roll
The operation which moves a two-way cross-connection between tributary i and tributary j to a two-way cross-connection between the same tributary i and a new tributary k with a single user command.

U

Unavailable Seconds (UAS)
In performance monitoring, the count of seconds in which a signal is declared failed or in which 10 consecutively severely errored seconds (SES) occurred, until the time when 10 consecutive non-SES occur.

Upstream
At or towards the source of the considered transmission stream, for example, looking in the opposite direction of transmission.

User Privilege
Permissions a user must perform on the computer system on which the system software runs.

User-to-Network Interface (UNI)
The specifications for the procedures and protocols between a user and the Asynchronous Transfer Mode (ATM) network.

V

Value
A number, text string, or other menu selection associated with a parameter.

Variable
An item of data named by an identifier. Each variable has a type, such as int or Object, and a scope.

Violation Monitor and Removal (VMR)
A provisionable mode for DS3 output that causes parity violations to be monitored and corrected before the DS3 signal is B3ZS encoded.

Virtual
Refers to artificial objects created by a computer to help the system control shared resources.

Virtual Circuit
A logical connection through a data communication (for example, X.25) network.

Virtual Tributary (VT)
A structure designed for transport and switching of sub-STS-1 payloads. There are currently four sizes: VT1.5 (1.728 Mb/s), VT2 (2.304 Mb/s), VT3 (3.456 Mb/s), and VT6 (6.912 Mb/s).

Virtual Tributary Group (VT-G)
A 9-row by 12-column structure (108 bytes) that carries one or more VTs of the same size. Seven VT groups (756 bytes) are byte interleaved with the VT-organized synchronous payload envelope.

Voice Frequency (VF) Circuit
A 64 kilobit per second digitized signal.

Volatile Memory
Type of memory that is lost if electrical power is interrupted.

VT1.5 Tributary
A SONET logical signal with a data rate of 1.728 Mbps. In the nine-row structure of the STS-1 SPE, a VT1.5 occupies three columns. VT-structured STS-1 SPEs are divided into seven VT groups. Each VT group occupies twelve columns of the nine-row structure and, for VT1.5s, contains four VTs per group.

W

Wait-to-Restore (WTR)
Applies to revertive switching operation. The protection group enters the WTR state when all Equipment Fail (EF) conditions are cleared, but the system has not yet reverted back to its working line. The protection group remains in the WTR state until the Wait-to-Restore timer completes the WTR time interval.

Wait to Restore Time (WRT)
Corresponds to the time to wait before switching back after a failure has cleared, in a revertive protection scheme. This can be between 0 and 15 minutes, in increments of one minute.

Wavelength Add/Drop (WAD)
The process of adding and dropping wavelengths to provide more efficient transmission.

Wavelength Division Multiplexing (WDM)
A means of increasing the information-carrying capacity of an optical fiber by simultaneously transmitting signals at different wavelengths.

Wavelength Interchange
The ability to change the wavelength associated with an OC-N signal into another wavelength.

WaveStar™ Optical Line System
Lucent Technologies' lightwave transmission system. Utilizing DWDM technology, the system combines multiple signals of different wavelengths, transmits the resulting signal over a single fiber, and then demultiplexes the signal at the receive end.

Wide Area Network (WAN)
A communication network that uses common-carrier provided lines and covers an extended geographical area.

Wideband Communications
Voice, data, and/or video communication at digital rates from 64 kb/s to 2 Mb/s.

Working
: Label attached to a physical entity. In case of revertive switching the working line or unit is the entity that is carrying service under normal operation. In case of non-revertive switching the label has no particular meaning.

Working State
: The working unit is currently considered active by the system and that it is carrying traffic.

X

X.25 Interface / Protocol
: The ITU packet-switched interface standard for terminal access that specifies three protocol layers: physical, link, and packet for connection to a packet-switched data network.

X-Terminal
: Workstation that can support an X-Windows interface.

Z

Zero Code Suppression
: A technique used to reduce the number of consecutive zeros in a line-coded signal (B3ZS, B8ZS).

Abbreviations and Acronyms

Overview

The following is a list of abbreviations and acronyms related to WaveStar SNMS.

A

ABN
Abnormal (condition)

ABS
Absent

AC
Alternating Current

ACO
Alarm Cut-Off

ACT
Active

ADM
Add/Drop Multiplexer

ADR
Add/Drop Ring

AGNE
Alarm Gateway Network Element

AID
Access Identifier

AIS
Alarm Indication Signal

AIP
Alarm Issuing Point

AITS
Acknowledged Information Transfer Service: Confirmed mode of operation of the LAPD protocol.

AMI
Alternate Mark Inversion

ANSI
American National Standards Institute

APD
Avalanche PhotoDiode

APS
Automatic Protection Switch

ASAP

Alarm Severity Assignment Profile

AS&C
Alarm, Status, and Control

APSD
Automatic Power Shutdown

ASCII
American Standard Code for Information Interchange

ASN.1
Abstract Syntax Notation 1

ATM
Asynchronous Transfer Mode

AUTO
Automatic

AVAIL
Available

B

B3ZS
Bipolar 3-Zero Substitution

B8ZS
Bipolar 8-Zero Substitution

BCLAN
Board Controller Local Area Network

BDFB
Battery Distribution and Fuse Bay

BER
Bit Error Rate

BITS
Building Integrated Timing Supply

BLK
Blank

BLSR
Bidirectional Line-Switched Ring

BOC
Bell Operating Company

C

CAC
Circuit Access Code

CCITT
Comité Consultatif International Télégrafique & Téléphonique

CCT
Cross-Connection Type

CDRH
Center for Devices and Radiological Health

CEPT
Conférence Européenne des Administrations des Postes et des Télécommunications

CID
Circuit Identifier

CIT or CIT-PC
Craft Interface Terminal

CL
Clear

CLEI
Common Language Equipment Identifier

CLLI
Common Language Location Identifier

CM
Communications Module

CMIP
Common Management Information Protocol. OSI standard protocol for OAM&P information exchange.

CMISE
Common Management Information Service Element

CO
Central Office

COV
Central Office Video

CP
Circuit Pack

CPE
Customer Premises Equipment

CR
Critical (alarm)

CSMA / CD
Carrier Sense Multiple Access with Collision Detection

CS&O
Lucent Technologies Customer Support and Operations

CSU
Channel Service Unit

CTIP
Customer Training and Information Products

CTS
Customer Technical Support within Lucent Technologies

CV
Coding Violation

D

DACS / DCS
Digital Access Cross-Connect System

dB
Decibels

DC
Direct Current

DCC
Data Communications Channel

DCE
Data Communications Equipment

DCN
Data Communications Network

DPLL
Digital Phase Locked Loop

DRI
Dual Ring Interworking

DRAM
Dynamic Random Access Memory

DRIP
Dual Ring Interworking on Protection

DS0, DS1, DS3
Digital Signal Levels 0, 1, 3

DS-N
Digital Signal, Level N

DS-NE
Directory Service Network Element

DSX
Digital Cross-Connect Frame

DTCU
Distant Terminal Channel Unit

DTE
Data Terminating Equipment

DTMF
Dual Tone Multifrequency

DWDM
Dense Wavelength Division Multiplexing

E

EBER
Equivalent Bit Error Rate

EC
Echo Canceller

EC-1, EC-N
Electrical Carrier, Levels 1 and N

ECI
Equipment Catalog Item

EEPROM
Electrically Erasable Programmable Read-Only Memory

EF
Equipment Fail

EIA
Electronic Industries Association

EM
Event Management

EMC
Electromagnetic Compatibility

EMI
Electromagnetic Interference

EMS
Element Management System

EPROM
Erasable Programmable Read-Only Memory

EPT
Event-per-Time

EQ
Equipped

EQPT
Equipment

ES
Errored Seconds

ESD
Electrostatic Discharge

ESF
Extended Super Frame (DS1 signal format)

ETSI
European Telecommunications Standards Institute

EVT
Event

EXM
Extended Switching Module

F

FCC
Federal Communications Commission

FDA
Food and Drug Administration

FDDI
Fiber Distributed Data Interface

FE
Far End

FEBE
Far End Block Error

FEPROM
Flash EPROM

FIT
Failure in Time

G

GB
Gigabytes

Gb/s
Gigabits per second

GHz
Gigahertz

GNE
Gateway Network Element

GR-XXX
Bellcore General Requirement-XXX

H

HDLC
High-Level Data Link Control

HS
High Speed

HW
Hardware

Hz
Hertz

I

IAF
Intelligent Alarm Filtering

IAO LAN
Intraoffice Local Area Network

ID
Identifier

IEC
International Electrotechnical Commission

IEEE
Institute of Electrical and Electronics Engineers

I/O
Input/Output

INTFC
Interface

IS
In Service

IS-3
Interconnect Signal-3

ISDN
Integrated Services Digital Network

ITCO
Independent Telephone Company

ITM
Integrated Transport Management

ITM-NM
Integrated Transport Management Network Module

ITM SNC
Integrated Transport Management SubNetwork Controller

ITU
International Telecommunications Union

ITU-R
International Telecommunications Union — Radio standardization sector. Formerly known as CCIR: Comité Consultatif International Radio; International Radio Consultative Committee.

ITU-T
International Telecommunications Union — Telecommunication standardization sector. Formerly known as CCITT: Comité Consultatif International Télégrafique & Téléphonique; International Telegraph and Telephone Consultative Committee.

IXC
Interexchange Carrier

K

Kbps
Kilobits per second

L

LAN
Local Area Network

LATA
Local Access and Transport Area

LBC
Laser Bias Current

LBFC
Laser Backface Currents

LBO
Lightguide Build-Out

LBP
LAN Bridge Port

LCN
Local Communications Network

LCT
Large Capacity Terminal

LEC
Local Exchange Carrier

LED
Light-Emitting Diode

LGX
Lightguide Cross-Connect

LMP
LAN Management Port

LNE
Logical Network Element

LOF
Loss of Frame

LOP
Loss of Pointer

LOS
Loss of Signal

LPBK
Loopback

LS
Low Speed

LTE
Line Terminating Equipment

M

µ
Microns

µm
Micrometer

MB
Megabytes

Mbpss
Megabits per second

MCOND
Maintenance Condition

MDS
Metallic Digital Server

MDSCU
Metallic Digital Server Channel Unit

MEM
Memory

MFA
Management Functional Area

MIPS
Millions of Instructions Per Second

MJ
Major (alarm)

MML
Human-Machine Language

MN
Minor (alarm)

ms
Millisecond

MTBF
Mean Time Between Failures

MTBMA
Mean Time Between Maintenance Activities

MTTR
Mean Time To Repair

N

NA
Not Applicable

NCC
Network Communication Controller

NE
Network Element

NEBS
Network Equipment-Building System

nm
Nanometer (10^{-9} meters)

NMA
Network Monitoring and Analysis System

NMA-F
Network Monitoring and Analysis-Facility

NMON
Not Monitored

NMS
Network Management System

NORM
Normal

NPPA
Non-Preemptible Protection Access

NRZ
Nonreturn to Zero

NSA
Non-Service Affecting

NSAP Address
Network Service Access Point Address (used in the OSI network layer 3)

NTF
No Trouble Found

NVM
Non-Volatile Memory

O

O&M
Operation and Maintenance

OA
Optical Amplifier

OALAN
Overhead Access Local Area Network

OAM&P
Operations, Administration, Maintenance, and Provisioning

OC, OC-N
Optical Carrier

OC-1
Optical Carrier, Level 1 Signal (51.84 Mb/s)

OC-3
Optical Carrier, Level 3 Signal (155.52 Mb/s)

OC-3c
Optical Carrier, Level 3 Concatenated Signal (155.52 Mb/s)

OC-12
Optical Carrier, Level 12 Signal (622.08 Mb/s)

OC-48
Optical Carrier, Level 48 (2488.32 Mb/s) (2.5 Gb/s)

OC-192
Optical Carrier, Level 192 (9953.28 Mb/s) (10 Gb/s)

ODU
Optical Demultiplexing Unit

OI
Operations Interworking

OILU
Optical Line Interface Unit

OLS
Optical Line System

OMU
Optical Multiplexing Unit

OOF
Out-of-Frame

OOS
Out-of-Service

OPS/INE
Operations System for Intelligent Network Elements

ORM
Optical Remote Module

OS
Operations System

OSI
Open Systems Interconnect

OSMINE
Operations Systems Modifications for the Integration of Network Elements

OT
Optical Translator

OTCTL
Optical Translator Controller

OTPM
Optical Translator Port Module

OTU
Optical Translator Unit

OW
Orderwire

P

PAD
Packet Assembler/Disassembler

PCB
Printed Circuit Board

PCM
Pulse Code Modulation

PDH
Plesiochronous Digital Hierarchy

PM
Performance Monitoring

PMD
Polarization Mode Dispersion

POH
Path Overhead

POP
Point of Presence

POTS
Plain Old Telephone Service

PRI
Primary

PROTN
Protection

PROV
Provisioned

PSDN
Public Switched Data Network

PSN
Packet-Switched Network

PSTN
Public Switched Telephone Network

PTE
Path Terminating Equipment

PTY
Parity

PVC
Permanent Virtual Circuit

PWR
Power

PWR ON
Power On

Q

QOS
Quality of Service

QOTU
Quad Optical Translator Unit

QRSS
Quasi-Random Signal Source

R

RAM
Random Access Memory

RCV
Receive

RCVR
Receiver

RDI
Remote Defect Indication

RF
Radio Frequency

RFI
Remote Failure Indication

RPP
Reliability Prediction Procedure

RT
Remote Terminal

RTAC
Regional Technical Assistance Center

RTRV
Retrieve

RTV
Remote Terminal Video

RZ
Return to Zero

S

SA
Service Affecting

SDH
Synchronous Digital Hierarchy

SDS
Standard Directory Service based on ANSI recommendation T1.245

SEC
Secondary

SES
Severely Errored Seconds

SF
Super Frame (DS1 signal format)

SLN
A 12-character circuit pack serial number

SNR
Signal-to-Noise Ratio

SOH
Section Overhead

SONET
Synchronous Optical Network

SPE
Synchronous Payload Envelope

STBY
Standby

STS
Synchronous Transport Signal

STS-1, STS-N
Synchronous Transport Signal, Levels 1 and N

STS-3
Synchronous Transport, Level 3

STS-3c
Synchronous Transport, Level 3 Concatenated Signal

STS-12
Synchronous Transport, Level 12

STS-12c
Synchronous Transport, Level 12Concatenated Signal

SVC
Switched Virtual Circuit

SYNC
Synchronizer

T

TA
Technical Advisory

TABS
Telemetry Asynchronous Byte Serial (Protocol)

TARP
Target Identifiers Address Resolution Protocol

TBD
To Be Determined

TBOS
Telemetry Byte-Oriented Serial (Protocol)

TCA
Threshold-Crossing Alert

TDM
Time Division Multiplexing

THz
Terrahertz (10^{12} Hz)

TID
Target Identifier

TIRKS
Trunks Integrated Records Keeping System

TL1
Transaction Language 1

TR
Technical Requirement

TSA
Time Slot Assignment

TSI
Time Slot Interchange

TSO
Technical Support Organization

TU
Tributary Unit

U

UAS
Unavailable Seconds

UITS
Unacknowledged Information Transfer Service. Unconfirmed mode of LAPD operation.

UNEQ
Path Unequipped

UPSR
Unidirectional Path-Switched Ring

USAM
User-Settable Alarm Monitoring

V

V
Volts

VAC
Volts Alternating Current

VDC
Volts Direct Current

VF
Voice frequency

VM
Violation Monitor

VMR
Violation, Monitor, and Removal

VRT
Virtual Remote Terminal

VT
Virtual Tributary

VT1.5
Virtual Tributary, Level 1.5

VT-G
Virtual Tributary Group

W

WAD
Wavelength Add/Drop

WAN
Wide Area Network

WaveStar™ OLS 40G / 80G / 400G
WaveStar Optical Line System 40G/80G/400G

WBS
Wideband Shelf

WDCS
Wideband Digital Cross-Connect System

WDM
Wavelength Division Multiplexing

X

X.25
An ITU standard defining the connection between a terminal and a public packet-switched network