Lucent Technologies
Bell Labs Innovations

WaveStar™ SubNetwork Management System (SNMS)

Administration Guide

190-224-122
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

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 190-224-120.

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
Administration Guide Release 4.2

190-224-122 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

Contents

Contents

Contents

Contents

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 Provisioning Guide is to instruct users how to administer WaveStar SNMS.

Intended audience

This guide is written primarily for operations personnel who will be administering WaveStar SNMS.

Reason for issue

This Provisioning 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

Commands to be input are shown in **bold** type.

Items shown in a command line in *italics* indicate the name of a directory/file or that this value is variable depending on the specific name of the data item, filename, or directory.

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	Security Management	Describes tasks performed to control access to WaveStar SNMS and its managed network elements
Chapter 2	System Administration	Describes tasks performed to start up, shut down, and reboot the WaveStar SNMS application.
Chapter 3	Database Maintenance	Describes tasks performed to maintain the WaveStar SNMS database.
Chapter 4	Management Communication of WaveStar SNMS	Describes tasks performed to configure communication interfaces with network elements managed by WaveStar SNMS
Chapter 5	Trouble Clearing	Describes tasks performed to facilitiate troubleshooting problems with software components of WaveStar SNMS and its communications interfaces

Section	Title	Description
Chapter 6	System Introduction	Provides an general introduction to WaveStar SNMS and its functions/ features
Chapter 7	Security Management Concepts	Provides general information about controlling access to WaveStar SNMS and its managed network element
Chapter 8	Trouble Clearing Concepts	Provides reference information to support tools used for troubleshooting WaveStar SNMS problems
Chapter 9	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

Security Management

1

Introduction

Summary

This chapter describes procedures performed to control access to WaveStar SNMS and its managed network elements.

Before you begin

Read the Security Management Concepts chapter to acquire a basic understanding of the Security Management features provided by WaveStar SNMS.

This chapter discusses the following topics:

Change Your User Password

Background

Use this procedure to change your user password.

Task

Complete the following steps to change your user password.

Step	Action
1	Select **Administration** from the main menu of the Map window. **Result:** This displays a sub-menu.
2	Choose **Security** from the displayed sub-menu. **Result:** This displays another sub-menu.
3	Choose **Change EMS Password** from the Security menu. **Result:** The Change Password window is displayed.
4	Type your current password into the Old Password field.
5	Type your desired new password into the New Password field. *Continued on next page*

Step	Action (Contd)	
6	Type the same desired new password into the Confirm New Password field.	
7	IF ... the new password entered is invalid	THEN ... the system issues a warning message. You must enter a password that is 6-10 characters, contains at least two non-alphabetic characters, and one special character (!#$%^&*()-+_=?). The following special characters are not permitted (:,;).
	you change the password to one previously used	If the “previous password” option in the Global Security Provisioning window is enabled, the system issues a message, advising that you cannot change the password to one previously used and that a different password must be chosen.
8	Select the OK button to enter the password change into the system. **Stop! End of Task.**	

Globally Administer NE Passwords

Background

Use this procedure to change the primary and/or secondary passwords for selected NE(s)/aggregate(s).

Before you begin

Before you begin this task, you must be logged into WaveStar SNMS. The NE(s) or aggregate(s) for which you are changing passwords must already exist in WaveStar SNMS. Be aware that if you are changing passwords for 20 or more NEs at a time, this may degrade system performance. Only one user can use the Global Administer NE Password function at a time.

Be aware that any changes to the primary/secondary passwords for NEs will affect logging into the NEs from all EMS and CIT interfaces.

BWM and TDM 10G (STM-64) NEs have a password aging feature for security reasons. When a software upgrade is performed for one of these NE types, one of the default NE passwords used to log into the NE to perform the upgrade automatically expires upon first use, and must be changed by the CIT. These default NE passwords are used by WaveStar SNMS to log into the NE and obtain information during the subnetwork autodiscovery process. The default NE passwords changed by the CIT during the software upgrade may not be known by WaveStar SNMS. However, as long as the second default NE password remains the same, WaveStar SNMS will be able to use it to log into the NE during subnetwork autodiscovery.

Once WaveStar SNMS has been able to log into a BWM or TDM 10G (STM-64) NE using the unchanged default NE password, you should use the Global Password Administration feature described in this task to manually change the NE password of the Super User Login that was changed by the CIT during installation. Then, WaveStar SNMS has access to both Super User NE logins/ passwords to log into BWM and TDM 10G (STM-64) NEs.

If one or both passwords that WaveStar SNMS used to successfully log into a BWM or TDM 10G (STM-64) NE expire, WaveStar SNMS issues an *ed-PID* command to change the passwords of the NE Super User logins to SNC+01 and WBM+01.

The password aging feature for BWM and TDM 10G (STM-64) NEs can be turned off via the CIT or by issuing the appropriate TL1 command through the WaveStar SNMS Cut-Through feature. Refer to the NE hardware documenation for the TL1 command needed to turn off the password aging feature.

The new passwords are updated in the WaveStar SNMS database of the current host after they are changed. Any additional EMS hosts or CIT interfaces have to be updated with the new passwords as well to enable logging into the affected NEs. Before using this feature, make sure that you really want to proceed with changing the primary/secondary passwords.

To perform this task, access the Map window.

Task

Complete the following steps to change the primary and/or secondary passwords for the selected NE(s)/aggregate(s).

Step	Action	
1	Select one or more NEs and/or aggregates on the Map window pane or subnetwork explorer, if you know for which NEs you want to perform this function. **OR** Select no NEs and/or aggregates at this point.	
2	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.	
3	Select **Security** from the Administration menu. The Security sub-menu is displayed.	
4	Select **Global Password Administration** from the Security sub-menu. The Global Password Administration window is displayed.	
5	TO CHANGE THE PASSWORD FOR...	CLICK THE...
	■ one or more NEs	■ Show NEs radio button.
	■ one or more aggregates	■ Show Aggregates radio button.
	■ a specific NE of the same type	■ List by Type radio button. Click the down arrrow for this field to display a list of NE types, then select the NE type.
6	Select the NE(s) or aggregate(s) for which the password(s) will be changed, from the Network Elements/Aggregates list. When you select an NE or aggregate, the item moves from the Network Elements/ Aggregates List to the Chosen NEs list. You can use the arrow push buttons to move NEs/aggregates back and forth between the two lists, as needed.	

Step	Action (Contd)
7	Enter the new Primary Password for the selected NE(s)/aggregate(s) in the Primary Password field.
8	Re-enter the new Primary Password in the Re-enter Primary Password field.
9	If desired, enter a new Secondary Password in the Secondary Password field.
10	If a new Secondary Password has been entered, re-enter it in the Re-enter Secondary Password field.
11	To abort the password change operation while it is in progress, click the Abort button. To initiate the password change(s), click the Apply button. To close the window, click the Close button. **NOTE:** If the number of NEs selected is 20 or more, a pop-up message window appears, advising you that the EMS performance may be impacted and asking if you want to continue with the operation. Choose **Y** to continue with the operation or **N** to cancel the operation. A Log Browser window is displayed, showing the status of the operation. This window remains open until you close it. **Stop! End of Task.**

Add a User

Background

Use this procedure to add a user's login and access permissions for WaveStar SNMS. A unique user ID (login) must be defined for each user that accesses WaveStar SNMS.

Task

Complete the following steps to add a user login.

Step	Action
1	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.
2	Select **Security** from the Administration menu. The Security sub-menu is displayed.
3	Select **User Provisioning** from the Security sub-menu. The Manage Users window is displayed, showing the current list of user logins.
4	Click the Add button. The Add a User window is displayed.

Continued on next page

Step	Action (Contd)
5	Fill in the following fields, as needed: ❯ Name—This is the user login field. A user login must be unique and contain 3-10 alphanumeric characters with no white spaces. Uppercase and lowercase letters are allowed. No special characters are allowed. Spaces are not allowed. This field is required. ❯ Alias—This is an alternate label for the user. A user alias can be 1-20 alphanumeric characters, in any combination. Uppercase and lowercase letters are allowed. Spaces are allowed. This field is required. ❯ Password—This is the user’s password. A user password can be 6-10 characters. The password must contain at least one alpha character, one numeric character, and one special character. This field is required. ❯ Confirm Password—This field is to confirm the user’s password. If the entry in this field is not identical to the password entered in the Password field, a pop-up window is displayed with a warning message when the OK button is clicked. This field is required. ❯ Copy this user’s settings—This field is used to copy another user’s Login Type, Command Group, and Target Group settings. Click the down arrow to the right of the field to display a list of users. Select a user login from which to apply settings and then click the Load Settings button. This field is optional, and settings can be modified after these fields have been populated. **Note: this function does not copy a user’s preferences for Map display settings.**

Step	Action (Contd)
	- Login Type—This field is used to specify the type of login. The types are: — GUI—This user ID category is only allowed to access the EMS via the GUI client. Default Command Group = Empty, Default Target Group = Empty — ITM-NM—This user ID category is reserved for the interface between the EMS and ITM-NM. Default Command Group = ALL. Default Target Group = ALL. The pre-defined user ID “itm” is defined as ITM-NM. — NMS—This user ID category is reserved for the inteface between the EMS and a generic Network Management System (NMS). Both Fault and Configuration Management functionality are available to this type of user ID. Default Command Group = Privileged, Default Target Group = ALL. The pre-defined user ID “nms” is defined as NMS. — NMS-CM—This user ID category is reserved fo rthe interface between the EMS and a generic Configuration Management provisioning system. Default Command Group = Provisioning, Default Target Group = ALL. The pre-defined user ID “opsine” is defined as NMS-CM. — NMS-FM—This user ID category is reserved for the interface between the EMS and a generic Fault Management collection system. Default Command Group = Maintenance, Default Target Group = ALL. The pre-defined user ID “nma” is defined as NMS-FM. Click the down arrow to the right of the field to display the choices. Select a login type. This field is required. - Command Group—This field is used to specify which Command Group the user can access. Click the down arrow to the right of the field to display a list of choices. The choices are: Empty or a specific Command Group. Select a Command Group for user access. This field is required. - Target Group—This field is used to specify which Target Group the user can access. Click the down arrow to the right of the field to display a list of choices. The choices are: Empty or a specific Target Group. Select a Target Group for user access. This field is required.

Step	Action (Contd)
6	Click the OK button. The Status Dialog window is displayed, indicating that the user is being added to WaveStar SNMS. **Stop! End of Task.**

Modify a User

Background

Use this procedure to change a user login's attributes. The Login Type, Alias, Password, Command Group, and/or Target Group can be changed.

Before you begin

Before you begin this task, you must create a user login.

To perform this task, access the Map window.

Task

Complete the following steps to modify a user login's attributes.

Step	Action
1	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.
2	Select **Security** from the Administration menu. The Security sub-menu is displayed.
3	Select **User Provisioning** from the Security sub-menu. The Manage Users window is displayed, showing the current list of user logins.
4	Select a user login from the list.
5	Click the Modify button. The Modify User window is displayed.
6	Change the Login Type, Password, Alias, Command Group, and/or Target Group fields as desired.
7	Click the OK button. The Status Dialog window is displayed, indicating that the changes to the user login are being made by the system. **Stop! End of Task.**

Delete a User

Background

Use this procedure to delete a user login from WaveStar SNMS.

Before you begin

Before you begin this task, be aware that TL1 Macro Builder Files created by a user remain in WaveStar SNMS. These files must be removed either by the owner of the files (the user) or the system administrator.

To perform this task, access the Map window.

Task

Complete the following steps to delete a user.

Step	Action
1	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.
2	Select **Security** from the Administration menu. The Security sub-menu is displayed.
3	Select **User Provisioning** from the Security sub-menu. The Manage Users window is displayed.
4	Select the user to be deleted from the list of user logins.
5	Click the Delete button. A pop-up window is displayed, asking if you really want to delete the user.
6	Choose Yes to delete the user. **Stop! End of Task.**

Add a Command Group

Background

Use this procedure to add a Command Group. A Command Group is a set of NE and WaveStar SNMS commands that a user can use. In creating a Command Group, you can copy a set of commands from an existing command group into the new one. Command Groups can also be modified or deleted.

Task

Complete the following steps to add a Command Group.

Step	Action
1	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.
2	Select **Security** from the Administration menu. The Security sub-menu is displayed.
3	Select **Command Groups** from the Security sub-menu. The Manage Command Groups window is displayed, showing the current list of Command Groups.
4	Click the Add button. The Add a Command Group window is displayed.
5	Fill in the following fields, as needed: ■ Command Group Name—This is the Command Group name. A Command Group name cannot contain spaces. This field is required. ■ Command Group Alias—This is the Command Group alias (alternate label). This field is required. **NOTE:** If you provide an invalid Command Group name or alias, the system informs you with a warning message. ■ Copy settings from this group—This field is used to copy a set of commands from an existing Command Group into the new one. Click the down arrow to the right of the field to display a list of Command Groups. Select a Command Group from which to copy a set of commands and then click the Load Settings button. This field is optional, and the contents of the EMS and NE Command fields can be modified after this information has been copied.

Continued on next page

Step	Action (Contd)
6	Use the push buttons to move commands from the list of available commands in the EMS Commands scroll list to the EMS Commands in This Group list, as needed.
7	Use the push buttons to move commands from the list of available NE commands in the Network Elements Commands scroll list to the NE Commands In This Group list, as needed.
8	Click the Apply button to activate your choices, or click the OK button to activate your choices and close the window. The Status window is displayed, indicating the Command Group is being added to WaveStar SNMS. Click the Close button to close the Status window and return to the Map window. **Stop! End of Task.**

Modify a Command Group

Background

Use this procedure to change a Command Group once it has been created.

Before you begin

Before you begin this task, be aware that the Command Group name or alias cannot be modified.

Task

Complete the following steps to modify a Command Group.

Step	Action
1	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.
2	Select **Security** from the Administration menu. The Security sub-menu is displayed.
3	Select **Command Groups** from the Security sub-menu. The Manage Command Groups window is displayed, showing the current list of Command Groups.
4	Select the Command Group to be modified from the list.
5	Click the Modify button. The Modify Command Group window is displayed.
6	Change the Copy From Group, EMS Command List, or NE Command List as desired.
7	Click the OK button. The Status window is displayed, indicating that the changes to the Command Group are being made by WaveStar SNMS. Click the Close button to close the Status window and return to the Map window. **Stop! End of Task.**

Delete a Command Group

Background

Use this procedure to delete a Command Group from WaveStar SNMS.

Before you begin

Before you begin this task, be aware that users for the Command Group being deleted must be reassigned to another Command Group. The reassignment is done as part of this task.

To perform this task, you must first access the Map window.

Task

Complete the following steps to delete a Command Group.

Step	Action
1	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.
2	Select **Security** from the Adminstration menu. The Security sub-menu is displayed.
3	Select **Command Groups** from the Security sub-menu. The Manage Command Groups window is displayed, showing the current list of Command Groups.
4	Select the Command Group to be deleted from the list.
5	Click the Delete button.
6	The Reassign Users to Command Group window is displayed if any users are assigned to the Command Group.
7	Choose a Command Group from the list to which you want to reassign all users of the Command Group being deleted.
8	Click the OK button. The Command Group is deleted. **Stop! End of Task.**

Add a Target Group

Background

Use this procedure to add a Target Group. A Target Group is a collection of NEs to which a user has access and can execute commands. A user is assigned to one and only one Target Group and can only access the NEs in this group. WaveStar SNMS is initially loaded with two Target Groups: one for all NEs and another with no NEs. Additional Target Groups can be defined as needed by a system administrator or a user with a privileged login. In creating a Target Group, you can copy a set of NEs from an existing Target Group into the new one. Target Groups can also be modified or deleted.

Before you begin

Before you begin this task, access the Map window.

Task

Complete the following steps to add a Target Group.

Step	Action
1	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.
2	Select **Security** from the Administration menu. The Security sub-menu is displayed.
3	Select **Target Groups** from the Security sub-menu. The Manage Target Groups window is displayed, showing the current list of Target Groups.
4	Click the Add button. The Add a Target Group window is displayed.

Step	Action (Contd)
5	Fill in the following fields, as needed: ■ Target Group Name—This is the Target Group name. A Target Group name cannot contain spaces. This field is required. ■ Target Group Alias—This is the Target Group alias (alternate label). This field is required. **NOTE:** If you provide an invalid Target Group name or alias, the system informs you with an error message. ■ Copy settings from this group—This field is used to copy a set of NEs from an existing Target Group into the new one. Click the down arrow to the right of the field to display a list of Target Groups. Select a Target Group from which to copy a set of NEs and then click the Load Settings button. This field is optional, and the contents of the Target Group can be modified after this information is copied.
6	Use the push buttons to move NEs from the Network Element list scroll list to the NEs in This Group list, as needed.
7	Click the OK button. The Status window is displayed, indicating that the Target Group is being added to WaveStar SNMS. Click the Close button to close the Status window and return to the Map window. **Stop! End of Task.**

Modify a Target Group

Background

Use this procedure to change a Target Group once it has been created.

Before you begin

Before you begin this task, be aware that the Target Group name or alias cannot be modified. Certain Target Groups cannot be modified or deleted; this is indicated on the Target Group Manager window.

To perform this task, access the Map window.

Task

Complete the following steps to modify a Target Group.

Step	Action
1	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.
2	Select **Security** from the Administration menu. The Security sub-menu is displayed.
3	Select **Target Groups** from the Security sub-menu. The Manage Target Groups window is displayed, showing the current list of Target Groups.
4	Select the Target Group to be modified from the list.
5	Click the Modify button. The Modify Target Group window is displayed.
6	Change the Copy From Group, and/or NEs in This Group fields, as desired.
7	Click the OK button. The Status Dialog window is displayed, indicating that the changes to the Target Group are being made by WaveStar SNMS. **Stop! End of Task.**

Delete a Target Group

Background

Use this procedure to delete a Target Group from WaveStar SNMS.

Before you begin

Before you begin this task, be aware that users of the Target Group to be deleted must first be reassigned to another Target Group. The reassignment is done as part of this task. Certain Target Groups cannot be modified or deleted; this is indicated on the Target Groups Manager window.

To perform this task, access the Map window.

Task

Complete the following steps to delete a Target Group.

Step	Action
1	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.
2	Select **Security** from the Administration menu. The Security sub-menu is displayed.
3	Select **Target Groups** from the Security sub-menu. The Manage Target Groups window is displayed, showing the current list of Target Groups.
4	Select the Target Group to be deleted from the list.
5	Click the Delete button.
6	The Reassign Users to Target Group window is displayed if there are any users assigned to the Target Group.
7	Choose a Target Group from the list to which you want to reassign all users of the Target Group being deleted.
8	Click the OK button. The Target Group is deleted. **Stop! End of Task.**

Add an NE Login

Background

Use this procedure to add an OLS 400G NE login.

Before you begin

Before you begin this task, the NE(s) to which you want to add the OLS 400G NE login must exist in WaveStar SNMS. Be aware that this feature is only available for OLS 400G NEs.

To perform this task, access the Map window.

Task

Complete the following steps to add an NE login to an OLS 400G NE.

Step	Action
1	Select an NE on the Map window. For instructions on selecting an NE, see the sub-procedure Selecting NEs and Aggregates on the Map Pane immediately following this procedure. **OR** Select no NE at this point.
2	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.
3	Select **Security** from the Administration menu. The Security sub-menu is displayed.
4	Select **NE Login Administration** from the Security sub-menu. If you did not choose an NE in Step 1, the Choose an NE window is displayed. Choose an NE from the list by double-clicking on the NE’s TID. The chosen NE is highlighted. Click the OK button. The Manage NE Login window for the chosen NE is displayed, showing the current list of NE logins.
5	Click the Add button. The Add login window for the chosen NE is displayed.

Continued on next page

Step	Action (Contd)
6	Fill in the following fields, as needed: ■ Login—This is the NE login. Up to 20 characters are allowed. This field is required. ■ Password—This is the NE login's password. Up to 20 characters are allowed. This field is required. ■ Copy this user's settings—click the down arrrow next to this field to display a list of NE logins from any applicable NE from which to copy login settings; in other words, the User Privilege Code(s) that define the level of NE access for the selected NE login. To load/display the User Privilege Codes for the NE login to be copied from, click the Load Settings button directly below the Copy this user's settings field. This field is optional. **Note: this function does not copy another login or password, which cannot be copied from another user).** ■ Login Type: (Check the Box, if this User is a Temporary User)—Click on this box to place a check in it if the NE login being created is for a temporary user. This field is optional. If this option is selected, enter a date (in MM-DD-YYYY format) in the User ID Expiration Date field. ■ User Privilege Code—This is the User Privilege Code field. Enter one or more User Privilege Codes to specify the level of NE access for this NE login. Enter an ampersand (&) between each User Privilege Code when entering more than one. ■ Passwords will expire after—This is the Password Aging field. Click the up and down arrows on this spinner field to select the number of days after which the specified password will expire. The default is 90 days. If you select 0 or leave the value at 0, the password will not expire for this NE login. This field is required.

Continued on next page

Step	Action (Contd)
7	Click the Apply or OK button to activate your choices. A status dialog window is displayed, indicating that the NE login request is being processed. When it is finished, the NE login has been added. **Stop! End of Task.**

SE 1-1: Selecting NEs and Aggregates on the Map Pane

Procedure

To select a single NE or aggregate on the Map pane, position the mouse pointer over the NE or aggregate icon and click the select mouse button.

To select a group of NEs or aggregates on the Map pane.

1. Position the mouse pointer over a portion of the background adjacent to the items to be selected.
2. Click the mouse select button and drag the mouse pointer. As you drag the mouse pointer, an outlined box appears over the selected area.
3. Drag the mouse pointer over the NE(s)/aggregate(s) to be selected, enclosing them in the selection box. As items in the Map pane are selected, they change color. Release the mouse select button. The items are selected.

To deselect a selected item in the Map pane, position the mouse pointer over the itme and single-click the mouse select button. To deselect a group of items, position the mouse pointer within the boxed region and single-click the mouse select button. Any item in the box that is already selected becomes deselected.

Modify an NE Login

Background

Use this procedure to modify the attributes of an OLS 400G NE login. If the same NE login is used for more than one NE, the same changes can be made for every NE using that login.

Before you begin

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

Task

Complete the following steps to modify an NE login for an OLS 400G NE.

Step	Action
1	Select an NE on the Map window. For instructions on selecting an NE, see the sub-procedure Selecting NEs and Aggregates on the Map Pane immediately following this procedure. **OR** Select no NE at this point.
2	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.
3	Select **Security** from the Administration menu. The Security sub-menu is displayed.
4	Select **NE Login Administration** from the Security sub-menu. If you did not choose an NE in Step 1, the Choose an NE window is displayed. Choose an NE from the list by double-clicking on the NE’s TID. The chosen NE is highlighted. Click the OK button. The Manage NE Login window for the chosen NE is displayed, showing the current list of NE logins.
5	Select the NE login to be modified from the list of NE logins. *Continued on next page*

Step	Action (Contd)
6	Click the Modify button. The Modify window for the chosen NE login is displayed.
7	Change the Password, Password Aging, Copy this user’s settings, Login Type, User ID Expiration Date (for the Login Type field), and User Privilege Code fields as desired.
8	Click the OK or Apply button to activate your choices. A status dialog window is displayed, indicating that your modifications are being processed. When it is finished, the modifications have been applied to the NE login. **Stop! End of Task.**

SE 1-2: Selecting NEs and Aggregates on the Map Pane

Procedure

To select a single NE or aggregate on the Map pane, position the mouse pointer over the NE or aggregate icon and click the select mouse button.

To select a group of NEs or aggregates on the Map pane.

1. Position the mouse pointer over a portion of the background adjacent to the items to be selected.
2. Click the mouse select button and drag the mouse pointer. As you drag the mouse pointer, an outlined box appears over the selected area.
3. Drag the mouse pointer over the NE(s)/aggregate(s) to be selected, enclosing them in the selection box. As items in the Map pane are selected, they change color. Release the mouse select button. The items are selected.

To deselect a selected item in the Map pane, position the mouse pointer over the itme and single-click the mouse select button. To deselect a group of items, position the mouse pointer within the boxed region and single-click the mouse select button. Any item in the box that is already selected becomes deselected.

Delete an NE Login

Background

Use this procedure to delete an NE login that is being used for an OLS 400G NE.

Before you begin

Before you begin this task, be aware than you cannot delete an OLS 400G NE login with a Super-Use Authorization Code from an OLS 400G NE. Be aware that this feature is only available for OLS 400G NEs.

Task

Complete the following steps to delete an NE login from an OLS 400G NE.

Step	Action
1	Select an NE on the Map window. For instructions on selecting an NE, see the sub-procedure Selecting NEs and Aggregates on the Map Pane immediately following this procedure. **OR** Select no NE at this point.
2	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.
3	Select **Security** from the Administration menu. The Security sub-menu is displayed.
4	Select **NE Login Administration** from the Security sub-menu. If you did not choose an NE in Step 1, the Choose an NE window is displayed. Choose an NE from the list by double-clicking on the NE’s TID. The chosen NE is highlighted. Click the OK button. The Manage NE Login window for the chosen NE is displayed, showing the current list of NE logins.
5	Select the NE login to be deleted from the list of NE logins.
6	Click the Delete button. A pop-up window is displayed, asking if you really want to delete the NE login.
7	Choose Yes to delete the NE login. **Stop! End of Task.**

SE 1-3: Selecting NEs and Aggregates on the Map Pane

Procedure

To select a single NE or aggregate on the Map pane, position the mouse pointer over the NE or aggregate icon and click the select mouse button.

To select a group of NEs or aggregates on the Map pane.

1. Position the mouse pointer over a portion of the background adjacent to the items to be selected.
2. Click the mouse select button and drag the mouse pointer. As you drag the mouse pointer, an outlined box appears over the selected area.
3. Drag the mouse pointer over the NE(s)/aggregate(s) to be selected, enclosing them in the selection box. As items in the Map pane are selected, they change color. Release the mouse select button. The items are selected.

To deselect a selected item in the Map pane, position the mouse pointer over the itme and single-click the mouse select button. To deselect a group of items, position the mouse pointer within the boxed region and single-click the mouse select button. Any item in the box that is already selected becomes deselected.

Terminate User Session

Background

Use this procedure to terminate one or more active user login sessions. When you terminate an active user session, the system gracefully exits out of the current session and does not cause any pending or scheduled tasks to be aborted. The user login that was terminated can start a new login session after the login/ password is validated.

Before you begin

Before you begin this task, see if the user is currently on the system via the Display Users window.

To perform this task, access the Map window.

Task

Complete the following steps to terminate one or more active user login sessions.

Step	Action
1	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.
2	Select **Security** from the Administration menu. The Security sub-menu is displayed.
3	Select **Terminate User Session** from the Security sub-menu. The Terminate EMS User Sessions window is displayed.
4	Select the user login(s) to be terminated from the Users Currently Logged list and, using the arrow push buttons, move the selected user login(s) to the User Sessions to be Terminated list. You can use the the arrow push buttons to move user logins back and forth between the two lists, as needed.
5	Click the OK button. A pop-up question dialog window is displayed, confirming that you have selected to terminate the user(s) session and asks if you to want to continue with the termination.
6	Choose Yes. Active GUI sessions for the user(s) selected are terminated. **Stop! End of Task.**

Enable/Disable User Logins

Background

Use this procedure to enable or disable user logins. Disabling a user login prevents that user from being able to log into WaveStar SNMS. If you disable a user login that is currently on the system, that user’s GUI session is automatically terminated. If there is a standing alarm against a user login that has been disabled, re-enabling the user login clears the alarm against it.

Before you begin

Before you begin this task, be aware that the *snms* login and other pre-defined logins may not be disabled. To see if a user is currently on the system, access the Display Users window through the GUI.

To perform this task, access the Map window.

Task

Complete the following steps to enable or disable one or more user logins for starting a GUI session.

Step	Action	Action
1	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.	
2	Select **Security** from the Administration menu. The Security sub-menu is displayed.	

Step	Action (Contd)	Action
3	Select **Disable/Enable Users** from the Security sub-menu. The Disable/Enable User Sessions window is displayed.	
4	TO ... ■ disable one or more users ■ enable one or more users **NOTE:** You can use the arrow push buttons to move users back and forth between the two lists, as needed.	SELECT ... ■ the user(s) in the Enabled Users list and move the user(s) to the Disabled Users list, using the arrow push buttons. ■ the user(s) in the Disabled Users list and move the user(s) to the Enabled User list, using the arrow push buttons.
5	Click the OK button. If you are disabling one or more users, a pop-up confirmation window is displayed, asking if you really want to prevent the selected user(s) from establishing login sessions. Choose Yes to disable the user(s). If you are enabling one or more users, a pop-up window is displayed asking if you want to enable the selected users. Choose Yes to enable the user(s). **Stop! End of Task.**	

Display Logged In Users

Background

Use this procedure to display all users that are currently logged into WaveStar SNMS.

Before you begin

Before you begin this task, access the Map window.

Task

Complete the following steps to display all users that are currently logged into WaveStar SNMS.

Step	Action
1	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.
2	Select **Security** from the Administration menu. The Security sub-menu is displayed.
3	Select **Display Logged-In Users** from the Security sub-menu. The Display Users window is displayed, showing, in table format, a list of users that are currently logged into the system, their user alias, and their login source.
4	Click the Close button to close the window. **Stop! End of Task.**

Globally Provision User Login/ Password Parameters (Global Security Provisioning Feature)

Background

Use this procedure to globally administer certain aspects of user login/password procedures enforced by WaveStar SNMS, such as the number of login attempts allowed, the login expiration period, the password aging interval, and the password history.

Before you begin

Before you begin this task, make sure that you are the administrator or a user with a privileged login allowed to provision these login/password parameters.

To perform this task, access the Map window.

Task

Complete the following steps to globally provision login/password parameters for users logging into WaveStar SNMS.

Step	Action
1	Select **Administration** from the main menu bar on the Map window. The Administration menu is displayed.
2	Select **Security** from the Administration menu. The Security sub-menu is displayed.

Continued on next page

Step	Action (Contd)
3	Select **Global Security Provisioning** from the Security sub-menu. The Global Security Provisioning window is displayed.
4	Fill in the following fields, as needed: ■ Allow user unsuccessful login attempts before disabling login ID—click the up and down arrows on this spinner field to select the number of consecutive failed login attempts before disallowing a user to log into the system. The default is three tries. ■ Delete login IDs after *x* days of user inactivity—click the up and down arrows on this spinner field to select the number of days that a user login is not in use before it expires (in other words, cannot be used to log into the system). The default is 45 days. ■ Prompt users to change passwords every *x* days—click the up and down arrows on this spinner field to select the number of days that a password can be used before it has to be changed. The default is 30 days. ■ Warn users *x* days prior to their password aging—click the up and down arrows on this spinner field to select the number of days prior to passwords expiring that a warning notice is issued. The default is seven days. ■ Remember users' last *x* previous passwords (and don't allow users to use thse previous passwords)—click the up and down arrows on this spinner field to select the number of previous passwords recalled and prohibited from being re-used. The default number is five passwords. ■ Session inactivity timeout interval—click the up and down arrows on this spinner field to select, in minutes, the session inactivity timeout interval before the user's GUI session automatically terminates. The default is 30 minutes. Setting the timeout interval to zero disables session timeout; a GUI session does not automatically terminate. ■ Enter an advisory message that users will see upon login—enter the text advisory message that is displayed to the user upon successfully logging into WaveStar SNMS. **NOTE:** Click the Get Defaults button to retrieve and display the system defaults for the numeric value fields.
5	Click the Apply button to activate your choices, or click the OK button to activate your choices and close the window. **Stop! End of Task.**

Convert to Trusted Mode System

Background

Use this procedure to convert the WaveStar SNMS host operating system to a "trusted mode" system.

In addition to the security mechanisms avaiable in the standard UNIX environment, HP-UX offers a utility for converting a host system into a "trusted" system which offers a greater security via mor stringent password and authentication policies.

Before you begin

Conversion to a trusted system should take should take place only after a successful coldStart installation has been completed. For details about coldStart installation procedures, see the *WaveStar SNMS Installation Guide*. In many cases, the ColdStart program needs to be re-run after the conversion. However, the system must be converted back to non-trusted mode before re-running coldStart.

Before converting to a trusted system, the locally defined NIS server and client have to be removed using the HP SAM tool. Otherwise, the conversion will not proceed. If the conversion still fails after removing the NIS server/client, check the file */etc/rc.confg.d/namesvrs* to make sure that NIS_MASTER_SERVER, NIS_SLAVE_SERVER and NIS_CLIENT are all set to 0.

Task

Complete the following steps to convert the WaveStar SNMS host operating system to "trusted mode"..

Step	Action
1	Using the HP SAM tool, highlight **Auditing and Security** and activate **Open** to get to the **Convert to Trusted System** prompt.
2	Select **Convert to Trusted System**.
3	At the confirmation prompt, press **Y** to begin the conversion process. **Result:** This conversion process: - creates a new protected password database (shadow password files) in */tcb/files/auth/* - replaces the password field in */etc/passd* with an asterisk (*) - forces all users to use passwords - creates an audit ID number for each user - sets the audit flag on for all existing users **NOTE:** After the system has been converted to a trusted system, each user’s security policy must be modified using the remaining steps in this procedure.
4	Select **Account for Users and Groups**
5	Select Users
6	Highlight the desired user and select **Modify Security Policy** *Continued on next page*

Step	Action (Contd)
7	Make sure that the **Password Format Policies** has the default settings as follows: › **Password Aging Policies**—**Disable Aging** › **General User Account Policies**—the **Infinite** setting for **Account Life Time** › **Max Period of Inactivity on Account**—**None** › **Unsuccessful Login Tries Allowed**—**20**
8	Select **OK** to confirm the changes.
9	Log into the WaveStar SNMS host as `root`. **Result:** If the new user password and authentication changes are in effect, the system displays two messages indicating the last successful login date/time for `root` and the last unsuccessful login as NEVER When logging in for the first time in “trusted mode”, the system prompts for a password change. ⇒ **NOTE:** Any changes to user accounts once the system has successfully been converted to “trusted mode” should be done using the SAM tool. **Stop! End of Task.**

System Administration

2

Introduction

Summary

This chapter describes the procedures for stopping, restarting, and rebooting a simplex (non-redundant) WaveStar SNMS system.

Contents

The following procedures are discussed in this chapter:

Bring Down the WaveStar SNMS Application (Non-Redundant System)

Background

The WaveStar SNMS application runs continuously on the host computer under normal operating conditions, gathering and routing network information. The procedures in this section describe how to start and stop the execution of the WaveStar SNMS application on a simplex (non-redundant) host computer should this become necessary.

NOTE:
Ordinarily the WaveStar SNMS application is stopped only under the following conditions:

- The host computer needs to be rebooted
- The WaveStar SNMS database needs to be restored
- A power outage affects the host computer
- A WaveStar SNMS problem needs to be corrected

Task

Perform the following steps to bring down the WaveStar SNMS application.

Step	Action
1	Log on to the WaveStar SNMS host computer using the `ems` login.
2	At the system prompt type **dn** and press the Return key.
3	After it's down, confirm that the application is in shutdown mode by typing **appstat** and then pressing the Return key. **Stop! End of Task.**

Bring Up the WaveStar SNMS Application

Task

Perform the following steps to bring up the WaveStar SNMS application.

Step	Action
1	Log on to the WaveStar SNMS host computer using the `ems` login.
2	At the system prompt type **up** and press the Return key.
3	When your screen displays a prompt asking whether to delete trace files, respond with **y** and press the Return key, unless the trace files are needed to diagnose a system problem.
4	Confirm that the application is running and that processes are not respawning by typing **appstat** and then pressing the Return key. **Stop! End of Task.**

Reboot the WaveStar SNMS Application (Using Shutdown Command) (Non-Redundant System)

Background

The Shutdown Command can be used to reboot the WaveStar SNMS application. This command will gracefully shut down the WaveStar SNMS application and Informix database and reboot the system.

NOTE:
Before rebooting the WaveStar SNMS application using the Shutdown command as described below, the system console **must** be powered on.

Task

Perform the following steps to reboot the WaveStar SNMS application.

Step	Action
1	Log in as `root` to the WaveStar SNMS host computer. **Result:** A # prompt is displayed.
2	Enter the following command: **cd /**
3	At the system prompt type **/etc/shutdown -r -y 0** and press the Return key. (r=reboot, y=yes, 0=now) **Stop! End of Task.**

Database Maintenance

3

Introduction

Summary

This chapter provides basic procedures for backing up and restoring the WaveStar SNMS database and exporting the database.

Before you begin

The procedures described in this chapter assume that you are working with a WaveStar SNMS database from the same release. If you are converting a WaveStar SNMS database from a different release, call 1-800-225-4672 for technical assistance.

Contents

The following procedures are discussed in this chapter:

Back Up the WaveStar SNMS Database

Background

Maintaining tape backups of the database is critical to the overall reliability of WaveStar SNMS. If a hardware failure or other mishap occurs, service disruptions resulting from loss of data can be minimized when a recently backed-up version of the database is available.

Before you begin

Consider the following items as you prepare for database backups:

- You must be able to physically access the WaveStar SNMS host computer to insert and remove backup tapes.
- The database should be backed up at least once a week (more frequently when disk activity is high).
- In addition to the above recommendations, a backup should be verified and saved permanently off-site every six months. This is an additional safeguard against problems resulting from a faulty tape and/or tape drive.
- A WaveStar SNMS database backup requires one or more tapes depending upon the size of the database.
- Be sure to label backup tapes with the date and contents of the tape as instructed by the Informix backup and restore processes.
- Restoring the WaveStar SNMS database requires that you bring the WaveStar SNMS system down and take the Informix database program off-line.

Task

Perform the following steps to back up the WaveStar SNMS application.

Step	Action
1	Insert a tape into the tape drive of the SNMS host computer.
2	To archive the database, you must log in as the Informix user. You can do this while logged in using your normal login by typing **su - informix** and pressing the Return key. (su - informix needs space before and after dash). **NOTE:** The WaveStar SNMS application does not have to be brought down to perform an archive.

3	At the system prompt, type **ontape -s -L 0** and press the Return key.
	Result: The following prompt is displayed:
	`Please mount tape 1 on /dev/rmt/0m and press the` Return `key to continue.`
	`10 percent done.`
	`100 percent done.`
	NOTE:
	An archive can take anywhere from 30 minutes to several hours, depending on the amount of data.

4	When the archive is complete, messages similar to the following appear:
	`Please label this tape as number 1 in the arc tape sequence.`
	`This tape contains the following logical logs:`
	`126`
	`Program over.`
	Stop! End of Task.

Restore the WaveStar SNMS Database

Task

The following procedure is used for restoring the WaveStar SNMS database.

NOTE:
The WaveStar SNMS application **must** be down to execute the restore procedure, and you **must** have the same database configuration.

Step	Action
1	Log into the WaveStar SNMS host using the `ems` login.
2	Bring the WaveStar SNMS application down by typing **dn** and pressing the Return key at the system prompt.
3	Log into Informix by entering **su - informix** at the system prompt. Press the Return key.
4	Make sure you have a correct *onconfig* file and *sqlhosts* file in /tools/informix/etc directory and *.profile* in the */tools/informix* directory.
5	Type **onmode -ky** to bring the Informix server offline.

6	To start the restore process, type **ontape -r** at the system prompt and press the Return key.
	
	Result: Prompts are displayed similar to:
	`Continue Restore (y/n):` **y**
	`Do you want to back up the logs? (y/n):` **n**
	`Restore a level 1 archive? (y/n):` **n**
	`Do you want to restore log tapes?` **n**
	`/tools/informix/bin/onmode -sy`
	
	`Program over.`

7	Type **onmode -m** and press the Return key to put Informix in online mode

Step	Action (Contd)
8	To confirm Informix is in online status, type **onstat -** and press the Return key. **Result:** The output is similar to the following: INFORMIX-OnLine Version 7.31 uc2xc--On-Line--Up 00:23:56 ---116936 Kbytes
9	Log out of Informix.
10	Start the WaveStar SNMS application by typing **up** and pressing the Return key at the system prompt. **Stop! End of Task.**

Back Up WaveStar SNMS Application and DSA Data

Background

Use this procedure to back up key WaveStar SNMS application data and database data, including NE directory information maintained by the Directory Services Agent (DSA). You have the option of backing up one database or set of application data at a time. You can back up the data to a single tape or multiple tapes.

Task

Complete the following steps to do a backup of the desired application data or database data.

Step	Action
1	Log into the WaveStar SNMS host using the ems login.
2	At the UNIX prompt, enter the **ems_backup** command. The form of the command is: **ems_backup [-d EMS|CF|PM|NQ|NCI|] [-one] [-app]** where: **-d** - back up one database at a time: ■ **EMS** - Informix database ■ **CF** - Configuration data ■ **PM** - Performance Monitoring data ■ **NQ** - Northbound CMISE data ■ **NCI** - CORBA interface data **-one** - back up all data onto one tape. Default is multiple tapes. If the **-one** option is used, you would insert one blank tape in the tape drive and execute the command **ems_backup -one** **-app** - back up only application data and DSA data **Stop! End of Task.**

Restore WaveStar SNMS Application and DSA Data

Background

Use this procedure to restore key WaveStar SNMS application data and database data, including NE directory information maintained by the Directory Services Agent (DSA). You have the option of restoring one database or set of application data at a time. You can restore the data from a single tape or multiple tapes.

Task

Complete the following steps to restore the desired application data or database data.

Step	Action
1	Log into the WaveStar SNMS host using the `ems` login.
2	At the UNIX prompt, enter the **ems_recover** command. The form of the command is: **ems_recover [-d EMS|CF|PM|NQ|NCI|] [-one] [-app]** where: **-d** - restore one database from tape: ■ **EMS** - Informix database ■ **CF** - Configuration data ■ **PM** - Performance Monitoring data ■ **NQ** - Northbound CMISE data ■ **NCI** - CORBA interface data **-one** - restore all data from one tape. Default is multiple tapes. If the **-one** option is used, you would insert one blank tape in the tape drive and execute the command **ems_recover -one** **-app** - restore only application data and DSA data from tape **Stop! End of Task.**

Export the WaveStar SNMS Database to a Directory

Background

A copy of the database can also be exported to an ASCII text format. This would allow you to transfer the database to another Informix environment that is configured differently. A minimum of five tapes are needed for this.

Task

The following procedure is used to perform a database export to a directory.

NOTE:
The WaveStar SNMS application **must** be shut down before doing a database export. Backup /ems/dsa directory to ensure system consistency after restart.

Step	Action
1	Log in as **ems**.
2	Bring the WaveStar SNMS application down.
3	At the UNIX prompt, use the following commands to back up the WaveStar SNMS database to a directory (execute each command individually): **dbexport $EMS_DBNAME -c -ss -o <directory>** **echo $NUMOFCFDBS** **dbexport ${CF_DBNAME}n -c -ss -o <directory>** (n is a single digit number from 1 to $NUMOFCFDBS. Repeat command with different n if n>1) **dbexport $PM_DBNAME -c -ss -o <directory>** (only if PM is collected) **dbexport $NQ_DBNAME -c -ss -o <directory>** (only for northbound CMISE) **dbexport $NCI_DBNAME -c -ss -o <directory>** (only for CORBA interface)
4	After each DB export command, the message “dbexport complete” indicates the procedure has been successfully completed. **Stop! End of Task.**

Export the WaveStar SNMS Database to Tape

Procedure

The following procedure is used to perform a database export to tape.

Step	Action
1	Log in as `ems`.
2	Bring the WaveStar SNMS application down.
3	At the UNIX prompt, use the following commands to back up the WaveStar SNMS database to tape. **NOTE:** Put in a new tape before executing each command. Each command may require more than one tape. Swap a new tape by following the instruction from the prompt. **dbexport $EMS_DBNAME -c -ss -t /dev/rmt/0m -b 512 -s 2000000** **echo $NUMOFCFDBS** **dbexport ${CF_DBNAME}n -c -ss -t/dev/rmt/0m -b 512 -s 2000000** Note: n is a single digit number from 1 to $NUMOFCFDBS. Repeat command with different n if n>1. **dbexport $PM_DBNAME -c -ss -t /dev/rmt/0m -b 512 -s 2000000** (only if PM is collected) **dbexport $NQ_DBNAME -c -ss -t /dev/rmt/0m -b 512 -s 2000000** (only for northbound CMISE) **dbexport $NCI_DBNAME -c -ss -t /dev/rmt/0m -b 512 -s 2000000** (only for CORBA interface)
4	After each DB export command, the message “dbexport complete” indicates the procedure has been successfully completed. **Stop! End of Task.**

Import the WaveStar SNMS Database from a Directory

Background

A copy of the database can also be “imported” from a database exported by **dbexport** (described previously).

NOTE:
The WaveStar SNMS application **must** be shut down before doing a database import. You must restore */ems/dsa* directory to ensure system consistency after restart.

Task

The following procedure is used to perform a database import from a directory.

Step	Action
1	Log in as `ems`.
2	If a WaveStar SNMS database exists, drop it by running the following command at the UNIX prompt (be careful using this command): **drdb** *Continued on next page*

Step	Action (Contd)
3	Use the following commands at the UNIX prompt: **dbimport $EMS_DBNAME -d snc_dbs -c -i <directory><Enter>** db_logging -U $EMS_DBNAME echo $NUMOFCFDBS dbimport ${CF_DBNAME}n -d snc_dbs -c -i <directory><Enter> db_logging -U ${CF_DBNAME}n (n is a single digit number from 1 to $NUMOFCFDBS. Repeat command with different n if n>1). dbimport $PM_DBNAME -d pm1_dbs -c -i <directory><Enter> (only if PM is collected) db_logging -U $PM_DBNAME If get_dbmodel returns SUPREME or SUPREME-N: dbimport $NQ_DBNAME -d nq1_dbs -c -i <directory> (only for northbound CMISE) db_logging -U $NQ_DBNAME Otherwise: dbimport $NQ_DBNAME -d fm2_dbs -c -i <directory><Enter> (only for northbound CMISE) db_logging -U $NQ_DBNAME If get_dbmodel returns SUPREME or SUPREME-N: dbimport $NCI_DBNAME -d nq1_dbs -c -i <directory><Enter> (only for CORBA interface) db_logging -U $NCI_DBNAME Otherwise: dbimport $NCI_DBNAME -d fm2_dbs -c -i <directory><Enter> (only for CORBA interface) db_logging -U $NCI_DBNAME
4	After each DB import command, the message “dbimport complete” indicates the procedure has been successfully completed. **Stop! End of Task.**

Import the WaveStar SNMS Database from Tape

Task

The following procedure is used to perform a database import from tape.

Step	Action
1	Log in as `ems`.
2	If a WaveStar SNMS database exists, drop it by running the following command at the UNIX prompt (be careful using this command): **drdb** *Continued on next page*

Step	Action (Contd)
3	Use the following commands at the UNIX prompt: **dbimport $EMS_DBNAME -d snc_dbs -c -t /dev/rmt/0m -b 512 -s 2000000** **db_logging -U $EMS_DBNAME** **echo $NUMOFCFDBS** **dbimport ${CF_DBNAME}n -d snc_dbs -c -ss -t/dev/rmt/0m -b 512 -s 2000000** **dblogging -U ${CF_DBNAME}n** (n is a single digit number from 1 to $NUMOFCFDBS. Repeat command with different n if n>1). **dbimport $PM_DBNAME -d pm1_dbs -c -t /dev/rmt/0m -b 512 -s 2000000** (only if PM is collected) **db_logging -U $PM_DBNAME** If **get_dbmodel** returns SUPREME or SUPREME-N: **dbimport $NQ_DBNAME -d nq1_dbs -c -t /dev/rmt/0m -b 512 -s 2000000** (only for northbound CMISE) **db_logging -U $NQ_DBNAME** Otherwise: **dbimport $NQ_DBNAME -d fm2_dbs -c -t /dev/rmt/0m -b 512 -s 2000000** (only for northbound CMISE) **db_logging -U $NQ_DBNAME** If **get_dbmodel** returns SUPREME or SUPREME-N: **dbimport $NCI_DBNAME -d nq1_dbs -c -t /dev/rmt/0m -b 512 -s 2000000** (only for CORBA interface) **db_logging -U $NCI_DBNAME** Otherwise: **dbimport $NCI_DBNAME -d fm2_dbs -c -t /dev/rmt/0m -b 512 -s 2000000** (only for CORBA interface) **db_logging -U $NCI_DBNAME**
4	After each DB import command, the message “dbimport complete” indicates the procedure has been successfully completed. **Stop! End of Task.**

Management Communication of WaveStar SNMS

4

Introduction

Summary

This chapter describes how to set up the interfaces to communicate with the NEs for all supported communication protocols.

Contents

The following topics are covered in this chapter.

Configure OSI in the WaveStar SNMS Host

Description

The WaveStar SNMS IAO-LAN interface provides an OSI standard, high-speed communications path to NEs. It enables the reduction of performance bottlenecks by providing faster communications between the EMS and NEs. The OSI LAN interface provides up to three high bandwidth communication paths or OSI associations to NEs. This communication model is based on the standard 7-layer OSI stack reference model.

Task

The following procedure is used for configuring OSI in the WaveStar SNMS host. The LAN card should be configured before running install.

Step	Action
1	Bring down the SNMS application by typing **dn**.
2	su to root.

Continued on next page

Step	Action (Contd)
3	Get the number or MAC address of the LAN card by using lanscan. (This is also done automatically).
4	Run installEms.
5	Select option #4) Configure EMS - making the provisioned parameters effective. **Result:** You will be prompted to select the OSI configuration options. **Notes:** 1. You will need a separate LAN card for the OSI LAN. There needs to be one LAN card for the SNMS local LAN and another card for the OSI to Network Element communications. 2. It is also recommended that each LAN card is connected to a different hub, as the hubs can sometimes cause communication problems. 3. For LAN redundancy you will need 2 LAN cards for OSI. You should also put a separate hub for each LAN card for extra redundancy. (Remember you cannot use the workstation LAN card for redundancy. You will need to purchase another LAN card for OSI support.) 4. LAN Cards 0 and 1 are part of the HP machine. They can be found on the back of the host. The HP host counts LAN cards from top left to bottom right. 5. When using external LAN cards you must power down the machine and move the LAN card jumpers from INT to EXT. The front two jumpers should be on. 6. Both LAN cards should be on a different SUBNET. **Stop! End of Task.**

Configure OSI and TCP/IP on Separate LAN Cards

Background

To configure OSI and TCP over OSI communications on different network interfaces, a total of at least three network cards are needed. One of them will be for general network purposes (remote shell/support), one for OSI and one for TCP over OSI communications.

As an example, suppose that we have 3 cards as seen below. We will use lan0 for OSI, lan1 for TCP over OSI, and lan2 for general network purposes.

```
# lanscan

Hardware Station       Crd Hdw     Net-Interface NM  MAC   HP-DLPI DLPI

Path     Address       In# State    NamePPA       ID  Type      Support Mjr#

10/4/4.1 0x0800095A7953 0   UP        lan0 snap0     1   ETHER     Yes     119

10/4/8   0x001083348188 1   UP        lan1 snap1     2   ETHER     Yes     119

10/12/6  0x001083278A69 2   UP        lan2 snap2     3   ETHER     Yes     119
```

Task

The following procedure is used for configuring OSI and TCP over OSI communications on different network interfaces. The LAN cards should be configured before running install.

Step	Action
1	Configure the LAN cards: **# ifconfig lan0** **lan0: flags=843<UP,BROADCAST,RUNNING,MULTICAST>** **inet 172.100.100.50 netmask ffff0000 broadcast 172.30.255.255** **# ifconfig lan1** **lan1: flags=843<UP,BROADCAST,RUNNING,MULTICAST>** **inet 192.192.0.100 netmask ffff0000 broadcast 192.192.255.255** **# ifconfig lan2** **lan2: flags=843<UP,BROADCAST,RUNNING,MULTICAST>** **inet 135.10.100.100 netmask ffff0000 broadcast 135.17.255.255**

Continued on next page

Step	Action (Contd)
2	Run installEms.
3	Select option #4) Configure EMS - making the provisioned parameters effective.
4	You will see the following screen output. User input to the screen prompts is shown in bold. Do you wish to continue with this installation (y/n)? **y** Do you wish to backup the EMS application database(y/n/q)? **n** 1. CD-ROM 2. Digital Audio Tape (DAT) Please enter the software media type [1/2/q]? Are you ready to proceed? (y) to proceed, <CR> to skip, or (q) to quit: **y** Hit <CR> to continue .... **<CR>** Are you ready to proceed? (y) to proceed, <CR> to skip, or (q) to quit: The EMS new host Informix Database configuration is about to begin. The Informix Database configuration will use socket instead of share memory. Please adjust your Name Service Switch accordingly. Do you want to continue this process (y/n/q): **n** Press [ENTER] to continue.

Continued on next page

Step	Action (Contd)
2	Run installEms.
3	Select option #4) Configure EMS - making the provisioned parameters effective.
4	You will see the following screen output. User input to the screen prompts is shown in bold. Do you wish to continue with this installation (y/n)? **y** Do you wish to backup the EMS application database(y/n/q)? **n** 1. CD-ROM 2. Digital Audio Tape (DAT) Please enter the software media type [1/2/q]? Are you ready to proceed? (y) to proceed, <CR> to skip, or (q) to quit: **y** Hit <CR> to continue .... **<CR>** Are you ready to proceed? (y) to proceed, <CR> to skip, or (q) to quit: The EMS new host Informix Database configuration is about to begin. The Informix Database configuration will use socket instead of share memory. Please adjust your Name Service Switch accordingly. Do you want to continue this process (y/n/q): **n** Press [ENTER] to continue.

Continued on next page

Step	Action (Contd)
5	The system responds with: The following LAN interface(s) have been detected: lan 0 10/4/4 lan0 CLAIMED INTERFACE HP J2146A - 802.3 LAN lan 1 10/4/8 lan1 CLAIMED INTERFACE HP J2146A - 802.3 LAN lan 2 10/12/6 lan2 CLAIMED INTERFACE Built-in LAN Press [Enter] to continue 1. Network Service Attatchment Point (NSAP) forms (Fixed/Flexible)?: **Fixed** 2. Activate SONET Directory Services (y/n)?: **y** 3. NE PROTOCOL INFORMATION The current configuration is displayed: CMISE: (y/n) **Y** OSI TL1: (y/n) **Y** X.25 TL1: (y/n) **Y** Please enter the item number [1-3] to make change. Enter "s" to save the above input and continue. Enter "q" to quit. **s**

Continued on next page

Step	Action (Contd)
6	The current OSI Configuration is summarized as following: 1. Primary OSI LAN interface number= 1 2. Organization Identifier= 000000 3. Routing Domain= 0000 4. OSI Area= 0000 5 OSI Lan Redundancy is not configured. 6. IP address for OSI over TCP/IP= 192192000100 We are using lan0 for OSI communications, but we entered the IP address for lan1 for TCP/IP over OSI communications. Changing these options is very easy, as explained below by following the prompts. The rest of the steps are self-explanatory. Enter the item number [1-6] to change the current value. Enter "s" to save the above input and continue. What would you like to do [1-6, or s] [q to quit]: **s**
7	Continue the install. **Stop! End of Task.**

Set Up NCC

Background

WaveStar SNMS supports OSI connections with NEs over a TCP/IP backbone network. In OSI over TCP/IP communications, an NCC or OLS 400G is required to perform OSI protocol conversion, as a transport bridge, for messages/ responses handled to/from the EMS and NEs.

An NCC can be provisioned to serve two main functions:

- Directory Services Agent (DSA) for SONET Directory Services (SDS)
- Transport bridge for TCP/IP to OSI protocol conversion for OSI-connected WaveStar BWM NEs communicating with WaveStar SNMS over a TCP/IP backbone network

If using a router instead of a Network Element, the router must be set up as follows:

- IS-IS Routing Protocol 10589
- TARP - TID Access Resolution Protocol (Bellcore standard GR-253 formerly TR-252)
- IEEE 802.3 Compliant
- OSI 7 layer stack

Task

The following commands can be issued at the NCC CIT in TL1 mode.

Step	Action

1	## Set Upper Layer Stack - Layer 3 Parameters
	ENT-ULSDCC-L3:NGN-NCC::189:::131v2is=enable;
	ENT-ULSDCC-L3:NGN-NCC::192:::L3AREA=0030;

2	## Set Upper Layer Stack Information - Layer 4
	ENT-ULSDCC-L4:NGN-NCC::194:::141ftm=10
	ENT-ULSDCC-L4:NGN-NCC::195:::14lftm=5;
	ENT-ULSDCC-L4:NGN-NCC::196:::14etof=enable;
	ENT-ULSDCC-L4:NGN-NCC::197:::14etpf=enable;
	ENT-ULSDCC-L4:NGN-NCC::198:::14etrf=enable;

3	## Retrieve Upper Layer Stack Information **RTRV-ULS:NGN-NCC::186**;

Continued on next page

Step	Action (Contd)
4	##Retrieve Upper Layer Stack Information - Layer 3 **RTRV-ULSDCC-L4:NGN-NCC::193;**
5	## Retrieve Upper Layer Stack Information - Layer 4 **RTRV-ULSDCC-L4:NGN-NCC::197;**
6	## Retrieve NE Level Parameters **RTRV-NE:NGN-NCC::210;** **Stop! End of Task.**

Configure OLS 400G Transport Bridge

Task

From the network element side the following commands are necessary to provision the 400G to be both a Transport Bridge and a Registration Manager.

Step	Action
1	Enter System command gives an IP address to the NE’s OS port. Do this if the NE is going to be a transport bridge. **ENT-SYS:TID::CTAG:::[Spec_block];** **Example:** The following is an example. It is on separate lines only to make it easier to read: ENT-SYS:WSOLS400G-----12345678-::XXX::: IP_ADDRESS=123.456.789,DFLTRTR_IPADDRESS=123.456.789, LOCAL_SUBNETMASK=255.255.255.0; a. The IP address is the IP address given to the Network Element by the network administrator. b. The dfltrtr ip address is the IP address of the default gateway. c. The NE will reset if the subnet mask is entered.
2	Enter Registration Manager. **ENT-RMA:TID:SYSTEM:CTAG:::[Spec_block]**; **Example:** The following is an example. It is on separate lines only to make it easier to read: ENT-RMA:WSOLS400G-----12345678-:SYSTEM:XXX1::: RM_ACTIVE=ENABLE,DSA_PSEL=0123,DSA_SSEL=012345, DSA_TSEL=012345, PRI_DSA_NSAP=1339840F80000000000000000000xxxxxxxxxxxx, PREFIX_COUNTRY=US,PREFIX_ORG=LUCENT,PREFIX_SUBORG1 =SNMS1; a. The primary DSA NSAP is the NSAP of SNMS southbound LAN card prefixed with a 13 for a total of 40 characters. Use this parameter only if not using a transport bridge. b. The PSEL, SSEL, and TSEL (presentation, session and transport layers) are the recommended values.

Step	Action (Contd)
3	Enter Transport Bridge. **ENT-TSB:TID:SYSTEM:CTAG:::[spec_block];** This needs to be entered in addition to the ent-sys command. ENT-TSB:WSOLS400G-----12345678-:SYSTEM:XXX::: PRI_TSB_NSAP=1339840f80000000000000000000xxxxxxxxxxxx, PRI_DSA_IP_ADDRESS=123.456.789; a. The PRI_TSB_NSAP is the NSAP of the transport bridge NE. Obtain the ethernet address of the NE using the WaveStar CIT interactive mode RTRV-SYS command. b. The DSA IP Address is the IP address of SNMS southbound LAN.
4	All the NEs in the network should now register themselves with SNMS. **Stop! End of Task.**

Configure CMISE Over Transport Bridge when Routers are Involved (OLS 400G)

Task Complete the following steps to configure CMISE over a transport bridge.

Step	Action
1	Login as **`root`** .
2	Create an alternate address as */etc/opt/OV/share/conf/ft_local_p_addr* by doing the following: **cd /etc/opt/OV/share/conf**
3	Use text editor to edit *ft_local_p_addr* **vi ft_local_p_addr**
4	Find the line with HOST IP address by the following: — identify the line ending in ":1006". An example line is as below: OVDM,ses0,tp0,0x5400728722031720100101000102400001:1006 — the 12 characters preceeding "0102400001" are the HOST IP address; so the HOST IP address from the example line is 172.10.10.100.
5	Replace the original host IP address with the router translated IP address and make sure the IP address is 12 characters long and using leading zeroes where necessary. **NOTE:** The format of the file is really sensitive, so please take extra caution when you do any modification.

Step	Action (Contd)
6	Save the file.
7	Login as `ems` and bring snms down then up or restart all Q3 managers (i.e. SB_Q3_400g01, SB_Q3_400g02, etc) to take effect.
8	Do the following verification after system is restarted: — login as **`ems`** — type in **sb400goam** — under ----> prompt, type in "address <TID>"; any valid <TID> can be used — the IP address displayed under TCPIP of File Transfer should be the same address as entered in the *ft_local_p_addr* — type in **quit** to exit sb400goam — done **Stop! End of Task.**

Set Up X.25 Global Link Settings

Background

The global link settings are, normally, Line Speed, Synchronous Timing Source, and Virtual Channel characteristics. These are Level 2 specifications that are used to gain the "synchronization" needed before data can be sent.

Task

Complete the following steps to set up X.25 global link settings.

Step	Action
1	Log in as `root`.
2	Get the physical address of the Mux interface cards by typing the following command: **ioscan -f | grep acc**
3	The global links file (sometimes called the "answer file") must be set up. It can be found in the following directory. (HP-UX Rel 11.0) **cd /opt/acc/cfg/**
4	Next you will vi the x25_config.answ file and define the physical address of the Mux card (see above for the correct address). Below is a small part of the x25_config.answ file. Interface-Definition * mx# bus#:slot# Mux 0 10:4:4 /opt/acc/mux/abs/x25.zabs Mux 1 10:4:12 /opt/acc/mux/abs/x25.zabs *Continued on next page*

Step	Action (Contd)
5	Now it is time to configure the timing source and the line speed. Ports 0 through 7 have been set for external timing and a line speed of 57600 (56k) using a V35 mux interface panel. If using the RS232 Mux interface panel, the line speed must be configured as 9600, as the RS232 port cannot support 57600 and the mux interface panel listing shown as RS232. Below is a small part of the x25_config.answ file. Port-Definition Port 00:00 RS232 57600 Ext SDLC x1 NRZ Port 00:01 RS232 57600 Ext SDLC x1 NRZ Port 00:02 RS232 57600 Ext SDLC x1 NRZ Port 00:03 RS232 57600 Ext SDLC x1 NRZ Port 00:04 RS232 57600 Ext SDLC x1 NRZ Port 00:05 RS232 57600 Ext SDLC x1 NRZ Port 00:06 RS232 57600 Ext SDLC x1 NRZ Port 00:07 RS232 57600 Ext SDLC x1 NRZ
6	The first line in each port’s Terminal Definition defines the specific X.25 driver to use and its Logical Presence Type (DTE or DCE). For SNMS, always use the X.25.LAPB driver. * device file: zx25m0p0 mux: 0 port: 0 * mknod zx25m0p0 c 125 0x0300 2>/dev/null Term 0001 0:0 X25.LAPB 0000h 4BEAh 10 0 0 0 0 "L2 DCE" no_autostart

Step	Action (Contd)
7	The remaining lines in each ports Terminal Definition specifies the Virtual Channels on this link. The two (2) types of Virtual Channels used are *x25.pvc* and *x25.svc.io*
8	Configure SVC communications. The following is an example: Term 020 0:0 x25.svc.io 0000h 0200h 99 0 0 0 0 “L3 svc” Term 021 0:0 x25.svc.io 0000h 0200h 99 0 0 0 0 “L3 svc” . . .
9	Configure PVC communications. The following is an example: Term 100 0:0 x25.pvc 0000h 0200h 99 0 0 0 0 “L3 pvc” Term 101 0:0 x25.pvc 0000h 0200h 99 0 0 0 0 “L3 pvc” . . . **Stop! End of Task.**

Set Up X.25 Specific Link Settings

Background

The **etc/x25/x25_config.XX** file defines the Level 3 characteristics of a specific X.25 port on the SNMS computer. There must be one of these files for each port you wish to use. These files are often referred to as the X.25 "config" files.

Procedure

Complete the following steps to set up specific link settings.

Step	Action
1	The **etc/x25/x25_config.XX** file must be manipulated by hand using a text editor such as "vi". Example: A sample file (with inserted comments) looks like: # # X.25 Initialization FileCreated: Fri June 16, 1995# # #SNMS - AI LINK DEFINITION for Mux 0, Port 4# # #Global Parameters # #File: x25_config.04 #Directory: /etc/x25 **Stop! End of Task.**

Set Up X.25 for LCT NE

Task

To configure an SVC channel for use with WaveStar SNMS, perform the following.

Step	Action
1	Log into the LCT using the CIT and Centerlink software.
2	From the menu select: **`Security→Enter Channel Identifier→security`**
3	From the menu, select the appropriate OS Type: MT, MA, CMDR, OTHR, RST, NONE (if using one SVC, you must select OTHR).
4	Enter svc calling address (CALLADDR). **Stop! End of Task.**

To configure a PVC channel for use with WaveStar SNMS, perform the following.

Step	Action
1	Log into the LCT using the CIT and Centerlink software.
2	From the menu select: **`Security→Enter Channel Identifier→security`**
3	Select **pvc**.
4	From the menu, select the appropriate OS Type: MT, MA, CMDR, OTHR, RST, NONE (if using one PVC, you must select OTHR).
5	Enter svc calling address (CALLADDR). **Stop! End of Task.**

Table 4-1. Table of Channel Types

OS Type	Function
MT	maintenance all autonomous message but REPT DBCHG
MA	memory-admin all REPT DBCHG messages
CMDR	cmt-response no autonomous messages
OTHR	all autonomous messages
RST	all autonomous messages but REPT EVT
NONE	Nothin

Set Up OSI for BWM NE

Background

The BWM NE uses the J175 or J177 DB9 connector for OSI communications. This can be found on the back of the control shelf.

⚠ **WARNING:**
WaveStar SNMS and the CIT must be plugged into separate ports in the back panel of the main controller. It is recommended that the J175 and J177 DB9 connectors found along the right-hand side of the system controller bay be used. Do not use the front connector or there will be a problem with connectivity.

Task

Complete the following steps to set up OSI for a BWM NE.

Step	Action
1	To retrieve the current configuration: **RTRV-ULSDCCL3**:tid:aid:ctag; TL1 Syntax
2	To enter or change the configuraton: **ENT-ULSDCCL3**:tid:aid:ctag:::spec_block; TL1 Syntax **Stop! End of Task.**

Set Up OSI for OLS 400G NE

Background

The 400G uses the J32OS DB9 connector located in the system bay interconnect panel.

Task

Complete the following steps to set up OSI for an OLS 400G NE.

Step	Action
1	To retrieve the current OSI configuration: **RTRV-OSI:TID::ctag**; **Example:** The following is an example of **retrieve** command. **RTRV-OSI:OLS-400G::rsf**; IP 789012 < OLS-400G 93-10-26 16:42:11 M 789012 COMPLD “localaddress=39000080,isislvl=Level-2,drp=64”
2	To enter or change the OSI configuraton: **ENT-OSI:TID::CTAG:{GEN_BLOCK}{:{:{SPEC_BLOCK}}}**; **Example:** The following is an example of **enter** command. **ent-osi:OLS-400G::rsf:::localaddress=0439000080,isislvl=Level-2,drp=64**; IP 123456 < 400G 93-10-26 16:42:11 M 123456 COMPLD **Stop! End of Task.**

Set Up LambdaRouter

Procedure

Complete the following steps to set up a LambdaRouter.

Step	Action
1	Login to the Lambda Router CIT default login - LUC01 Default password - OXC+1
2	Select **Administration** from the main menu bar.
3	A pulldown menu appears. Select **Name/Address Administration...**
4	Select the appropriate TID from the TID pulldown menu.
5	The IP address of the selected NE appears in the IP address box. **NOTE:** Write down the IP address to be used.
6	Select Cancel to close the window. **Stop! End of Task.**

Trouble Clearing

5

Introduction

Summary

This chapter describes procedures that can facilitiate troubleshooting problems with software components of WaveStar SNMS and its communications interfaces.

Contents

This chapter discusses the following topics:

Check the Status of the WaveStar SNMS Application

Background

Use this procedure to check the status of the WaveStar SNMS application.

Task

Complete the following steps to check the status of the WaveStar SNMS application.

Step	Action
1	Log in as `root`.
2	At the UNIX prompt, enter the command **appstat** **Result:** If the application is up, the system displays the CURRENT RUN LEVEL (status) as “Running” and lists the demon name, process ID (pid), process name, run status (option), persistance, and number of respawns of each application process. The WaveStar SNMS processes are as follows: - *EMS:BR_bacres*- NE Backup and Restore Module - *EMS:CF_NeAgent*- NE Configuration Module - *EMS:CF_NeProxy*- NE Configuration Module Proxy Server - *EMS:NT_Manager*-Network Topology Management Module - *EMS:CM_Server*- Communications Manager - *EMS:SM_Security*- Security Management Module - *EMS:FM_Server*- Fault Management Module - *EMS:OAM_Scheduler*- Process Scheduling Module - EMS:*PM_DC*- Performance Management Module - *EMS:PM_FTAM*- Performance Management Module through FTAM - EMS:*LM_Logger*- Log Management Module - EMS:*SDS_Server*- SONET Directory Service Module If the application is down, the following message is displayed: `CURRENT RUN LEVEL IS: Shutdown` *Continued on next page*

Step	Action (Contd)
	There are three states for the application: - Shutdown—The WaveStar SNMS application is not up. - Administrative—The WaveStar SNMS application is in transition (coming up or going down). - Running—The WaveStar SNMS application is up. The `Respawns` field should be 0 for every process. If any of these fields has a number larger than 0, then that process terminated and automatically restarted for some reason. The `Pid` field should have a number greater than 0 for every process. If any of these fields has a 0, then that process terminated and is no longer running. The application must be restarted.
3	If you execute the **appstat** command, everything may look normal but the process may not be bound to Orbix. The **psit** command shows you if the appstat is true. At the UNIX prompt, enter the command **psit | more** to see if the process is running and bound to Orbix. **Stop! End of Task.**

Check the Status of Stopped Process

Background

Use this procedure to report the status of stopped processes. Any process reported under this section means that process has been terminated and is no longer running. The process needs to restarted either by executing **appstart -n** <process name> or the application must be restarted.

Task

Complete the following steps to report the status of stopped processes.

Step	Action
1	Log in as `ems`.
2	At the UNIX prompt, enter the command **appstx** **Result:** The system displays output that shows the current run level (application status) and a list of processes, by demon name, that have stopped, if any. **Stop! End of Task.**

Check the Communication Status of NEs

Background

Use this procedure to check the communication status of managed network elements.

Task

Complete the following steps to check the communication status of managed network elements

Step	Action
1	Log in as `ems`.
2	At the UNIX prompt, enter the command **cmtool -a** **Result:** The system displays output that shows, for each NE: - The communications port - The NE's TID - A communications active flag (Y = Yes) - The communications type - The communications channel ID - The communications link status (Up or Down) - The NE's login status (On or Off) **Stop! End of Task.**

Activate a Network Element

Background

Use this procedure to activate a network element

Related information

To see the complete list of **cmtool** features that can be utilized, at the UNIX prompt, enter the command **cmtool -l**. The **cmtool** command can provide:

1. All GNE LinkStatus
2. One NE LinkStatus
3. One GNE LinkStatus
4. NE Activate/Deactivate
5. Resync config file
6. Switch primary/backup GNEs
7. Change NE password

```
cmtool usages:
    cmtool [-a] display all Ne status
    cmtool [-h hostname]
    cmtool [-s] option for switch primary/backup GNE with -p -b options
    cmtool [-p primary GNE tid] [-b backup GNE tid]
    cmtool [-l] list all tool features for select
    cmtool [-f functional_index] [-n|g netid [-o op]]
    cmtool [-n Netid] display Ne status
    cmtool [-g Gnetid] display Gne status
    cmtool [-c netid] change ne password
    cmtool [-o [a|d]] option of activate/deactivate
    cmtool [-?] for help
```

Task Complete the following steps to activate a network element.

Step	Action
1	At the UNIX prompt, enter the command **cmtool -n <*TID*> -o a** **Result:** The system displays output indicating that a new NE connection has been made and the IP address of the NE **Stop! End of Task.**

Deactivate a Network Element

Background

Use this procedure to deactivate a network element.

Task

Complete the following steps to deactivate a network element.

Step	Action
1	At the UNIX prompt, enter the command **cmtool -n <*TID*> -o d** **Result:** The system displays output indicating that a deactivate process has been invoked and the IP address of the NE **Stop! End of Task.**

Check Logged In Users

Background

Use this procedure to show the present GUIs, the logged in users, and from which IP address they are logged in.

Task

Complete the following steps to check the number of GUI clients currently running on the WaveStar SNMS host, the user login(s) for each GUI, and information about all queues.

Step	Action	
1	At the UNIX prompt, enter the command **GUI_Probe <***hostname***> :GUI_SERVER** **Result:** The system displays output indicating that a connection has been made to the GUI server and the GS prompt.	
2	At the GS> prompt, enter **?** **Result:** The system displays the HELP menu for the **GUI_PROBE** command that shows the list of command option you can issue to obtain information	
3	TO...	DO THIS...
	Get a list of GUI clients, the user logins currently running on the GUI Server, and the IP address of the logged in user ID	Enter **clients** at the GS> prompt
	Show information about all the queues	Enter **queues** at the GS> prompt
	Exit the **GUI_PROBE** program **Stop! End of Task.**	Enter **exit** at the GS> prompt

Check the Association Status of OLS 400G NEs

Background Use this procedure to show the association status of the managed OLS 400G NEs.

Task Complete the following steps to obtain the association status of the managed OLS 400G NEs.

Step	Action	Action
1	At the UNIX prompt, enter the command **s400goam** **Result:** The system displays the prompt - - ->	
2	TO...	ENTER...
	Show the status of all OLS 400G NEs	**assocstatus**
	Show the status of one OLS 400G NE	**assocstatus** *NE name*
	Set the trace level	**trace**
	List active transactions	**listxn**
	Shut down communications with NEs	**shutdown**
	Set logcontrol level	**logcontrol**
	Report the number of active, confirmed associations	**assocnt**
	Abort association	**assocabort**
	Set up an association	**assocreq**
	Activate watchdog	**watchdog**
	Display statistics	**statistics**
	Change the state of overload controls	**overload**
	Start association request on threads	**assocthread**
	Request an association follow by an abort	**assocandabort**
	Stop! End of Task.	

Retrieve the Informix Software Version

Background

Use this procedure to retrieve the version of Informix. The WaveStar SNMS Release 4.2 software uses Informix Dynamic Server Release 7.31 uc2xc to maintain a relational database.

Before you begin

To execute the command described in this procedure, you must be logged in as the user `informix` or `ems`.

Task

Complete the following steps to retrieve the Informix software release version.

Step	Action
1	At the UNIX prompt, enter the command **dbaccess -v** **Result:** The system displays messages indicating the Informix software version number and the software serial number. Each system has a unique software serial number for its location. **Stop! End of Task.**

Retrieve Informix Database Locks

Background

Use this procedure to retrieve the locks that the WaveStar SNMS application are holding on the Informix database.

Before you begin

To execute the command described in this procedure, you must be logged in as the user `ems`.

Task

Complete the following steps to retrieve the database locks that the WaveStar SNMS are holding on the Informix database.

Step	Action
1	At the UNIX prompt, enter the command **locks** **Result:** The system displays a three column message. The first column is the number of database locks being held. The next two columns are the PID and process name, respectively, which are holding the locks. **NOTE:** If some locks persistently show up, the system may be experiencing some congestion. If the situation persists, the WaveStar SNMS application may need to be restarted.
2	To retrieve detailed lock table information, enter the command **tblocks** **Result:** The system displays a two column message. The first column is the table name and the locks being held. The second column shows the number of locks held on the table. **Stop! End of Task.**

Check Informix Database Space Usage

Background

Use this procedure to retrieve the Informix database space usage

Before you begin

To execute the command described in this procedure, you must be logged in as the user `informix` or `ems`.

Task

Complete the following steps to check the Informix database space usage.

Step	Action
1	At the UNIX prompt, enter the command **onstat -d** **Result:** The system displays output indicating the current Informix software release version, the dbspaces, and the chunk usage information. **NOTE:** Verify that the free column for the dbspace partitions is not approaching 0. If it is, it indicates that the database is running out of free space. Use **add_dbs dbspacename** to add additional 10M to the dbspace specified. Verify again by **onstat -d.** The application does not have to be brought down to add dbspace. **Stop! End of Task.**

Check Informix Error Codes

Background

Use this procedure to display error codes and text for Informix errors.

Before you begin

To execute the command described in this procedure, you must be logged in as the user `informix` or `ems`.

Task

Complete the following steps to display Informix error codes and text.

Step	Action
1	At the UNIX prompt, enter the command **finderr** *xxx* where *xxx* is the specific Informix error code. **Result:** The system displays output indicating the Informix error code, the error code message text, and a brief statement about the possible solution to the error. **Stop! End of Task.**

Check Level 2 Status of X.25 Network Connections

Background

Use this procedure to display the status of each X.25 port on the WaveStar SNMS host.

Task

Complete the following steps to display the status of each X.25 port on the WaveStar SNMS host.

Step	Action
1	At the UNIX prompt, enter the command **x25_check *[Mux #]*** where ***[Mux #]*** is an optional parameter (0 to 3). The default = 0 (MUX Card 0). **Result:** The system displays output indicating the status of each X.25 port. **NOTE:** The first four lines indicate the low-level X.25 processes are running; they should all have a status of UP. If any of the X.25 processes report a status of DOWN, the X.25 connection needs to be restarted. The second section of the message, titled X.25 Port Status, displays the current Level 2 synchronization status for each link. - Up—indicates the SNMS computer has synchronized with the PSN connected to this port. - Down—indicates that Level 2 synchronization cannot be achieved on this port. Check the following: 1. Is a Synchronous Modem Eliminator required? 2. Is the timing source set correctly in the X.25 answer file? For HP-UX Release 10.0, this file is found under */opt/acc/cfg/x25_config.answ* 3. Is the Data Rate set properly? 4. Have the Level 3 DTE/DCE network types been set properly in the X.25 *answer* file and specific X.25 *config* file? 5. Does the PSN support a V.35 interface? 6. Is the V.35 cable good? 7. Is the V.35 cable connected to the correct port? **Stop! End of Task.**

Check Level 3 Status of X.25 Network Connections

Background

Use this procedure to obtain various levels of detail about a specific X.25 port.

Task

Complete the following steps to obtain various levels of detail about a specific X.25 port..

Step	Action
1	At the UNIX prompt, enter the command **x25stat -d *[device_file] [options]*** where ***[device_file]*** is of the form **/dev/zx25MMPP** Example: /dev/zx25m0p0 The last four characters indicate the MUX Card (MM) and Port Number (PP) to report on. **NOTE:** Refer to Table 5-1 for a listing of device files for X.25 ports. **Result:** The system displays lines of detail about the specified X.25 port. **Stop! End of Task.**

Check the Virtual Channel Status of an X.25 Port

Background

Use this procedure to obtain the status of virtual channels on a specific X.25 port.

Task

Complete the following steps to obtain the status of the virtual channels for a specific X.25 port.

Step	Action
1	At the UNIX prompt, enter the command **x25stat -d** *device_file* where *device_file* is of the form **/dev/zx25MMPP,** for example: **/dev/zx25m0p0** The last four characters indicate the MUX Card (*MM*) and Port number (*PP*) to report on. In the example above, MUX Card 0, Port 0 (Connector J0) has been specified. Refer to Table 5-1 immediately following this procedure for a listing of device files for X.25 ports. **Result:** The system displays output that indicates, for each virtual channel of the specified X.25 port, the virtual channel type, the local address, its foreign address (if applicable), the virtual channel number, and whether it is currently connected. All channels of VC type PVC appear whether they are in use or not. If the `Local Address` field has dashes, the PVC is defined but not actively in use. If the `Local Address` field has an X.121 Address displayed (this had been previously defined in the X.25 *config* file for this port), then the PVC has been restarted and communication *may* be established. SVC channels that are currently in use appear after the last PVC channel. If no SVC channels are in use, then none are reported. However, they still are defined. The above display shows that PVCs 3 and 8 have been reset and *may* be in use. SVC 20 is active and connected to X.121 address 9089492000. **NOTE:** If the x25stat command is run on a port that is not connected to a PSN or is not configured properly, you will see the following message: x25stat WARNING: Level 2 is DOWN Check the following: 1. Were the right MUX and Port queried? 2. Does the PSN support a V.35 interface? 3. Is the V.35 cable connected to the right port on the PSN? 4. Is the V.35 cable connected to the right port on the SNMS computer? **Stop! End of Task.**

The following table provides a listing of device files for all possible ports (if equipped)

Table 5-1. Device Files for X.25 Ports.

	MUX Card 0	MUX Card 1	MUX Card 2	MUX Card 3
Port 0:	/dev/zx25mop0	/dev/zx25m1p0	/dev/zx25m2p0	/dev/zx25m3p0
Port 1:	/dev/zx25m0p1	/dev/zx25m1p1	/dev/zx25m2p1	/dev/zx25m3p1
Port 2:	/dev/zx25m0p2	/dev/zx25m1p2	/dev/zx25m2p2	/dev/zx25m3p2
Port 3	/dev/zx25m0p3	/dev/zx25m1p3	/dev/zx25m2p3	/dev/zx25m3p3
Port 4:	/dev/zx25m0p4	/dev/zx25m1p4	/dev/zx25m2p4	/dev/zx25m3p4
Port 5:	/dev/zx25m0p5	/dev/zx25m1p5	/dev/zx25m2p5	/dev/zx25m3p5
Port 6:	/dev/zx25m0p6	/dev/zx25m1p6	/dev/zx25m2p6	/dev/zx25m3p6
Port 7:	/dev/zx25m0p7	/dev/zx25m1p7	/dev/zx25m2p7	/dev/zx25m3p7

Obtain X.25 Virtual Channel Non-Data Packet Statistics

Background

Use this procedure to obtain virtual channel non-data packet statistics for a specific X.25 port.

Task

Complete the following steps to obtain virtual channel non-data packet statistics for a specific X.25 port..

Step	Action
1	At the UNIX prompt, enter the command **x25stat -d** *device_file* **-p** where *device_file* is of the form **/dev/zx25MMPP,** for example: **/dev/zx25m0p0** The last four characters indicate the MUX Card (*MM*) and Port number (*PP*) to report on. In the example above, MUX Card 0, Port 0 (Connector J0) has been specified. Refer to Table 5-1 for a listing of device files for X.25 ports. **Result:** The system displays output that indicates, for each virtual channel of the specified X.25 port, the virtual channel state the current virtual channel user, the number of interrupt messages generated, and the number of resets. All channels appear as in the previous section except that the VC type is not specified. The `VC User` is the protocol that is active on this virtual channel. In the display above, VCs 3 and 20 have an active Level-3 (packet level) Programmatic Access user on them. This indicates that a machine is sending and receiving X.25 data over these channels. The next section will give you a clearer picture of this. **NOTE:** VC 8, however, shows no current user. Even though the display in the previous section showed PVC 8 was connected, the fact is, the VC was successfully reset but no further data was exchanged on the channel. **Stop! End of Task.**

Obtain X.25 Virtual Channel Data Counters

Background

Use this procedure to obtain the status of the virtual channel data counters on a specific X.25 port.

Task

Complete the following steps to obtain the status of the virtual channel data counters on a specific X.25 port.

Step	Action
1	At the UNIX prompt, enter the command **x25stat -d** *device_file* **-t** where *device_file* is of the form **`/dev/zx25MMPP,`** for example: **`/dev/zx25m0p0`** The last four characters indicate the MUX Card (*MM*) and Port number (*PP*) to report on. In the example above, MUX Card 0, Port 0 (Connector J0) has been specified. Refer to Table 5-1 for a listing of device files for X.25 ports. **Result:** The system displays output that indicates, for each virtual channel of the specified X.25 port, the virtual channel state, the number of inbound messages, the number of outbound messages, the number of inbound data packets, the number of outbound data packets, and the number of inbound octets. *Continued on next page*

Step	Action (Contd)
	All channels appear as in the previous sections and the VC type is not specified. In the sample output above, `Imsgs,Ipackets,` and `Ioctets` refer to messages *received* over the X.25. `Omsgs`, `Opackets,` and `Ooctets` refer to messages *transmitted* over the X.25. In the display above, VCs 3 and 20 appear to have traffic flowing in **both** directions. Typically, there are more messages received than transmitted. As the SNMS system sends single commands to the NEs, the responses are sometimes long and received in several pieces (packets). **NOTE:** VC 8, however, appears to be having a problem. Messages have been transmitted, but none received. The first display in the previous section showed VC 8 was connected. The next sections provide a more accurate picture. There is no current user because the VC is not transmitting **and** receiving data in both directions. Check the following: ■ If the VC is a PVC: 1. Has the PVC been mapped correctly through the PSN? 2. Is SNMS using the right PVC? ■ If the VC is an SVC: Is the Called X.121 Address correct? ■ Other items to be checked (if attempting *pvctest* or *svctest*): 1. Is the TID of the NE correct? 2. Is the NE connected to the PSN? **Stop! End of Task.**

Reset an X.25 MUX Port

Background

Use this procedure to reset a specific X.25 port without disrupting other data communications links.

Task

Complete the following steps to reset a specific X.25 MUX port.

Step	Action
1	Log in as `root`, or `su` (super-user).
2	At the # prompt, enter the command **/usr/sbin** *device_file* where *device_file* is of the form: **/dev/zx25*MMPP*,** for example: **X25stop -d /dev/zx25m0p4** This shuts down MUX Card 0, Port 4. You may specify any MUX/Port equipped in the computer. There is no output to this command.
3	At the # prompt, enter the command: **/usr/sbin/x25init -c /etc/x25/ x25_config.*MP*** where ***MP*** is the MUX Card and Port Number, for example: **x25_config.04** identifies MUX Card 0, Port 4. This re-initializes MUX Card 0, Port 4. You may specify any MUX/Port equipped in the computer. If the re-initialization was successful, there will be no output to this command. **NOTE:** If there was a failure or inconsistency of some kind, you will receive an error message. Check the following: ■ Refer to the HP-UX NACC X.25 section and verify that the relationships between the X.25 *answer* file and this X.25 *config* file are correct. ■ It is possible that restarting a link may not work even though everything appears to be set up properly. In that case, it is best to restart the X.25 processes again. Refer to the procedure Restart X.25 Processes. **Stop! End of Task.**

Restart X.25 Processes

Background

Use this procedure to reset the X.25 communications server to clear potential communications problems. Restarting the X.25 communications server drops all connections to the Packet Switched Network (PSN) and re-restablishes the connections.

Task

Complete the following steps to reset the X.25 communications server.

Step	Action
1	Log in as `root` or `su` to *root*.
2	At the # prompt, enter the command **/etc/x25/x25_config.rc** **Result:** The system displays messages indicating that the X.25 communications server processes are being brought down and then restarted. The X.25 server output is directed to the */usr/adm/x25server.log* file. **Stop! End of Task.**

Deactivate/Reactivate System Links to Gateway Network Elements

Background

Use this procedure to deactivate and then reactivate communications links with an X.25-connected Gateway Network Element (GNE). This procedure should be used if the various procedures for troubleshooting X.25 communication problems have failed to identify the source of the problem and recover communications. The problem may be a “hang” in the system X.25 drivers. This can occur if a PVC link to an NE is lost. This procedure can be used to remove the X.25 “hang”.

Related tasks

- Check Level 2 Status of X.25 Network Connections
- Check the Virtual Channel Status of an X.25 Port
- Obtain X.25 Virtual Channel Non-Data Packet Statistics
- Obtain X.25 Virtual Channel Data Counters
- Reset an X.25 MUX Port
- Restart X.25 Processes

Task

Complete the following steps to deactivate and then reactivate communications links with an X.25-connected GNE.

Step	Action
1	Log in as `ems`
2	To deactivate system links, enter the command **cmtool -n <TID> -o d** Repeat this step for any GNEs that have a communications problem
3	To reactivate system links, enter the command **cmtool -n <TID> -o a** Repeat this step for all GNEs *except* for the failed one. **Stop! End of Task.**

Obtain Virtual Circuit Information for Gateway Network Elements

Background

Use this procedure to obtain Packet-Switched Network (PSN) information about X.25-connected GNEs.

Task

Complete the following steps to obtain PSN information about X.25-connected GNEs.

Step	Action
1	At the UNIX prompt, enter the command **gneVcinfo** Result: The system outputs a listing of GNEs (by TID), the VC types used by each GNE, and the type of PSN used by each GNE. **Stop! End of Task.**

Test Permanent Virtual Circuit Connection to a Network Element

Background

Use this procedure to test communication via a specified permanent virtual circuit (PVC) to a network element.

Once an NE has been entered into the WaveStar SNMS database, the application will automatically try to gain communication to that element.

Before you begin

If you wish to run a **pvctest** to a network element which has already been databased, you must first deactivate the network element using the **cmtool** command.

Related task

Use the following procedure to deactivate a network element

- Deactivate a Network Element

Task

Complete the following steps to test communication via a specified permanent virtual circuit (PVC) to a network element.

Step	Action
1	At the UNIX prompt, enter the command **pvctest** Result: The system displays messages about the **pvctest** utility and a prompt for the NE's TID.
2	Enter the NE's TID. **Result:** The system prompts for the X.25 port.
3	Enter the X.25 port. **Result:** The system prompts for the PVC number.
4	Enter the X.25 PVC number. **Result:** The system prompts for a privileged login.
5	Enter a privileged login (for example, **LUC01**). **Result:** The system prompts for the privileged login password.
6	Enter the password for the privileged login. **Result:** The system displays a message and a prompt for the NE type (the prompt identifies each NE type by number; for example, NE Type 1 equals a DDM-2000).
7	Enter the appropriate number for the NE type. **Result:** The system displays a menu of choices.

Step	Action (Contd)
8	Select Menu Option 1 (ACT-USER). **Result:** The system displays output for the ACT-USER command. If the command is successful, the system displays messages confirming that you have successfully tested the PVC channel to the selected NE. Go to Step 9. **NOTE:** If you do not receive a response from the NE, press Ctrl **C** or the Delete key to break out of the program. Check the following: ■ Is the NE powered up and operational? ■ Is the NE connected to the X.25 network? ■ Is the TID of the NE set properly? ■ Are the channel maps in the local PSN (on the WaveStar SNMS side) set correctly? ■ Are the channel maps in the remote PSN (on the NE side) set correctly?
9	Select Menu Option 2 (CANC-USER). **Result:** The system displays output for the CANC-USER command. If the command is successful, the system displays a message indicating that the command issued is completed.
10	Select Menu Option 99 (Exit). **Stop! End of Task.**

Test Switched Virtual Circuit Connection to a Network Element

Background

Use this procedure to test communication via a specified switched virtual circuit (SVC) to a network element.

Task

Complete the following steps to test communication via a specified switched virtual circuit (SVC) to a network element.

Step	Action
1	At the UNIX prompt, enter the command **svctest** Result: The system displays messages about the **svctest** utility and a prompt for the NE’s TID.
2	Enter the NE’s TID. **Result:** The system prompts for the X.25 port.
3	Enter the X.25 port. **Result:** The system prompts for the X.25 X.121 address for the NE.
4	Enter the X.25 X.121 address for the NE. **NOTE:** Time-out and sub-address parameters should be added to the end of the Calling Address. These only work on the command line. The default value for time-out is 30 and for sub-address is 1. Even though SNMS will work with one VC, software management will not. It must have the second channel. **Result:** The system prompts for a privileged login.
5	Enter a privileged login (for example, **LUC01**). **Result:** The system prompts for the privileged login password.

Step	Action (Contd)
6	Enter the password for the privileged login. **Result:** If the login and SVC Call Request was processed successfully by the PSN, the system outputs a menu listing for NE types. **NOTE:** On occasion, you may receive an error message indicating the SVC call was not successful, such as “connection refused.” This would imply that there is a problem in the PSN trying to route the call. Check the following: ■ Do the PVC and SVC definitions on the PSN match the PVC and SVC definitions on the host? ■ Is the SVC Address translation in the PSN mapped correctly?
7	Select Menu Option 1 (ACT-USER). **Result:** The system displays output for the ACT-USER command. If the command is successful, the system displays messages confirming that you have successfully tested the PVC channel to the selected NE. Go to Step 8. **NOTE:** If you do not receive a response from the NE, press Ctrl **C** or the Delete key to break out of the program. Check the following: ■ Is the NE powered up and operational? ■ Is the NE connected to the X.25 network? ■ Is the TID of the NE set properly? ■ Are the channel maps in the local PSN (on the WaveStar SNMS side) set correctly? ■ Are the channel maps in the remote PSN (on the NE side) set correctly?

Step	Action (Contd)
8	Select Menu Option 2 (CANC-USER). **Result:** The system displays output for the CANC-USER command. If the command is successful, the system displays a message indicating that the command issued is completed.
9	Select Menu Option 99 (Exit). **Stop! End of Task.**

Monitor OSI Stack on the WaveStar SNMS Host

Background

Use this procedure to monitor the OSI stack on the WaveStar SNMS host. Once the **osipu** process is running, you can send TARP requests to network elements.

Task

Complete the following steps to monitor the OSI stack on the WaveStar SNMS host.

Step	Action	Action
1	At the UNIX prompt, enter the command **osipu** **Result:** The system outputs messages indicating that the **osipu** process has started and returns with a UNIX prompt.	
2	TO....	ENTER THE COMMAND...
	Send a TARP request to a specific network element	**tarp getnsap C<*TID*>** **NOTE:** There is a complimentary command to the tarp getnsap C command. The command is: **tarp gettid H** (nsap of the network element you would like the TID for) If output from the completed TARP request obtained from isssuing the above command shows that the origin is from TDC, you must flush the TDC cache.
	Flush the TDC cache	**tarp tdc flush**

Step	Action (Contd)	Action
3	TO ... Exit the **osipu** command session **Stop! End of Task.**	ENTER.... **$exit** **NOTE:** You must exit the **osipu** session before bringing WaveStar SNMS down and then up, or problems may occur.

Verify IP Addresses and Names

Background

Use this procedure to verify network device IP addresses and names for WaveStar SNMS hosts and workstations.

Hosts and other network devices that are in the same physical location are either connected via 10baseT unshielded twisted pair cables through a hub or they are connected to each other directly by coaxial cable.

Network devices that are not at the same location are connected over T1 lines using Channel Service Units/Data Service Units (CSU/DSUs) and routers.

Task

Complete the following steps to verify network IP addresses and names for systems on the same network.

Step	Action
1	At the UNIX prompt, enter the command **cat /etc/hosts | pg** Result: The system the contents of the */etc/hosts* file. Each line contains an IP address and name for systems on the same network. All WaveStar SNMS system names must be six characters or less, and begin and end with a letter. **Stop! End of Task.**

Test LAN Connectivity

Background

Use this procedure to check IP connectivity to other devices on the same network.

Task

Complete the following steps to check IP connectivity to other devices on the same network.

Step	Action
1	Log into the host system as `ems`
2	At the UNIX prompt, enter the command **cat /etc/hosts | pg** Result: The system the contents of the */etc/hosts* file. Each line contains an IP address and name for systems on the same network.
3	Take note of the name of the host, workstation, or device to be tested.
4	At the UNIX prompt, enter the command **/etc/ping *name*** where ***name*** is the name of the device to be tested for connectivity. Wait a few seconds for the system to transmit packets of data to remote workstations and get them back.
5	Press Ctrl **C** to stop the test. **Stop! End of Task.**

Test Twisted Pair Wiring

Background

Use this procedure to test network devices that use twisted pair wiring. Follow this procedure if the router responds positively and the workstation does not respond.

Before you begin

Check the following possibilities for networks tht use twisted-pair wiring:

- Devices are powered off or unplugged.
- Loose connections or broken wires between the workstation and hub or hub and router.

Try pinging the workstation using the procedure Test LAN Connectivity. If pinging the workstation still fails, follow this procedure.

Task

Complete the following steps to test network devices, such as a workstation, that use twisted-pair wiring.

Step	Action	Action
1	Reboot the workstation.	
2	Log into the workstation.	
3	At the UNIX prompt, enter the command **/etc/reboot**	
4	IF...	THEN...
	Pinging the workstation still fails	Try rebooting both the router and hub by turning them off and back on.
	Trouble still persists	Try replacing wiring and swapping out the hub.
	Stop! End of Task.	

Test Stations Connected Via Coaxial Cable

Background

Use this procedure to test network devices connected via coaxial cable.

Before you begin

Check the following possibilities for networks tht use coaxial cable:

- Devices are powered off or unplugged
- AUIs are loosely connected
- Cables between nodes are improperly connected or non-terminated

Task

Complete the following steps to test network devices, such as a workstation, that use coaxial cable.

Step	Action	Action
1	Ping the workstation using the Test LAN Connectivity procedure.	
2	IF... Pinging the workstation still fails Trouble still persists **Stop! End of Task.**	THEN... Reboot the workstation and router. Try swapping AUIs and replacing cables.

Verify Northbound Interface to WaveStar NMS Server

Background

Use this procedure to verify the Northbound interface to WaveStar NMS.

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 WaveStar NMS 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 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.

If notifications are not received by WaveStar NMS (SONET), verify that the local DNS Domain Name is not set.

Task

Complete the following steps to verify the Northbound interface to WaveStar NMS..

Step	Action
1	Telnet into the same port used by WaveStar NMS to check if it is active by entering, at the UNIX prompt, the command **telnet <***TCP/IP hostname or IP address***> 10160** Result: The system connects to a TL1 command session. If the telnet session hangs or fails, check the hostname/IP address of the server. Ping the server to insure there is LAN connectivity.
2	Log into the WaveStar NMS server by entering the TL1 command **act-user:<SNMS hostname>:itm:::itm123**; **NOTE:** To exit the telnet session at any time, press the CNTL and] keys and type **quit** at the telnet prompt. **Stop! End of Task.**

Test WaveStar SNMS to WaveStar NMS Cut-Through

Background

Use this procedure to test the WaveStar SNMS-to-WaveStar NMS Cut-Through interface.

Task

Complete the following steps to test the WaveStar SNMS-to-WaveStar NMS Cut-Through interface...

Step	Action	
1	Log into WaveStar NMS and go to the WaveStar NMS controllers map.	
2	Place the mouse cursor over the center of the SNMS icon.	
3	Click the mouse button that brings up the pop-up menu.	
4	Select the VCIT menu item via the cascading menus: Session->Virtual Craft Interface Terminal	
5	IF... The WaveStar NMS GUI is not working	THEN... Invoke the WaveStar SNMS GUI by telneting and logging into the WaveStar SNMS server, change directory to the SNMS GUI software directory and entering the command **[snms -host <hostname> -nobs -up itm itm+123**
6	IF... The login is successful If the login is unsuccessful	THEN... Proceed to step 10 Check the password of the itm login. If the password is not itm+123, it might be itm123. If you need to define an itm password that is NOT itm+123, edit the configuration file to override the default itm password for the F-interface. If the GUI displays an error indicating that the “EMS is not running”, log in to the SNMS server and execute the command: **appstat**
7	IF... The WaveStar SNMS application not running The WaveStar SNMS application is already up and running	THEN... Bring up the WaveStar SNMS application by entering the command **up** Enter the command psit | grep GUI_Server If a message is displayed indicating that the GUI server is running, the application is running

Step	Action (Contd)	
8	IF... The WaveStar SNMS application is running but there are still problems	THEN... The WaveStar NMS host is using a host name that is mapping to the wrong WaveStar SNMS server IP address. Check the IP addressing in the file M:{Winnt|Wtsrv}\system32\drivets\etc\hosts
9	IF... There was no command output messages displayed from running the **psit** command in Step 7	THEN... Restart the GUI_Server process by entering the command chexstate -p GUI_Server -a restart Once the **chexstate** command is complete, retry the command psit | grep GUI_Server
10	Check NM batch file for the correct SNMS classpath.	
11	Edit the file */jui/bin/run_jnm.bat*. The SNMS classpath should be defined for each NM CLASSPATH definition.	
12	Check F-interface configuration file for correctness and enable debugging. The F-interface configuration file is: */jui/jnm/itm/southbound/ems/emsFint/emsFint.cfg*. Check to see whether each release in the configuration file maps to the correct GUI software directory. Once editing is complete, try again to launch the SNMS interface via the controllers map and the VCIT menu item. If the cut-through still fails, you will need to examine the NM debug log to determine the problem. The name of the debug log is displayed at NM startup time and the file is always located in the /jui/logs directory. If you examine the log immediately after the cut-through failure, then the debug output should be near the end of the log. Check the following: ■ determine whether the configuration file was found by the software. ■ whether the correct GUI software was being launched for the specified SNMS host. The log file contents should indicate whether the proper instance of the SNMS GUI software is being launched. Unless a new bug emerges in the software, the problem is always the result of the wrong version of SNMS GUI software being launched. **Stop! End of Task.**	

System Introduction

6

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 6-1). Recovery relies on switching control to another resource on the same host such as a backup LAN card or mirrored disk.

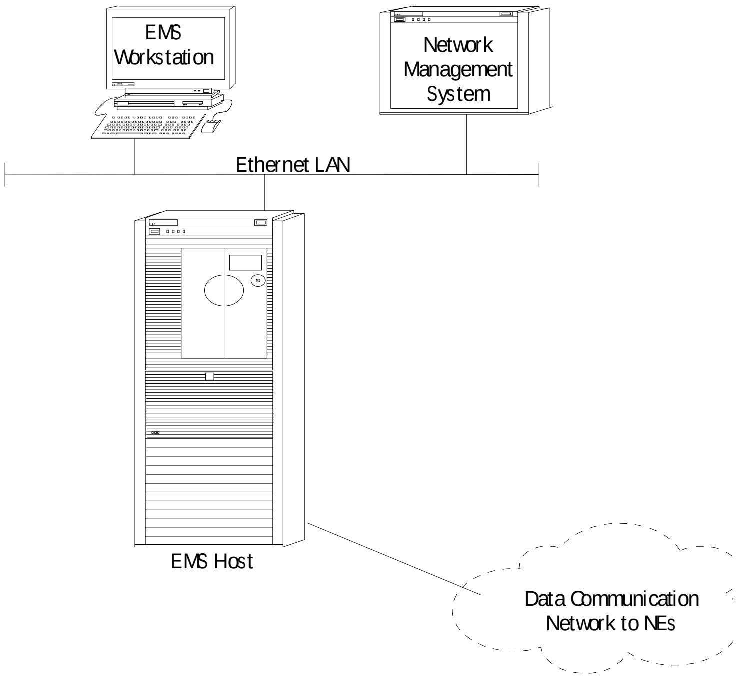

Figure 6-1. EMS Basic Host Redundancy Configuration

Local redundancy

Local redundancy employs two similarly equipped hosts located in the same building (Figure 6-2). Each host is configured with redundant hardware components. Should the primary host fail, the backup host is activated automatically without user intervention.

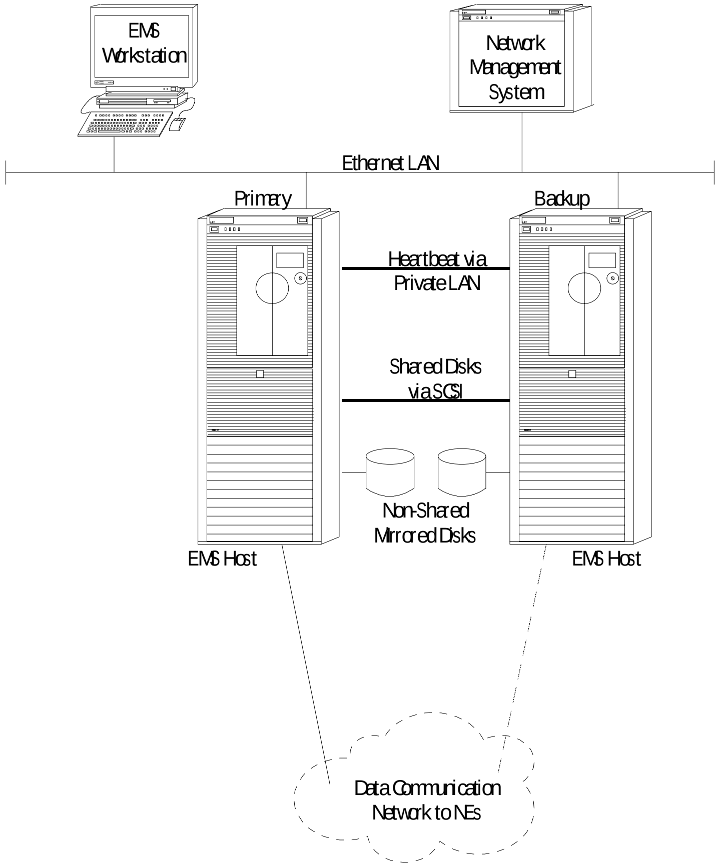
EMS Workstation
Network Management System
Ethernet LAN
Primary
Backup
Heartbeat via Private LAN
Shared Disks via SCSI
Non-Shared Mirrored Disks
EMS Host
EMS Host
Data Communication Network to NEs

Figure 6-2. 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 6-3). 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.

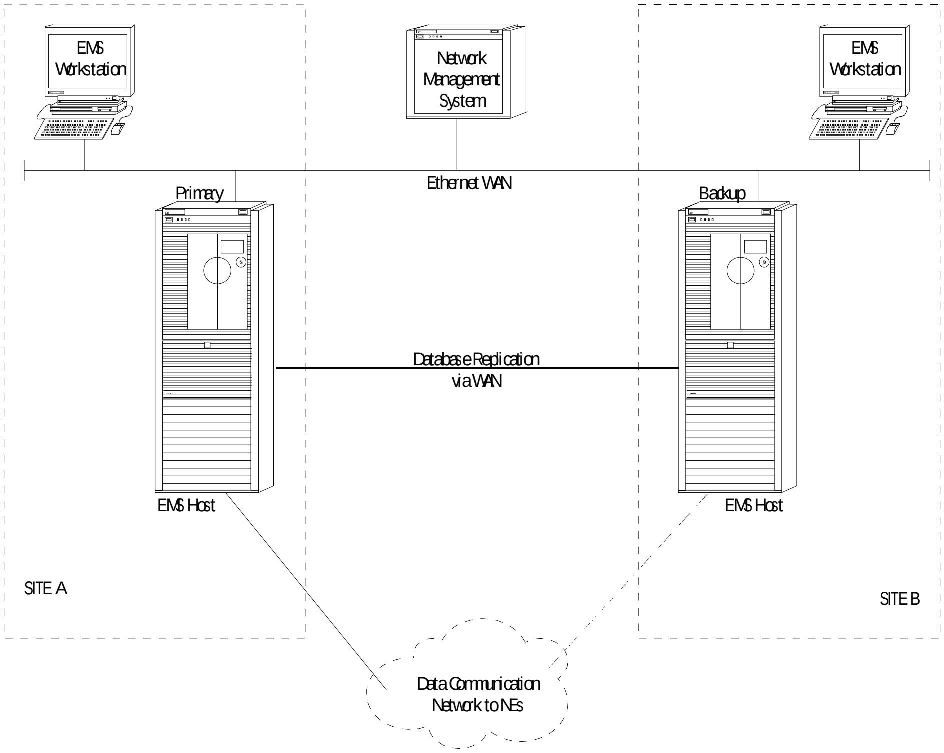
EMS Workstation
Network Management System
EMS Workstation
Ethernet WAN
Primary
Backup
Database Replication via WAN
EMS Host
EMS Host
SITE A
SITE B
Data Communication Network to NEs

Figure 6-3. 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 6-4, both Site A and B have two hosts that can be employed to monitor the network.

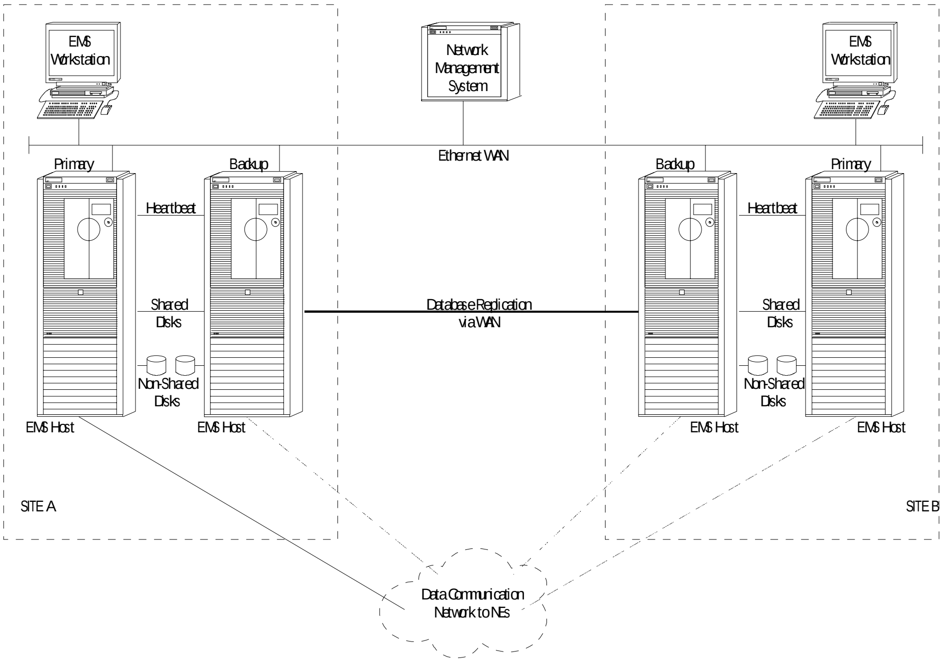

Figure 6-4. EMS Dual Redundancy Configuration

The following redundancies are implemented using the architecture shown in Figure Figure 6-4.

- 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:

3. 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.
4. 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 6-1. 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.

Security Management Concepts

7

Introduction

Purpose

This chapter provides general information about controlling access to WaveStar SNMS and its managed network elements.

Objectives

This chapter explains how to do the following:

- Change user and NE passwords
- Set up users and their level of access to NEs, functions, and commands in WaveStar SNMS

Contents

This chapter discusses the following topics:

Password Administration

Overview

The WaveStar SNMS GUI provides functions for administering user passwords and NE passwords.

Changing an EMS user's password

The Change Password function is the only Administration function that is available to the EMS application user. An EMS user password can be changed at any time. The system verifies that the old password entered matches the one stored in its database for the user.

The first time a user ID (login) is used to log into WaveStar SNMS, the system enforces that the default password must be changed to a new password, and displays the Change Password window for changing it.

Passwords must be changed after a certain period of time (as defined by the system administrator via the Global Security Provisioning window). If a password is about to expire, and a user attempts to log into the system, a pop-up window advises that the password is about to expire and allows the user to change the password at this point. If the expiration period is reached, and the user does not change the password before attempting to log into the system, system access is denied.

WaveStar SNMS maintains a history of password usage. If a user attempts to change the password to one previously used, the system advises that a different password must be specified.

An EMS user login, however, can only be changed by the WaveStar SNMS administrator. See Users for additional information about changing EMS user logins.

Global password administration

NEs have default login/passwords that are defined at the manufacturer prior to shipment. The NE login/password is required by the EMS user to gain access to the NE. The system GUI allows you to modify an individual NE's primary and backup password through the Add/Modify an NE window or via Cut-Through mode. However, if the network has a large number of NEs, this can be a very time-consuming process.

The Global Password Administration feature, which is available only for Lucent Technologies NEs, through the GUI, allows you to change the primary and/or backup passwords for a number of NEs at the same time. This feature allows global password change for:

- Individual NEs (by TID)
- All NEs
- NEs by type
- Aggregate (collection of NEs)

Changes to the primary and/or backup NE passwords are sent to the selected NE(s) and the local WaveStar SNMS database is automatically updated with the password information.

The global password update process can be aborted at any time while the Global Password Administration window is open.

Only one person can use the Global Password Administration feature at a time.

Related tasks

See the related tasks in the Security Management chapter.

Network Security

Introduction

The WaveStar SNMS system provides network security by allowing an administrator to define users and the extent of their access to NEs in the network and capability of performing certain functions and commands through the system.

Levels of access are defined by:

- User/password administration and NE/command access
- Command Groups
- Target Groups
- NE login administration

Users

A user is identified by a login and password and is provided access to the functions and features of the system as defined by the system administrator.

A user ID is defined for each user that accesses the system. The user ID (login) assigned to each user must be unique and contain 3-10 alphanumeric characters with no white spaces. When a user logs into WaveStar SNMS, the user ID is validated with the current password. If a user fails to log in with a valid user ID/ password combination after a number of times (as defined by the administrator), the user ID is automatically disabled and prohibited from logging into WaveStar SNMS. An “Invalid Login” message is displayed, an alarm is issued, and the user ID session is terminated.

The WaveStar SNMS system administrator can create, delete, and modify users (by user login) and their access permissions. Before any user can access the system, the user must be assigned a login and appropriate Target Group and Command Group access permissions.

The administrator can also copy the login group settings, Command Group, and Target Group settings from an existing user to a newly defined one.

When a user login is created by the administrator, it is initially set up with the following default values:

- User ID Login Type—GUI
- Password—no default password, must be entered by the administrator
- Command Group—Empty
- Target Group—Empty

Changing a user’s login

To change a user’s login, the system administrator must first delete the user and then re-enter the user in the system with a new login.

User management

WaveStar SNMS has a number of built-in security features to inhibit or prevent unauthorized user access to the system and to monitor user activity.

Through GUI functions, an WaveStar SNMS administrator or a user with a privileged login can:

- terminate an active user login’s session
- enable or disable user logins
- set a limit of the number of failed login attempts before preventing a user from logging into WaveStar SNMS
- set the password aging interval for user logins
- issue a warning notice to users when their password is about to expire
- maintain a history of previously used passwords
- set the session timeout interval for logins
- set the expiration period for user logins
- specify the message that is issued when a user successfully logins into WaveStar SNMS
- view all currently active user login sessions

Alarms and user logins

WaveStar SNMS generates a Minor alarm when any of the following conditions occur:

- a user ID is automatically disabled due to excessive failed login attempts
- a user ID is deleted due to lack of use
- a password change for a user ID is unsuccessful

Any of the above conditions may indicate a possible threat or attempted breach of system security. A Minor alarm is generated against the application itself (TID=EMS) which can only be accessed by the EMS system administrator.

Related tasks

See the related tasks in the Security Management chapter.

Command groups

A Command Group, also known as a user class, is a collection of EMS and NE commands that a specified user is allowed to enter through the system GUI. Each user is assigned to one and only one Command Group.

The system has a set of pre-defined Command Groups:

- Maintenance Command Group—This Command Group allows access to all Maintenance and Performance Management Category commands with Authorization Level 4 or less. (For an explanation of Authorization Levels, see the NE logins (OLS 400G NEs only) section in this chapter.) This group of commands allows a user to view and modify all NE Maintenance information.
- Provisioning Command Group—This Command Group allows access to all Provisioning Category command with Authorization Level 4 or less. This group of commands allows a user to view and modify all NE provisioning information.
- Report-Only Command Group—This Command Group allows access to all categories of commands with Authorization Level 2 or less. (For an explanation of Authorization Levels, see the NE logins (OLS 400G NEs only) section in this chapter.) This restricts a user to only being allowed to view NE information but not change it.
- General Command Group—This Command Group allows access to all categories of commands with Authorization Level 3 or less. This allows a user to view and modify most NE information.
- Privileged Command Group—This Command Group allows a user access to all categories of commands with Authorization Level 4 or less. (For an explanation of Authorization Levels, see the NE logins (OLS 400G NEs only) section in this chapter.) This allows a user to view and modify almost all NE information, except for Administrator functions.
- All Command Group—This Command Group allows access to all commands, including Administrator functions supported by the NE. This is the super-user NE Command Group and is automatically assigned to the *admin* logins; other user IDs may be assigned to this command group. It is usually reserved for the EMS administrator.
- Empty—This Command Group is set up with no commands.

The WaveStar SNMS system administrator can add, modify, or delete Command Groups. Additional Command Groups can be defined as needed by the administrator.

The system administrator can also copy the contents of an existing Command Group to a newly defined one.

Related tasks

See the related task in the Security Management chapter.

Target groups

A Target Group is a collection of NEs that a user can access. Together with Command Groups, Target Groups define user permissions and provide network security. Each user is assigned to one and only one Target Group.

The system has two pre-defined Target Groups:

- All Targets—provides access to all NEs in the network
- Empty—denies access to any NEs

The WaveStar SNMS administrator can add, modify, or delete Target Groups. Additional Target Groups can be defined as needed by the system administrator.

The system administrator can also copy the contents of an existing Target Group to a newly defined one.

Related tasks

See the related tasks in the Security Management chapter.

NE logins (OLS 400G NEs only)

WaveStar SNMS allows an administrator or a user with a privileged login to administer user logins that are used to log directly into an OLS 400G NE. The level of NE access and the type of activities available to an NE login can be defined.

WaveStar SNMS allows you to define:

- NE logins
- Passwords for NE logins
- User Privilege Codes—a listing of exact permission levels to access functionality provided by the NE
- Temporary NE logins with an expiration date
- Copy of settings (User Privilege Codes) from another login (**Note: this does not include the ability to copy the login or password from another NE login**.)
- Password Aging/Expiration Time—the length of time (in days) that a password for an NE login can be used before it has to be changed to a new one

User privilege codes

When adding or modifying an NE login or copying another NE login's settings, a User Privilege Code is used to indicate the level of access to NE functions. A User Privilege Code is a combination of the Function Category and Authorization Level allowed.

The Functional Categories are as follows:

- **Maintenance (M)** - This Functional Category contains all of the Fault Management-related functions/features.
- **Provision (P) -** This Functional Category contains all of the Configuration Management-related functions/features.
- **Performance Management (PM) -** This Functional Category contains all of the Performance Management-related functions/features.
- **Security (S) -** This Functional Category contains all of the EMS Security and Administration-related functions/features.
- **Test (T) -** This Functional Category contains all of the Test Access-related features (applies to WaveStar BWM NEs only)

Each Functional Category has Authorization Levels consistent with NE privileges. The Authorization Levels are as follows:

- 1 - Empty (Lowest)
- 2 - Reports Only
- 3 - General
- 4 - Privileged
- 5 - Super User (Highest)

NOTE:
The User Privilege Code on Super User NE logins cannot be modified.

The combination of a Functional Category and Authorization constitutes a User Privilege Code for a specific set of features.

Each NE must have at least one NE login with a Super User Authorization Level, to support any management task that may be required in the NE.

Example: user privilege code

The User Privilege Code “M3” indicates that an SNMS user login is authorized to execute all Maintenance Category functions with Authorization Level 3 or less. Therefore, the user logging into an NE with this User Privilege Code is allowed to use the following EMS features:

- Cut-Through
- TL1 Macro Builder
- TL1 Broadcaster
- View Alarm Monitoring Statistics
- View Alarm Severity Assignment Profiles

- Resynchronize Alarms
- View Protection Switch Messages
- Provision Alarm Provisioning

Functions available by authorization level/functional category

The following table shows the functions/features that can be performed for each Authorization Level by Functional Category.

Table 6-1. **Functions Available By Authorization Level/Functional Category**

Auth. Level	Maintenance (M)	Provision (P)	Performance Management (PM)	Security (S)
1	CUT-THROUGH, TL1 MACRO BUILDER, TL1 BROADCASTER	CUT-THROUGH, TL1 MACRO BUILDER, TL1 MACRO SCRIPTS, TL1 BROADCAST	CUT-THROUGH, TL1 MACRO BUILDER, TL1 MACRO SCRIPTS, TL1 BROADCASTER	CHANGE PASSWORD, VIEW USER PREFERENCES
2	VIEW ALARM MONITORING STATISTICS, VIEW ALARM SEVERITY PROFILES, MODIFY ALARM SEVERITY PROFILES	RING UTILIZATION, VIEW CROSS CONNECT, VIEW EQUIPMENT, VIEW PATH, VIEW PROVISION NE, VIEW PROVISION PORT	VIEW PM DATA	COPY POSITIONS, COPY PREFERENCES, MOVE NODE, RESTORE MAP SETTINGS, RESTORE POSITIONS, RESTORE PREFERENCES, SAVE MAP SETTINGS, SAVE POSITIONS, SAVE PREFERENCES, VIEW ALL CMDRSP LOGS, VIEW LOGS
3	FILTER ALARMS RESYNCHRONIZE ALARMS, VIEW PROTECTION SWITCH MESSAGES, PROVISION ALARM PROVISIONING	ADD CROSS CONNECT, ADD PATH, COPY PATH, CREATE OPTICAL ASSOCIATION, DELETE CROSS CONNECT, DELETE OPTICAL ASSOCIATION, DELETE PATH, MANUAL DNO, MODIFY CROSS CONECT, MODIFY OPTICAL ASSOCIATION, MODIFY PATH, PROVISION EQUIPMENT, PROVISION NE, PROVISION PORT, PROVISION PROTECTION GROUPS		AUTO DNO, AUTO DTSYNC, BACKUP NE, MANUAL DNO, MANUAL DTSYNC, SCHEDULE BACKUP, SCHEDULE DNO, SCHEDULE DTSYNC, SPRING FALL CHANGE

Table 6-1. **Functions Available By Authorization Level/Functional Category**

Auth. Level	Maintenance (M)	Provision (P)	Performance Management (PM)	Security (S)
4	ALL ALARM MONITORING, ENABLE FULL ALARM MONITORING, ENABLE PARTIAL ALARM MONITORING, PROVISION PROTECTION SWITCH	ESTABLISH EQUIPMENT, REMOVE EQUIPMENT	GLOBAL PM MGMT, NE PM MANAGEMENT	ADD AGGREGATE, ADD GNE ASSOCIATION, ADD NE, ADD SUBNET, ADD TRAIL, CHANGE AGGREGATE CONTENTS, DATE TIME MANAGEMENT, DELETE AGGREGATE, DELETE GNE ASSOCIATION, DELETE NE, DELETE SUBNET, DELETE TRAIL, GLOBAL PASSWORD ADMIN. MODIFY AGGREGATE, MODIFY GNE RNE ASSOCIATION, MODIFY NE MODIFY SUBNET, NE SW ACTIVATE, NE SW COPY, NE SW DELETE, NE SW DOWNLOAD, NE SW TRANSFER, PROVISION DSA, RESTORE NE, RETRY INTERVALS, SCHEDULE SW ACTIVATE, SCHEDULE SW COPY, SCHEDULE SW DOWNLOAD, SWITCH ACTIVE GNE, VIEW DESCRIPTIVE INFORMATION
5				ADD COMMAND GROUP, ADD TARGET GROUP, ADD USER, DELETE COMMAND GROUP, DELETE TARGET GROUP, DELETE USER, MODIFY COMMAND GROUP, MODIFY TARGET GROUP, MODIFY USER,

TL1 commands available by authorization level/functional category

A User Privilege Code also defines the TL1 commands that can be issued to the NE when an NE login is added or modified.

The Functional Categories defined for TL1 commands are:

- **Maintenance (M)** - This Functional Category contains all the Fault Management-related features.
- **Provision (P)** - This Functional Category contains all the Configuration Management-related features.
- **Performance Management (PM)** - This Functional Category contains all the Performance Management-related features.

- **Security (S)** - This Functional Category contains all NE Security and Administration-related features.
- **Test Access (T)** - This Functional Category contains all the Test Access-related features (applies to Wavestar BWM NEs only).

The Authorization Levels for issuance of TL1 commands are:

- 1 - Minimal (Lowest)
- 2 - Reports Only
- 3 - General
- 4 - Privileged
- 5 - Super User (Highest)

The following table shows the TL1 commands that can be issued for WaveStar NEs for each Authorization Level by Functional Category.

Table 6-2. **WaveStar Network Element TL1 Commands by Authorization Level/Functional Category**

Auth. Level	Maintenance (M)	Provision (P)	Performance Management (PM)	Security (S)	Test (T)
1	ACT-USER, CANC-USER, RTRV-ALM, RTRV-ALM-ENV, RTRV-ASAP-ASGNMT, RTRV-ASAP-PROF, RTRV-CMD-STAT, RTRV-COND, RTRV-FLT-ISLT, RTRV-FLT-STATE, RTRV-LRBK, RTRV-OW, RTRV-PROTN-GRP, RTRV-SYNCN	ACT-USER, CANC-USER, RTRV-rr, RTRV-EQPT	ACT-USER, CANC-USER, RTRV-TCA-ASGNMT, RTRV-TCA-PROF	ABT-CMD, ACT-USER, CANC-USER, ED-PID, RTRV-EQPT, RTRV-FECOM, RTRV-FECOM-LAN, RTRV-HDR, RTRV-MAP-NEIGHBOR, RTRV-MAP-NETWORK, RTRV-NE, RTRV-PRMTR-DATA, RTRV-PRMTR-SFTWR, RTRV-STATE-EQPT, RTRV-ULS, RTRV-ULS-DCC-L3, RTRV-ULSDCC-L4	ACT-USER, CANC-USER, RTRV-TACC
2	RTRV-BSW, RTRV-BSW-PORT, RTRV-MAP-RING, TEST-ALM, TEST-LED, TEST-TRMSN	RTRV-CRS,RTRV-RSVN, RTRV-STATE-EQPT, RTRV-TMSLT	RTRV-PM-rr	RTRV-AO, RTRV-LOG-ALM, RTRV-LOG-NTFCN, RTRV-LOG-PROTNSW, RTRV-LOG-USER, RTRV-MAP-RING, RTRV-NE-SECU	CONN-TACC, DISC-TACC

Table 6-2. **WaveStar Network Element TL1 Commands by Authorization Level/Functional Category**

Auth. Level	Maintenance (M)	Provision (P)	Performance Management (PM)	Security (S)	Test (T)
3	ALW-ALM, ALW-MSG, DLT-ASAP-PROF, ED-ASAP-PROF, ENT-ASAP-PROF, INH-ALM, INH-MSG, OPR-EXT-CONT, OPR-LPBK, RLS-EXT-CONT, RLS-LPBK, SET-ATTR-ALM, SET-ATTR-CONT, SET-ATTR-ENV, SET-OW, SET-SYNCN	CNVT-CRS-TPY, DLT-CRS, DLT-EQPT, DLT-RSVN, ED-CRS, ED-rr, ED-EQPT, ED-RSVN, ENT-CRS, ENT-EQPT, ENT-ROLL, ENT-RSVN	INIT-REG	ALW-NVM-MIRROR, DLT-ULSDCC-L4, ED-NE, ENT-FECOM, ENT-FECOM-LAN, ENT-ULS, ENT-ULS-DCC-L3, ENT-ULSDCC-L4, INH-NVM-MIRROR, RTRV-SECU-USER, SET-SID	CHG-ACCMD, CHG-TACC, ENT-TSTPT, RLS-TSTPT
4	DLT-PROTN-GRP, ED-PROTN-GRP, ED-STATE-EQPT, ENT-PROTN-GRP, OPR-PROTNSW, OPR-SNCNSW, RLS-PROT-NSW, RLS-SNCNSW, RMV-EQPT, RST-EQPT	ED-RDL	DLT-TCA-PROF, ED-TCA-PROF, ENT-TCA-PROF	APPLY, CPY-MEM, CPY-NVM, ED-DAT, ED-EQPT, ED-NE-SECU, ED-STATE-EQPT, INIT-EQPT, INIT-SYS, RMV-LINK, RST-LINK	
5				CANC-USER-SECU, DLT-USER-SECU, ED-USER-SECU, ENT-USER-SECU, RTRV-LOG-SECU	

Related tasks

See the related tasks in the Security Management chapter.

.

Trouble Clearing Concepts

8

Introduction

Purpose

This chapter provides reference information to assist in troubleshooting problems with WaveStar SNMS and its communications interfaces.

Contents

This chapter discusses the following topics:

X.25 Log Files

Overview

The X.25 software on the HP computer maintains a log of any unusual events that may have occurred during the day. These files are located in the */var/opt/acc/log* directory.

Daily X.25 logs

There is one log file for each day of the week. The files are named as follows:

mon.tlog *tue.tlog* *wed.tlog*

thu.tlog *fri.tlog* *sat.tlog*

sun.tlog

NOTE:
Be careful to check the date and time stamp of each file. If today is Friday, but the date and time stamp for the *fri.tlog* file is old, then that file is from a previous Friday and no messages have been logged to the file today. This is very common and indicates there was no unusual activity on the X.25.

X.25 messages

Every X.25 message that appears on the console terminal is also echoed to the appropriate log file.

Here are two of the more common messages that may be found in a log file:

Sample #1:

```
-----------------------------------------------------------------
Wed Mar 27 14:32:19 1996: zmlog: message logging resumed
-----------------------------------------------------------------
14:32:19 x25cn 00811 1 Link ZLU 5 DOWN: Link disc. on loss of carrier
14:32:35 x25cn 00812   Link ZLU 5 Link established
14:32:35 x25cn 00820   Link ZLU 5 Link restarted
```

The ZCOM Logical Unit (ZLU) Link number is actually the Physical Port Number +1. On the MUX Panel, the ports are labeled J0 through J7 for ports 0 to 7. The ZLU links are numbered 1 to 8, respectively.

Therefore, the above message indicates that Port 4 lost carrier at 14:32:19 on Wed March 27. The link then came back at 14:32:35 and successfully established and restarted Level 2 synchronization.

Sample #2:

```
------------------------------------------------------------------
Sat Mar 23 11:55:55 1996: zmlog: message logging resumed
------------------------------------------------------------------
11:54:04 zcom  00000   System bootup
11:55:55 zmon  00002   Resource manager (Rev 1.31) for ZCOM 4.3.0.0
11:55:55 zmon  00005   Stopping system ...
11:55:55 zmon  00075   ZCOM system stopped
11:55:55 zmon  00002   Resource manager (Rev 1.31) for ZCOM 4.3.0.0
11:55:55 zmon  00003   Cold start with: /usr/zcom/cfg/x25.tmem
11:55:56 zmon  00100   Card 0 starting up ...
11:56:04 zmon  00110   Card 0 startup successful, card READY
11:56:04 zmon  00020   Cold start completed, ZCOM system ready
11:56:04 zmon  00004   Waiting for ZMON requests ...
11:56:04 zcom  00165   Node 123 comes UP
11:56:05 x25cn 00000   X.25 Control Rev 12.2.11p2 - 940303
11:56:05 x25cn 00000   Logical terminal area X25CNT: 88 Bytes
11:56:05 x25cn 00139   Trace logging disabled
11:56:05 x25cn 00000   COLD start : HGrp# [1-10] : HGrp size [1-20]
11:56:05 x25cn 00816   Link ZLU 1 X.25 shutdown complete
11:56:06 x25cn 00811 1 Link ZLU 1 DOWN: Link disc. on loss of CTS
11:56:06 x25cn 00816   Link ZLU 2 X.25 shutdown complete
11:56:06 x25cn 00816   Link ZLU 3 X.25 shutdown complete
11:56:06 x25cn 00811 1 Link ZLU 2 DOWN: Link disc. on loss of CTS
11:56:06 x25cn 00811 1 Link ZLU 3 DOWN: Link disc. on loss of CTS
11:56:06 x25cn 00816   Link ZLU 4 X.25 shutdown complete
11:56:06 x25cn 00816   Link ZLU 5 X.25 shutdown complete
11:56:07 x25cn 00816   Link ZLU 6 X.25 shutdown complete
11:56:07 x25cn 00811 1 Link ZLU 6 DOWN: Link disc. on loss of CTS
11:56:07 x25cn 00816   Link ZLU 7 X.25 shutdown complete
11:56:07 x25cn 00811 1 Link ZLU 7 DOWN: Link disc. on loss of CTS
11:56:07 x25cn 00816   Link ZLU 8 X.25 shutdown complete
11:56:08 x25cn 00812   Link ZLU 8 Link established
11:56:08 x25cn 00811 1 Link ZLU 5 DOWN: Link NOT established on
ENABLE
11:56:10 x25cn 00812   Link ZLU 5 Link established
11:56:10 x25cn 00820   Link ZLU 5 Link restarted
11:56:12 x25cn 00812   Link ZLU 4 Link established
11:56:12 x25cn 00813   Link ZLU 8 reset: Reset due to received SABM
11:56:12 x25cn 00820   Link ZLU 4 Link restarted
11:56:15 x25cn 00820   Link ZLU 8 Link restarted
```

The preceding message indicates that the X.25 processes were restarted at 11:54:04 and finished re-establishment of communications at 11:56:15. The software download to the MUX Card was successful. If there was a problem with the MUX Card, it would have been reported here.

The Link ZLU lines at the bottom of the display report which links re-established Level 2 synchronization.

Checking X.25 level 2 status

You can retrieve the Level 2 status by using the **X25_check** command at any time.

Related tasks

See the following related tasks in the Trouble Clearing chapter:

- Check Level 2 Status of X.25 Network Connections
- Check the Virtual Channel Status of an X.25 Port
- Obtain X.25 Virtual Channel Non-Data Packet Statistics
- Obtain X.25 Virtual Channel Data Counters
- Reset an X.25 MUX Port
- Restart X.25 Processes

WaveStar SNMS/WaveStar NMS Interface Troubleshooting

Overview

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 WaveStar 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 NM and 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.

NOTE:
If notifications are not received by WaveStar NMS (SONET), verify that the local DNS Domain Name is not set.

GUI-to-GUI interface setup

Configuration File

A configuration file, called *emsFint.cfg*, is delivered with each release of WaveStar SNMS. This file will define the operation of the F-interface. The configuration parameters defined by this file are:

1. whether debugging is enabled for the F-interface software
2. the idle-session timeout for the F-interface.
3. mapping of the SNMS software version number to directories containing SNMS GUI software on the NT Terminal Server
4. override username and password settings for WaveStar SNMS login

The file is a flat, ASCII text file editable by the notepad program. Configuration parameters are defined as name value pairs. Help text in the file explains the purpose of each parameter.

The path of the default F-interface configuration file is:

<default root directory of SNMS/SNMS GUI directory>/ems/fint/emsFint.cfg

The file is identical across all versions of WaveStar SNMS software.

For the F-interface to work properly, this file must be properly configured and a copy of this file MUST be installed in the NM GUI software directory location:

/jui/jnm/itm/southbound/ems/emsFint

Debugging Configuration Parameter

The default debugging parameter configuration file entry is:

```
debug          false
```

The valid values for the true and false. The value should be set to true when the F-interfce is not working and more detailed information about the fault is required.

When debugging is enabled on the F-interface, the debug output will be captured in the WaveStar NMS output log file.

Idle Timeout Configuration Parameter

The default idle session timeout configuration file entry is:

```
idleTimeout          600
```

This timeout value overrides the WaveStar SNMS GUI timeout defined on the Global Security Parameter Screen because the F-interface is a resource intensive interface and it should not be allowed to remain active as long as an individual WaveStar SNMS user login session.

The timeout value is defined in seconds so the default timeout value, as displayed above, is ten minutes. The idle session timeout can be disabled by setting the value to 0.

Release Number/GUI Directory Mappings

When an EMS is defined in the WaveStar NMS database, the type of EMS is defined and the release number of the EMS Software is also defined. When the F-interface is invoked, this release number is used by the F-interface software to find the correct version of the SNMS GUI Software.

Valid release numbers can be any string, but typical values are: R3.0, R2.1. The configuration file must define a directory for each release number defined in WaveStar NMS.

The default configuration file entries for these mappings are:

```
release     default      \snmsR2
release     R10.0        \snmsR3
release     R9.0        \snmsR21
release     R8.0        \snmsR2
release     R6.0        class=itm.southbound.ems.emsfint.EmsFint
```

The first line defines the GUI software that will be used when an undefined release number is found by the F-interface. In this case, when a unknown release number is sent via the F-interface, the GUI contained in the \snmsR2 directory will be used.

IMPORTANT: these definitions assume that the WaveStar NMS GUI and the WaveStar SNMS GUIs are located on the same drives (generally C drive).

Username and Password Configuration Parameters

By default, the user login name for the F-interface is itm and the password is itm+123. For security reasons, default passwords are not defined in the configuration file. However, if configuration parameter entries are entered in the configuration file, the defined entries will override the default values.

Valid configuration file entries for username and password are:

```
user          itm
password      itm123
```

WaveStar NMS Software Configuration

Since some WaveStar SNMS java code runs in the WaveStar NMS JVM, a single instance of the SNMS GUI must be included in the NM classpath. The NM classpath is defined in the file:

/jui/bin/run_jnm.bat

Generally, the NM is preconfigured to invoke an WaveStar SNMS R3 GUI located in the \snmsR3 directory. If an SNMS R3 GUI does not exist in \snmsR3 directory on the NT Terminal Server, the NM configuration file will need to be changed.

The typical classpath definition for a WaveStar SNMS CLASSPATH in the run_jnm.bat file is:

```
EMSDIR=%3\emsR10
EMSPATH=%EMSDIR%;%EMSDIR%\jars\swing.jar;%EMSDIR%\jars\IE.jar;%
EMSDIR%\jars\org.jar

CLASSPATH=<NM Classpath>;%EMSPATH%
```

WaveStar SNMS R2.1 and WaveStar SNMS R4.2 Cut-through Interoperability

Due to functionality changes between WaveStar SNMS Releases 2.1 and 4.2, the data communicated on the F-interface is different between the two releases of GUI software. Therefore, the data file (i.e. java class file) from the SNMS R4.2 software must be copied into the snmsR2.1 directory.

To copy the file, execute the following command on at the MS_DOS prompt:

```
copy \snmsR3\ems\fint\emsFintObject.class\snmsR2.1\ems\fint\emsFintObject.class
```

In addition, the *\jui\jnm\run_jnm.bat* needs to be changed so that the WaveStar SNMS R4.2 replaces the WaveStar SNMS R2.1 classpath in the NM startup script: */jui/bin/run_jnm.bat*

Related tasks

See the following related tasks in the Trouble Clearing chapter:

- Verify Northbound Interface to WaveStar NMS Server
- Test WaveStar SNMS to WaveStar NMS Cut-Through

Glossary

9

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