Lucent Technologies
Bell Labs Innovations

WaveStar® ITM-SC Release 8.0

Administration Guide

365–312–518
CC109076802
Issue a
June 2001

For permission to reproduce or distribute, please contact:

Customer Training and Information Products (CTIP)	1 800 645 6759 (continental) 1 317 322 6847 (international)

Notice

Every effort was made to ensure that the information in this Information Product (IP) was complete and accurate at the time of printing. However, information is subject to change. This IP describes certain hardware, software, features, and capabilities of Lucent Technologies products that may not be the same as the equipment that you have. The IP is for information purposes, and you are cautioned that it may not describe your specific equipment

Mandatory Customer Information

Overview EMC/ESD Safety

The EMC/ESD boundary has been defined at Rack/Subrack level. The principle is based on the “Faraday Cage” theory. If there are doors, then the doors must be closed. With every rack/subrack an ESD (electrostatic discharge) earth socket and an ESD sticker are supplied. On the Rack frame ETSI an ESD bonding point for an ESD wrist strap is present. It is mounted in a way that it’s always accessible for installation, normal operation and maintenance activity.

Wrist Strap

Wrist Strap The wrist strap must be worn when opening the Subrack doors.

Electrostatic Sensitive Devices

The equipment described in this guide contains static sensitive devices. Electrostatic Discharge Precautions should be taken when operating or working on this equipment.

Special handling precautions apply whenever installing or removing parts of the equipment include:

- Leaving components or equipment in original packaging until required for use.
- Removing plug-in units with previously discharged hands (e.g. using grounded wrist straps connected to the ESD Bonding Point on the Cabinet).
- Returning items for repair in suitable antistatic packaging.

Trademarks

UNIX is a registered trademark of UNIX Systems Laboratories, Inc.

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

HP-VUE is a registered service mark of Hewlett-Packard, Inc.

INFORMIX is a registered trademark of Informix Software, Inc

OSF/Motif is a registered trademark of Open Software Foundation.

Microsoft is a registered trademark of Microsoft Corp.

Windows is a registered trademark of Microsoft Corp.

Netscape is a trademark of Netscape Communications Corp.

Netscape Navigator is a trademark of Netscape Communications Corp.

Netscape Communicator is a trademark of Netscape Communications Corp.

Pentium is a registered trademark of Intel Corp.

QuickTime is a registered trademark of Apple Computer Inc.

Adobe is a trademark of Adobe Systems Inc.

Acrobat is a trademark of Adobe Systems Inc.

PostScript is a trademark of Adobe Systems Inc.

Ordering Information

The order number of this document can be found on the frontpage.

Support

Technical support

Please contact your Lucent Technologies Local Customer Support Team (LCS) for technical questions about the information in this document.

Information product support

Lucent Technologies values your comments!

Lucent Technologies
Bell Labs Innovations

WaveStar® ITM-SC Release 8.0
Administration Guide

365–312–518 Issue a June 2001

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

Lucent Technologies values your comments!

Lucent Technologies
Bell Labs Innovations

WaveStar® ITM-SC Release 8.0
Administration Guide

365–312–518 Issue a June 2001

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

Section: Modifying ITM-SC User Information

Section: Deleting ITM-SC Users

Section: Creating User Roles

Section: Editing User Roles

Section: Deleting User Roles

Section: Configuring Access Groups

Section: Assigning User Role and Access Domain

Section: Logging in as Root

Section: Changing Password

Section: Configuring Password Ageing

Section: Configuring Illegal Access

Section: Displaying the CIT Access List

Section: Editing CIT Access

Section: Changing the Default ITM-SC Server

Section: Configuring Message of the Day

Section: Managing Shutdown Broadcast

Section: Managing NE Timing

Section: Managing MEC Files

Section: Managing Card Types

Section: Configuring Systems Alarm Monitoring

Section: Configuring ITM-SC for Double Alarm Acknowledgment

Section: Enable ITM-SC for Alarm Beeping

Section: Setting EMS Event Parameters

Section: Setting EMS Event Control

Section: Setting All NE Event Control

Section: Enabling Alarm Color Indication Modification

Section: Changing Alarm Color Indication

Section: Viewing Event Storage Capacity

Section: Managing ITM-SC Database Archives

Section: Managing Event Archives

Section: Archiving PM Data

Section: Backing up the Entire ITM-SC System

Section: Backing Up the ITM-SC Database

Section: Disk Mirror Installation and Setup

Section: Configuring a cold stand-by ITM-SC

Section: Installing a Uninterruptible Power System (UPS)

Section: Adding or Deleting a Peer ITM-SC

Section: Adding Network Elements to the Geographic Redundancy Scheme

Section: Removing Network Elements from the Geographic Redundancy Scheme

Section: Enabling or Disabling Protection of Network Elements

Section: Displaying Protected Network Elements

Section: Displaying Protecting Network Elements

Section: Transferring Network Element Control to the Secondary ITM-SC

Section: Returning Network Element Control to the Primary ITM-SC

Section: Editing the Gateway Address

7 Management Communication of the ITM-SC

Section: Maintaining Network Addresses

8 Trouble Clearing

Section: Restoring the ITM-SC Database

Section: Restoring the Entire ITM-SC System

Section: Performing a MIB Upload

Section: Performing a MIB Download

Section: Using the Event Lists

Section: Managing ITM-SC Log Files

Section: Managing Operator Log Files

Section: Managing Operator Log Archives

9 ITM-SC Upgrade

Section: Starting and Stopping the ITM-SC

Section: ITM-SC Maintenance Upgrade

10 Concepts

Section: Security Management

Section: ITM-SC System Administration

Section: Provisioning Environment Setup

Section: Maintenance Environment Setup

Section: ITM-SC Reliability

Section: Management Communication of the ITM-SC

Section: Trouble Clearing

11 Using the ITM-SC Interface

Section: HP-Vue Specific Subjects

Section: ITM-SC Specific Modules and Windows

Section: ITM-SC General Tasks

Section: ITM-SC Network Map

About this information product

Purpose

The purpose of the ITM—SC Administration Guide (AG) is to provide the system administrator with all information necessary to administer the Integrated Transport Management-Subnetwork Controller (ITM-SC) so that it can be used as a centralized management system. The SAG is a management system oriented manual and is shipped to all sites where the ITM-SC is installed.

Reason for reissue

First issue.

Safety labels

Safety guidelines are not applicable for the ITM-SC.

Intended audience

The intended audience of the Subnetwork Controller Administration Guide is personnel who take care of administering the centralized management system in the SDH networks.

How to use this information product

The Subnetwork Controller Administration Guide (SAG) is divided into a number of chapters. Through this division readers can quickly select the subject of their interests and needs.

This guide is divided into the following chapters:

- *About this information product*: brief description over how to use this guide.
- *Security Management*: describes how to administer ITM-SC users by using the ITM-SC. It describes how each user can have different functionality and can have different NEs to manage. Furthermore it describes how the ITM-SC can be used to control the ITM-cit users.
- *ITM-SC System Administration*: comprises typical administration task such as provisioning date and time, add licenses and modify server settings.
- *Provisioning Environment setup*: comprises features how to set up the ITM-SC environment for provisioning operators.
- *Maintenance Evironment Setup*:describes how to set up the ITM-SC environment for maintenance operators.
- *ITM-SC Reliability*: describes tasks which will increase the reliability of the ITM-SC its functionality. This can be done by adding extra hardware or creating a software backup of the ITM-SC.
- *Management Communication of the ITM-SC*: taks to set or change the address of the ITM-SC in a network.
- *Trouble Clearing*: help when the ITM-SC system is halted or interrupted in its normal operation. Tasks to investigate the cause of the problems are provided as well.
- *ITM-SC Upgrade*: provides information how to perform an upgrade of the ITM-SC.
- *Concepts*: provides concepts of some topics addressed in this guide.
- *ITM-SC Tutorial:*This chapter explains the concepts over how to use the ITM-SC in combination with a Network Element and describes procedures to configure the ITM-SC so that it can communicate with the Network Element.
- *Glossary*: In this chapter all the special terms, used in this manual, are listed.

Conventions used

This guide uses the following notations

⚠ DANGER

Suggests the possibility of a personal injury

CAUTION

Suggests the possibility of service interruption

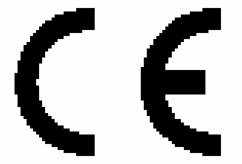
WARNING

Suggests the possibility of equipment damage or software corruption

Important! Gives supplementary information

Approval mark

The following CE approval mark applies to this product.



CE Marking is the indicator for products conform with relevant European Community (EC) Directives. CE stands for Conformité Européenne. The CE-marked transmission equipment is compliant with one EC Directive: 89/336/EEC - Electro-magnetic compatibility (EMC). In this manual you will find several chapters in relation with the CE-marking, for example the use of EMC closed connector Hoods, filtered connectors, and warnings to use a wrist strap when handling equipment.

Related industry standards

The whole masking tree is described in the following standards:

- ITU-T recommendation G.783, issue April 1997
- ETSI standard ETS 300 417-1-1, issue January 1996
- ETSI standard ETS 300 417-2-1, issue April 1997
- ETSI standard ETS 300 417-3-1, issue June 1997
- ETSI standard ETS 300 417-4-1, issue June 1997

Related documents

The following documents are Subnetwork Controller related:

- For more detailed information on the Integrated Transport Management-Subnetwork Controller (ITM-SC), technical characteristics, features, cross-product interworking and system planning and engineering, refer to the: ITM-SC APPLICATION AND PLANNING GUIDE
- For information on installation of the Integrated Transport Management-Subnetwork Controller (ITM-SC), refer to the: ITM-SC INSTALLATION GUIDE
- For information on how to give users access to the Integrated Transport Management-Subnetwork Controller (ITM-SC) and to backup and restore databases, refer to the: ITM-SC ADMINISTRATION GUIDE
- For information on maintenance of the Network Elements with the use of the Integrated Transport Management-Subnetwork Controller (ITM-SC), refer to the: ITM-SC MAINTENANCE GUIDE
- For information on provisioning of the Network Elements with the use of the Integrated Transport Management-Subnetwork Controller (ITM-SC), refer to the: ITM-SC PROVISIONING GUIDE
- For information on corrective procedures and action tables of the Integrated Transport Management-Subnetwork Controller (ITM-SC) refer to the: ITM-SC ALARM MESSAGES AND MAINTENANCE

How to comment

A feedback form has been placed after the title page for your comments or suggestions about this information product. Please copy this feedback form and follow the instructions on the form to submit your feedback.

How to order

Copies of this document can be obtained from CTIP-NL. The website with ordering information: http://www-nds.lucent.com/~sdh

1 Security Management

Overview

Purpose

This chapter describes how to manage the security of the ITM-SC. This is done by administering ITM-SC users. It will describe how each user can have a different functionality and can be assigned to different NEs. Furthermore the ITM-SC can be used to control the CIT users to have restricted access to NEs.

Intended Use

The initial creation or modification of a login name must be performed by the ITM-SC Administrator. Other tasks can both be performed by the ITM-SC Supervisor and ITM-SC Administrator.

Online documentation available

The ITM-SC provides on line documentation of all guides on all ITM products. Short-cut: *Help -> On Line Documentation*.

Abbreviations used

When Network Elements OLS 80G, ADM 4/1, ADM 16/1, ADM16/1c, AM 1 (Plus) and TM 1 are described WaveStar®OLS 80 G, WaveStar®ADM 4/1, WaveStar® ADM 16/1, WaveStar® ADM16/1 compact, WaveStar® AM 1 (Plus) and WaveStar® TM 1 are meant.

Topics

The following topics are discussed:

- creating a user account and assigning users to User Classes
- creating User Roles
- creating Access Groups
- assigning users to User Roles and Access domain
- password Ageing
- changing passwords

- configuring illegal access
- CIT access restriction via the ITM-SC

□

Section: Adding ITM-SC Users

Overview

Purpose Use this procedure to enable a new ITM-SC user to use the ITM-SC.

□

Adding ITM-SC Users

When to perform To create a new user log-in.

Before you begin No specific prerequisites or precautions are needed.

Related information Related procedures are:

- Modifying ITM-SC User Information
- Deleting ITM-SC Users

The related concept is:

- Security Management Overview [10-3]

Parameters used in this procedure can be found at Parameters for Adding ITM-SC Users [1-6].

Procedure Perform the steps below to add users to the ITM-SC:

1 From the *ITM-SC Administration* menu, select the *User Administration* icon.

Result:

The *ITM-SC User Administration* window is displayed.

2 Highlight *Add* and select `Edit`.

Result:

The ITM-SC Add User window is displayed.

3 Enter the *new User Login* name.

4 Highlight the *Password* field. Type the new User Password. Password entries are not visible for security reasons.

5 Set *Class* to the required user class and select `Apply`.

Result:

The *Confirm Password* window is displayed.

6 Re-enter the *User Password* and select `OK`.

Result:

The *Confirm Password* window closes.

7 Select *Close* in the *ITM-SC Add User* window to exit.

8 Select *Close* again to exit from the *ITM-SC User Administration* window.

9 Exit the ITM-SC application

10 Log in as the new user. Only when the new user has performed his first log in the user is added to the database. A user can be selected only when it is present in the database.

END OF STEPS

Follow-up to procedure

After the *new user* has logged in the administrator can assign the new user to a User Role. Log in as administrator to assign the *new user* to a User Role (for procedures refer to *Assigning User Roles* in this chapter). To omit illegal access the administrator is advised to perform the first log in for the new user to test the privileges.

□

Parameters for Adding ITM-SC Users

Introduction

The parameters, as indicated below, are used to add a user login entry.

User Login Name

Indicates the User Login Name. It requires a length of 8 characters. Characters that can be used are: a..z, A ..Z, 0..9 as well as _ + & etc.

Password format and length

Indicates the Password. It requires a length of 6 characters with a maximum of 12. It must contain a minimum of two alphabetic characters and one non-alphabetic character. These characters can be a..z, A..Z, 0..9 and characters such as _ + & etc.

□

Section: Modifying ITM-SC User Information

Overview

Purpose Use this procedure to modify existing user information. This procedure does not affect the user role or the privileges of the user set by the user role.

□

Modifying ITM-SC User Information

When to perform To change a user password and/or user class.

Before you begin The following precautions needs to be considered:

- All password entries are “blanked” for security reasons. Either the current class or password must be changed, otherwise an error message appears when the `OK`button is pressed. During password entries, system messages may be displayed indicating system administrator error of password data entry.

Related information Related procedures are:

- Adding ITM-SC Users
- Deleting ITM-SC Users

Related concepts are:

- Security Management Overview [10-3]

Procedure Follow these steps to modify ITM-SC users:

1 Select the *User Administration* icon from the *ITM-SC Administration* menu.

Result:

The *ITM-SC User Administration* window is displayed.

2 Set *Operation* to Modify.

3 Select the user to modify from the list.

Result:

The selected user is highlighted.

4 Select `Edit`.

Result:

The *ITM-SC Modify User* window is displayed.

5 In the *Password* entry box, fill in the *User Password*.

6 Change *RoleName* to required user class. Select `OK`.

Result:

A *confirm password* window is displayed

7 Re-enter the *User Password*.

Result:

The *Confirm* and *ITM-SC Modify User* windows are closed.

8 Select `Close` to exit from the *ITM-SC User Administration* window.

9 Logout and login as new user to activate the new User Class.

END OF STEPS

□

Section: Deleting ITM-SC Users

Overview

Purpose Use this procedure to delete an existing ITM-SC user. When users are removed from the system, the entry will still exist in the database along with the assigned user role. A deleted user is unable to log into the system.

□

Deleting ITM-SC Users

When to perform To prevent an unused log-in user name to be used.

Before you begin No specific prerequisites or precautions are needed.

Related information Related procedures are:

- Adding ITM-SC Users
- Modifying ITM-SC User Information

Related concepts are:

- Security Management Overview [10-3]

Procedure Follow these steps to delete users from the ITM-SC:

1 Open the *ITM-SC Administration* menu and select the *User Administration* icon.

Result:

The *ITM-SC User Administration* window is displayed.

2 Set *Operation* to *Delete*.

3 Highlight the user to delete from the list and select `Edit`.

Result:

The *ITM-SC Delete User* window is displayed.

4 Select `Yes` or press **ENTER**.

Result:

The user is deleted from the user list.

5 Select `Close` to exit from the *ITM-SC User Administration* window.

END OF STEPS

□

Section: Creating User Roles

Overview

Purpose Use this procedure to create a new user role by means of another user role.

□

Creating User Roles

When to perform

To create a new set of privileges. A privilege consist of a function and access level.

Before you begin

Before performing this procedure make sure::

- the Extended User Class license key is activated.

Related information

Related procedures are:

- Editing User Roles
- Deleting User Roles
- Configuring Access Groups
- Assigning User Role and Access Domain

Related concepts are:

- Security Management Overview [10-3]
- User Roles [10-6]

Procedure

Follow these steps to create a new user role using another user role as a template:

1 Select *User Access* -> *Create User Role*.

Result:

The *Create User Role Menu* is displayed.

2 Click the `Selection Dialog` button to select an available User Role. This available user role will be used as template for the new user role.

Result:

The *User Role Selection Dialogue* window is displayed.

3 Select a user role and select `OK`.

Result:

The *User Role Selection Dialogue* window closes.

4 Highlight the *New Role Name* field. Enter the *new User Role name* in this field. Select `Apply`.

Result:

The new User Role is created.

5 Select `Close` to stop creating new User Roles.

END OF STEPS

□

Section: Editing User Roles

Overview

Purpose When a user need a change in privileges due to for example change in job responsibility the privileges of its User Role needs to be changed accordingly.

□

Editing User Roles

When to perform

To change the privileges of users assigned to a User Role.

Before you begin

When performing this procedure considere the following precaution:

- When changing the privileges of a User Role all users assigned to this User Role will be subject to these changes.

Related Information

Related procedures are:

- Creating User Roles
- Deleting User Roles
- Configuring Access Groups
- Assigning User Role and Access Domain

Related concepts are:

- Security Management Overview [10-3]
- User Roles [10-6]

Parameters used in this procedure can be found at Parameters for Editing User Roles [1-18].

Procedure

Follow these steps to edit a User Role:

1 Select *User Access* -> *User Role Information*.

Result:

The *EMS - User Role Information window* is displayed

2 Select the `Selection Dialog` button.

Result:

The *EMS - User Role Selection Dialogue* window is displayed.

3 Select appropriate *User Role* and select `OK`.

Result:

The *EMS - User Role Selection Dialogue* window disappears.

4 Select `Edit` in *EMS- User Role Information* Window.

Result:

The *EMS - Edit User Role* window is displayed.

5 Change each feature its access level (operation) by selecting feature and appropriate access level (operation) successively. Select `Apply` .

Result:

The changes are made.

6 Select `Close` to stop editing User Roles.

Result:

The *EMS - User Role Edit* window disappears.

7 Select `Close`.

Result:

The *EMS - User Role Information* window disappears.

END OF STEPS

□

Parameters for Editing User Roles

User access levels The available User Role Access Levels are described below:

Access Level	What It Allows
Disabled	Feature is not accessible to the user.
Information	Information windows of features are available but no edit facilities are provided.
Edit	Full access to feature.

□

Section: Deleting User Roles

Overview

Purpose Use this procedure to delete an existing User Role.

□

Deleting User Roles

When to perform When the User Role is not used anymore it is advised to delete the User Role because the number of User Roles is limited.

Before you begin When performing this procedure considere the following precaution:

- It is not possible to delete a User Role when a user is assigned to this User Role.

Related information Related procedures are:

- Creating User Roles
- Editing User Roles
- Configuring Access Groups
- Assigning User Role and Access Domain

Related concepts are:

- Security Management Overview [10-3]
- User Roles [10-6]

Procedure Follow these steps to delete a user role:

1 Select *User Access-> Delete User Role*.

Result:

The *EMS - Delete User Role* window is displayed.

2 Select the `Selection Dialog` button.

Result:

A list of available User Roles is displayed.

3 Select the *User Role* to delete. Note that only user defined user roles can be deleted.

4 Select `OK`.

Result:

The selected User Role is deleted.

5 Select `Close` to stop deleting User Roles.

Result:

The *Delete User Role* window disappears.

END OF STEPS

□

Section: Configuring Access Groups

Overview

Purpose

Access Groups are arbitrarily chosen groups of NEs. An access Group is used to limit the number of accessible NEs for a specific group of users. The Access Domain of a user restricts the access of a user to NEs in this domain. An Access Domain consist of on or several Access Groups. An Access Group can be present in one or more Access Domains.

□

Configuring Access Groups

When to perform

User this procedure to create a new unique Access Group in order to group logical related NEs.By means of the windows described in this section it is also possible to add, modify and delete Access Groups. Only the Add Access Groups procedure is provided below.

Before performing this procedure considere the following precaution:

- There is no correlation between Map Groups and Access Groups. Map Groups are also groups consisting of NEs but only used to customize the Network Map. Access Groups can be used to control user access. The content of Map Groups and Access Groups can be different.

Related information

The related procedures are:

- Creating User Roles
- Assigning User Role and Access Domain

Related concepts are:

- Security Management Overview [10-3]
- User Roles [10-6]

Parameters used in this procedure can be found at Parameters for Configuring Access Groups [1-25].

Add Access Group procedure

Follow these steps to add an Access Group.

1 Select *User Access -> Access Groups*.

Result:

The *EMS - Access Group List* window is displayed.

2 Select `Edit`.

Result:

The *EMS - Edit Access Group* window is displayed.

3 Set operation to *Add*

4 Type the new *Access Group* name in *New Access Group Name* field.

5 Type comment in *comment* field.

6 Select all NEs you want to place in the *New Access Group* from the available NEs list. Select the `Add` button respectively.

7 To remove NEs out of the *Access Group* select the `Remove` button after selecting the NEs.

8 Select `OK`.

Result:

The *EMS - Edit Access Group* window disappears.

9 Select `Close`.

Result:

The *EMS - Access Group List* window disappears.

END OF STEPS

□

Parameters for Configuring Access Groups

Introduction

Below the fields in the Access Group List and Edit Access Group window are listed.

(New) Access Group Name

Name of the Access Group in a maximum of 20 characters.

In Use

Indicates whether the Access Group is assigned to an user. If so deletion will not be allowed.

Comment

Text to help the user identifying Access Groups. A maximum of 50 characters is allowed.

Operation

The user is able to perform the following actions:

- Add: adding a new Access Group to the list of existing Access Groups.
- Modify: changing an existing Access Group. This is only possible if the Access Group is not in use.
- Delete: deleting an existing Access Group. This is only possible if no users are assigned to Access Domains containing these Access Groups.

NE Name

Name of the NE

Type

Type of the NE (for example ADM 16/1)

Primary ITM-SC

The ITM-SC the NE belongs to.

Buttons description

The buttons in the Edit Access Group window are:

Button	Action
Add	Adds the NE(s) in the All NEs list to the subject Access Group list
Remove	Removes the NE(s) in the subject Access Group from the list and returns them to the list of available NEs in the All NEs list.

□

Section: Assigning User Role and Access Domain

Overview

Purpose Once a User Role is designed for a user or a group of users the User Role can be assigned to them in order to give them the appropriate privileges. To restrict a user to manage all Nodes and NEs, Access Domains can be created. When the user is assigned to an Access Domain he will only have access to NEs or Nodes within this domain. □

Assigning User Role and Access Domain

When to perform

Use this procedure to assign a user to a User Role and an Access Domain.

Before you begin

Before performing this procudure make sure the following prerequisites are met:

- Before assigning a user to a User Role the user must be added to the ITM-SC as ITM-SC User and must be given a User Class of Administrator, Supervisor or Operator.
- In order to group several Access Groups into one Access Domain, first the appropriate Access Groups must be created.

Before performing this procedure consider that:

- whenever changes are made to the user’s Access Domain and/or User Role the changes will not be effective in the current session of this user. Only after a new login procedure the changes will be effective.

Related information

The related procedures are:

- Adding ITM-SC Users
- Creating User Roles
- Configuring Access Groups

Related concepts are:

- Security Management Overview [10-3]
- User Roles [10-6]

Parameters used in this procedure can be found at Parameters for Assigning User Role and Access Domain [1-29].

Procedure

Follow these steps to assign a user role and user domain:

1 Select *User Access* -> *User Access Profiles* from the top level menu.

Result:

The *EMS - User Access Profiles* window pops up.

2 To see which Access Groups are assigned to a user select a *User Name*.

Result:

The assigned Access Groups of the user selected are displayed.

3 Select `Edit`.

Result:

The *EMS - Edit User Access Profiles* window pops up.

4 Select the appropriate *Operation*.

5 If the operation *Modify* is chosen select a *User*.

6 If the operation *Add* is chosen type in a new user in the user field.

7 Change the *Role* when possible and necessary

8 Use the arrows to transfer *Access Groups* to and from the *Access Domain* field.

Result:

The new NEs will remain in the *Access Domain* field.

9 Select `OK` and `Close`.

Result:

The *EMS - User Access Edit* window will disappear.

10 Select `Close` in the *EMS - User Access Information* window to complete the procedure.

Result:

The *EMS- User Access Information* window will disappear.

END OF STEPS

□

Parameters for Assigning User Role and Access Domain

Introduction

The parameters in the User Access Profiles and Edit User Access Profiles window are described below.

Details

Information about User Name, User Role and Access Domain of the user selected. In the Access Domain window all Access Groups are displayed which are currently assigned to the user.

Operation

A group of three buttons used to set the mode of operation to:

- Add: adding a new user to the list of users with a Access domain and/or User Role.
- Modify: to alter and existing users Access Domain and/or User Role
- Delete: to remove a user from the list.

At default the modify mode will be selected.

Selection

A list of users and corresponding User Roles. One user is always selected unless the list is empty. User defined User Roles are identified with an asterisk.

User

Only when in the operation field add is selected, a new user its login name can be typed in this field.

Role

An option menu of all the available User Roles. Roles that are user defined are identified with an asterisk. Initially when a user is selected, the menu will display that user’s assigned User Role. Is no user is selected the selected User Role reverts to the default value of Operator.

Access Domain

A list of Access Groups assigned to the selected user. Several Access Groups can be selected at a time. By means of the right-pointing arrow the selected Access Groups are transferred to the “Available Access Groups list.

Available Access Groups

A list of Access Groups available to assign to the selected user. Access Groups that already been assigned will be removed form the list. Several Access Groups can be selected at a time. By means of the left-pointing arrow the selected Access Groups are transferred to the Access Domain list.

□

Section: Logging in as Root

Overview

Purpose For some actions it is necessary to log in as Root. During installation the user is asked to choose a Root password. This is needed during log in as root.

□

Log in as Root via the ITM-SC login window

When to perform

To log in as root when the user is asked to do so.

Before you begin

There are no prerequisites or precautions to be considered.

Related information

The related procedure is:

- Log in as Root via the UNIX terminal window

Procedure

1 Exit the ITM-SC application.

2 Wait until the *ITM-SC login* screen is displayed.

3 Type `root` in user name field.

4 Fill in the password chosen during installation.

Result:

You are now logged on.

END OF STEPS

□

Log in as Root via the UNIX terminal window

When to perform To log in as root when the user is asked to do so.

Before you begin There are no prerequisites or precautions to be considered.

Related information The related procedure is:

- Log in as Root via the ITM-SC login screen

Introduction to procedures Two procedures are provided to log in as root. The first is via the ITM-SC login screen. The second is performed via a Unix terminal window.

Procedure

1 Select the *Terminal Control* (the Lucent Technologies Logo). A Unix Terminal Window is displayed.

2 Type `su root` at the prompt.

3 Fill in the password chosen during installation.

Result:

You are now logged on.

END OF STEPS

□

Section: Changing Password

Overview

Purpose To increase the security of the ITM-SC and its network managed the user is able to change his/her own ITM-SC password.

□

Changing ITM-SC passwords

When to perform

To change the ITM-SC password of the user currently logged in.

Before you begin

Before performing this procedure consider the following precaution:

- ITM-SC user passwords, as they belong to the ITM-SC login name, can only be changed when the ITM-SC application is activated. Each ITM-SC user is enabled to change his/her own password. The ITM-SC administrator is able to delete the user account.

Related information

Related procedures are:

- Modifying ITM-SC User Information
- Configuring Password Ageing.
- Changing non-ITM-SC passwords

The related concept is:

- Security Management Overview [10-3]

Procedure

Follow the script below to change the ITM-SC password.

1 Open the *ITM-SC Management* menu and select the *Changing Password* icon.

Result:

A shell window is displayed asking the user for the current password.

2 Enter the *current password*. Press **ENTER**.

Result:

The user is asked to enter a new password.

3 Enter a *new password*. Press **ENTER**.

Result:

The user is asked to re-enter the new password.

4 Re-enter the *new password*. Press **ENTER**.

Result:

If the new password is accepted the following message will be displayed: Password has been updated successfully. The shell window will disappear automatically.

END OF STEPS

□

Changing non-ITM-SC passwords

When to perform

When changing non—ITM—SC passwords.

Before you begin

Before performing this procedure consider the following precaution:

- non-ITM-SC passwords can need a specific user level, make sure you have the right privileges.

Related information

Related procedures are:

- Changing ITM-SC passwords
- Modifying ITM-SC User Information
- Configuring Password Ageing.

The related concept is:

- Security Management Overview [10-3]

Procedure

1 Enter the command: `yppasswd <username>`

2 Log in as the user for which to change the password.

3 Follow instructions on screen.

4 To obtain help enter: `man yppasswd`

END OF STEPS

□

Section: Configuring Password Ageing

Overview

Purpose

To increase the security of the ITM-SC and so the network managed by the ITM-SC password ageing can be enabled. Use this procedure to configure password ageing.

□

Configuring Password Ageing

When to perform To implement password ageing or change password ageing settings.

Before you begin There are no prerequisites or precautions to be considered.

Related information Related procedures are:

- Modifying ITM-SC User Information
- Changing Password

The related concept is:

- Security Management Overview [10-3]

Parameters used in this procedure can be found at Parameters for Configuring Password Ageing [1-39].

Procedure Perform this procedure to enable a group or user for password ageing or change the password ageing properties:

1 Open the *ITM-SC Administration* menu and select the *Password Ageing* icon.

Result:

The *Password Ageing Administration* window is displayed.

2 Select the appropriate *User Class* or *User Name*. Multiple selections are possible

3 In the *Operation* field select *Enable* or *Disable*

4 Set the *Minimum number of weeks* and *Maximum number of weeks* by adjusting the slides.

5 Select `Apply`

Result:

The Status field will indicate the progress of the operation

6 Select `Cancel` in the *Password Ageing Administration* menu.

Result:

The *Password Ageing Administration* window disappears.

END OF STEPS

Parameters for Configuring Password Ageing

Introduction

Below the fields in the Password Ageing Administration and Password Ageing Update Confirmation windows are listed.

Operation

Indicates whether the selected User Class or user is enabled for Password Ageing or not.

Minimum number of weeks

After the specified minimum number of weeks are expired the user is asked to change his password

Maximum number of weeks

Before the specified Maximum number of weeks expire the user must change his password.

Buttons description

The following buttons are available on the Password Ageing Administration and Password Ageing Update Confirmation windows

Button	Description
Apply	Select to store current password ageing properties for the selected class or username
Cancel	Select to exit the screen

□

Section: Configuring Illegal Access

Overview

Purpose To increase the security of the ITM-SC a user entering its password wrong repeatedly this user can be banned from accessing the ITM-SC. □

Configuring Illegal Access

When to perform To enable the Illegal Access or to change the Illegal Access properties on the ITM-SC.

Before you begin There are no prerequisites or precautions to be considered.

Related information Related procedures are:

- Modifying ITM-SC User Information
- Deleting ITM-SC Users
- Changing Password
- Configuring Password Ageing

The related concept is:

- Security Management Overview [10-3]

Parameters used in this procedure can be found at Parameters for Configuring Illegal Access [1-42].

Procedure Follow these steps to enable of to change the properties of Illegal Access.

1 Select *Illegal Access* icon from the *ITM-SC Administration* menu.

Result:

The *Illegal Access Monitor* window is displayed.

2 To either *Enable* or *Disable* in the *Operation* field

3 If the *Operation* is set to *Enable* change the *Allowable number of invalid access attempts* if required

4 If the *Operation* is set to *Enable* change the *Monitor Sleep Time* if required.

5 Select `Apply`

Result:

The operation is carried out and the *Illegal Access Monitor* window disappears.

END OF STEPS

□

Parameters for Configuring Illegal Access

Introduction

The parameters as described below will impact the behavior of the Illegal Access feature.

Operation

The user can select to enable or disable Illegal Access.

Allowable No. of Invalid Access Attempts

Indicated the number of access attempts before access to the ITM-SC is denied at all. For example: when a user is failing to access the ITM-SC for 5 times the ITM-SC will be blocked for this user if the Allowable No. of Invalid Access Attempts had the value of 5.

Monitor Sleep Time

Indicates the sleep time which monitors the number of illegal access attempts which have occurred on a periodic basis.

□

Section: Displaying the CIT Access List

Overview

Purpose

Use this procedure to view NEs currently under management of a CIT.

□

Displaying the CIT Access List

When to perform

To display all NEs currently managed by a CIT as well to force a log out of the CIT connected to the NE.

Before you begin

There are no prerequisites or precautions to be considered.

Related information

The related procedure is

- Editing CIT Access

Related concepts are:

- Security Management Overview [10-3]
- CIT Access [10-9]

Parameters used in this procedure can be found at Parameters for Displaying the CIT Access List [1-45].

Procedure

Use this procedure to view the CIT access list and to force a connection termination.

1 Select *User Access -> CIT Access List*.

Result:

The *CIT Access List* window is displayed.

2 To print the data to a report select `Print`

3 To terminate a CIT connection to an NE select the appropriate NE and select `Force Logout`.

Result:

On the CIT a message will be displayed that the connection with the NE is lost.

4 Select `Close`.

Result:

The *CIT Access List* window disappears.

END OF STEPS

□

Parameters for Displaying the CIT Access List

Introduction

The parameters in the CIT Access List window are listed below.

NE name

Name of NE currently managed by a CIT

NE type

Type of NE to which the CIT is connected

CIT Role

Indicates the CIT (User) Role currently managing the NE by using the CIT. Available CIT User Roles are: View, Config and Admin.

Connection Type

Indicates whether the connection with the CIT to the NE is remote (via other NE) or local.

Lock-Out State

Indicates the access options. A

- Locked state will not allow a CIT to connect to the NE.
- No-Request and Not-Locked state allow a CIT to connect to the NE with or without password.

Access Start Time

The time at which the connection from the CIT to the NE was made. This is the time at the NE.

Sorting

In the CIT Access List, sorting can be performed by selecting the header on top of the columns. By default the list will also be sorted by the access start time. This is the secondary sort key.

Force Logout

Selecting on of more NEs and selecting the Force Logout button forces the CIT to terminate the connection to its managed NEs.

□

Section: Editing CIT Access

Overview

Purpose To change the properties of all CIT Roles for each Network Element.

Related procedure The related procedure is:

- Displaying the CIT Access List

□

Editing CIT Access

When to perform When changing the properties of all CIT Roles for each Network Element.

Before you begin There are no prerequisites or precautions to be considered.

Related information The related procedure is:

- Displaying the CIT Access List

Related concepts are:

- Security Management Overview [10-3]
- CIT Access [10-9]

Parameters used in this procedure can be found at Parameters for Editing CIT Access [1-49].

Procedure Use this procedure to set CIT Access Control.

1 Select *User Access -> CIT Access Control*.

Result:

The *EMS - CIT Access Control Information* window is displayed.

2 Select one or more *NEs* you wish to change regarding the CIT Access

3 Select `Edit`.

Result:

The *EMS - Edit CIT Access Control Information* window is displayed.

4 Change Lock-Out state to either:

- *Not Locked*: the CIT user can access the NE.
- *Locked*: the CIT user cannot access the NE
- *No Request*: no change in current state.

This can be set for each CIT user role.

5 Set clear or fill in both *password* and *confirm* password boxes.

Result:

If the password boxes remain empty the password is left unchanged. If clear is set no password is required.

6 Fill in the Inactivity Timer box or set the:

- *Disable box*: the connection will not be terminated due to a period of inactivity on the CIT to NE connection.
- *No Change box*: no change in current value

This can be set for each CIT user role.

7 Select `Apply` to confirm the settings. Select `Close`.

Result:

The *EMS - Edit CIT Access Information* window disappears.

8 Select `Close`.

Result:

The *EMS - CIT Access Information window* disappears.

END OF STEPS

□

Parameters for Editing CIT Access

Introduction The following parameters are present on the window being used.

NE name Name of NE to which the CIT is connected

NE type Type of NE to which the CIT is connected

CIT Role Indicates the CIT Role currently managing the NE by using the CIT. Available CIT user roles are: View, Config and Admin.

Lock-Out State Indicates whether the CIT user can connect to the NE. The

- `Locked` state indicates that no CIT can connect to the NE
- `Not-Locked` and `No-Request` state indicate the CIT can connect to the NE without password (clear is highlighted) or with (the password is entered).

This field is available for each CIT Role.

Inactivity Timer If there is no activity on the CIT to NE connection for this period, the CIT will be automatically disconnected by the NE. This field is available for each CIT Role.

CIT Logged In Indicates whether this NE currently has a CIT managing it.

Clear If the clear radio button is highlighted no password is necessary to connect to the NE via a CIT.

Password Field to enter a new password

Confirm Password Field for entering a new password once more to confirm the new password.

Sorting In the CIT Access List, sorting can be performed by selecting the header on top of the columns. By default the list will also be sorted by the access start time. This is the secondary sort key.

□

2 ITM-SC System Administration

Overview

Purpose

This chapter comprises typical administration tasks. These task need to be performed at least at initial startup of the ITM-SC and whenever needed during normal operation.

Intended Use

The topics in this chapter are not correlated like in other chapters. Therefore each section will provide enough information to perform the specific task successfully.

Contents

The following features are described:

- set the correct time (zone) and date on the ITM-SC.
- view and enter required license keys.
- defining printer and device names
- select the server that subsequent administration commands will be applied in a multiple server system.
- configure and activate the message of the day
- broadcast a shutdown message to all ITM-SC Clients
- configure the NE Timing.

On-line documentation available

The ITM-SC provides on line documentation of all guides on all ITM products. Short-cut: Help -> On Line Documentation.

Abbreviations used

When Network Elements OLS 80G, ADM 4/1, ADM 16/1, ADM16/1c, AM 1 (Plus) and TM 1 are described WaveStar®OLS 80 G, WaveStar®ADM 4/1, WaveStar® ADM 16/1, WaveStar® ADM16/1 compact, WaveStar® AM 1 (Plus) and WaveStar® TM 1 are meant.

□

Section: Setting System Time

Overview

Purpose All NEs managed by the ITM-SC and all connected workstations need to be synchronized. Synchronization is required for all systems in order to report the correct date and time for an event which will be reported to the ITM-SC. The local date and time are entered at the location where the ITM-SC resides and converted to (universal time coordinate) UTC internally. The screen is initialized with the current system time.

□

Setting System Time

When to perform

When changing the system time on the ITM-SC.

Before you begin

Before performing this procedure make sure that

- he ITM-SC application is stopped (shutdown).

Related information

There no related information available.

Procedure

Follow these steps to set the ITM-SC system time.

1 Select *System Administration* icon in the *ITM-SC Administration* menu.

Result:

The *ITM-SC System Control* window is displayed.

2 Select `Time`.

Result:

The *Set System Time* window is displayed.

3 Select the required *month/year* by using scroll button. (To step backward use the <<-button or forward use the >>-button)

4 Select the *Day* in the calendar field.

5 Select and fill in the *Hour, Minute and Second* field.

6 Select `OK`.

Result:

The Set System Time window closes.

7 Select `Exit` to complete the procedure.

Result:

The *ITM-SC System Control* window closes.

END OF STEPS

Validate system time

After Changing the system time log in as Root and shutdown the machine by typing: `shutdown -r -y` now to validate the change.

□

Section: Changing the Time Zone

Overview

Purpose When an ITM-SC has changed its physical location it can be necessary to change the time zone on the ITM-SC Client or ITM-SC Stand-alone. Perform this procedure to change the time zone on an ITM-SC Client or ITM-SC Stand-alone.

□

Changing the Time Zone

When to use Perform these steps to change the time zone on a ITM-SC Client:

Before you begin No prerequisites or precautions are needed when performing this procedure.

Related information No related information is available.

Procedure

1 Log in as root onto the ITM-SC and enter the following command:

```
set_parms timezone
```

Result:

A screen, displaying a list of locations, is displayed.

2 Choose the number corresponding to your required location and press **ENTER**.

Result:

A list of time zones is displayed.

3 Enter the number of the time zone you require and press **ENTER**.

Result:

A confirmation of the selection made will be asked.

4 Confirm the selection made.

Result:

The time zone on the ITM-SC Client is changed.

END OF STEPS

□

Section: Managing ITM-SC Licenses

Overview

Purpose

Use this procedures to view the available software licenses on the ITM-SC and to add a new license.

Licenses enable the ITM-SC with additional features, for example: maximum network elements allowed, network element performance monitoring, and geographic redundancy.

□

Viewing the ITM-SC Licenses

When to perform To display the capabilities of the ITM-SC.

Before you begin No prerequisites or precautions are needed when performing this procedure.

Related information The related concept is:

- License Key [10-11]

Procedure Follow these steps to view ITM-SC licences:

1 Select *Tools* -> *Licenses*.

Result:

The *EMS - License Information* window is displayed.

2 Select `Print` to download the license information into a report.

3 Select `Close`

Result:

The *EMS-License Information* window closes to complete the procedure.

END OF STEPS

□

Adding a ITM-SC license

When to perform

To display or add the capabilities of the ITM-SC.

Before you begin

Before starting this procedure make sure:

- a valid license key is available. This can be obtained via your Lucent Technologies service provider. To apply for a license key the Host ID of the ITM-SC is needed.
- ITM-SC application is shut down.

Related information

The related procedure is:

- Starting and Stopping the ITM-SC

The related concept is:

- License Key [10-11]

Important! If the License keys are not entered properly, the ITM-SC will NOT be accessible for the other users.

Procedure

Make sure you comply with the requirements as detailed in the overview of this section. If so, follow these steps to add a new license:

1 Select the *Licenses* icon from the *ITM-SC Administration* menu.

Result:

The *License Information* window is displayed, displaying the Host Id and the modules of the ITM-SC.

2 Select `Edit`.

Result:

The *ITM-SC License Edit* window is displayed.

3 Fill in the *New License Key*. Make sure that you enter the exact *License Key* for a module.

4 Select `OK`.

Result:

The *ITM-SC License Edit* window closes.

5 Select `Close` in the *License Information* window and restart the ITM-SC to activate the license.

END OF STEPS

□

Section: Defining Printer Names

Overview

Purpose Use this procedure to set ITM-SC printer names.

□

Defining Printer Names

When to perform To set or change the Printer properties.

Before you begin No prerequisites or precautions are needed when performing this procedure.

Related information No related information is available.

Procedure Follow these steps to set or change ITM-SC printer names.

1 Select *File* -> *Reports* -> *Properties*.

Result:

The *EMS - Report Properties Information* window is displayed.

2 Select `Edit`.

Result:

The *EMS - Edit Report Properties Information* window is displayed.

3 In the *Printer Name* field, enter the printer name.

4 Click `OK` to set the printer name.

Result:

The *EMS - Edit Report Properties Information* window disappears.

5 Select `Close` to complete the procedure.

END OF STEPS

□

Section: Changing Default Device Names

Overview

Purpose

Use this procedure to view and change default device names. Default names changed by the Administrator are set to be the report properties by default for ALL users.

□

Changing Default Device Names

When to perform To change the default device name settings.

Before you begin No prerequisites or precautions are needed when performing this procedure.

Related information No related information is available.

Procedure Follow these steps to change default device names:

1 Select *Tools -> Default Devices*.

Result:

The *EMS - Default Device Information* window is displayed.

2 Select `Edit`.

Result:

The *EMS - Edit Default Device Information* window is displayed.

3 Enter the *Device Name*. This should be *rmt/0m* for tape.

4 Enter the *Device Host Name* of the system to which the device is connected.

5 Enter the *Printer Name*. If the default printer has to be used then fill in NIL as the Printer Name.

6 Select `OK`.

Result:

The *EMS - Edit Default Device Information* window disappears.

7 Select `Close`.

Result:

The *EMS - Default Device Information* window closes to complete the procedure.

END OF STEPS

□

Section: Accessing Non-Default ITM-SC Servers

Overview

Purpose

In a multiple server system, the system administrator must select a server before performing administrative functions. All administrative actions other than user access apply only to the selected server.

This procedure describes how to select a server which is not the default server.

□

Accessing Non-Default ITM-SC Servers

When to perform

To change to another ITM-SC server to manage another set of NEs.

Before you begin

When changing to an other ITM-SC Server the functions which are affected are:

- System Administration
- Log File Administration
- Backup and Restore of the Databases
- Add Licenses
- Set Alarm Priorities

User Administration applies to the whole system and is therefore remains unaffected when switching to another ITM-SC server.

Related information

The related procedure is:

- Changing the Default ITM-SC Server

Procedure

Follow these steps to access a non-default ITM-SC server.

1 Select the *ITM-SC Management Module* from the Front Panel.

2 Select `Any ITM-SC NE Management`.

Result:

The *ITM-SC Address* window is displayed.

3 Enter the *name* or *IP Address* of the ITM-SC you wish to access. Select **ENTER**.

4 Confirm by typing *y*(es) followed by **ENTER** to complete the procedure.

END OF STEPS

□

Section: Changing the Default ITM-SC Server

Overview

Purpose To change the initial ITM-SC Server at start up use this procedure to change the default ITM-SC server. This procedure can be done via the ITM-SC Administration Module or via the ITM-SC Management Module both from the front Panel.

□

Changing the Default ITM-SC Server

When to perform To change the default ITM-SC server. The default ITM-SC server is entered directly when selecting NE Management out of Administration or Management Module.

Before you begin No prerequisites or precautions are neede when performing this procedure.

Related information The related procedure is:

- Accessing Non-Default ITM-SC Servers

Procedure Follow these steps to set a default ITM-SC:

1 Open the *ITM-SC Administration* Module.

2 Select `Set Default ITM-SC`.

Result:

A window with the question “

```
ITM-SC....
    is the current default server. Do you wish to change
       it
```

” is displayed.

3 Enter *Y*(es) or *N*(o).

Result:

If yes is selected the user is asked to enter the default ITM-SC server name.

4 Enter *ITM-SC Server* name. If no server is selected the current server’s name is used.

Result:

The entered server name is set up for administration commands.

5 Press **ENTER** to continue and complete the procedure.

Result:

The window is closed.

END OF STEPS

□

Section: Configuring Message of the Day

Overview

Purpose To inform users of the ITM-SC with a specific message at start up a Message of the Day can be configured.

□

Configuring Message of the Day

When to perform To configure/enable a daily message for users of the ITM-SC

Before you begin No prerequisites or precautions are needed when performing this procedure.

Related information Parameters used in this procedure can be found at Parameters for Configuring Message of the Day [2-22].

Procedure Perform this procedure to enable the Message of the Day or to change its properties:

1 Open the *ITM-SC Administration* menu and select the *Message of the Day* icon.

Result:

The *ITM-SC Message of the Day Administration* window is displayed.

2 In the *Operation* field select *Enable* or *Disable*

3 In the *Confirmation* field select *Enable* or *Disable*

4 If selected *Enable* in the confirmation window set the *Time-out* value

5 Enter a *message* by using the *Graphical Options*.

6 Select a *Test* if necessary.

Result:

The status field will indicate the result of the test.

7 Select `Apply` to activate the current settings

Result:

The Status field will indicate the progress of the operation

8 Propagate the current settings to another host by selecting first the *host* and then selecting *Update*.

Result:

The status field will indicate the result of the propagation operation.

9 Select `Cancel` to complete the procedure.

Result:

The *ITM-SC Message of the Day Administration* window disappears.

END OF STEPS

□

Parameters for Configuring Message of the Day

Introduction The fields needed to configure the Message of the Day are described below.

Operation Indicates whether the message will be displayed at login of the ITM-SC or not at all.

Confirmation Indicates whether the user has to confirm the Message of the Day before continue to work with the ITM-SC.

Time-out (seconds) When confirmation is disabled the Message of the Day will disappear after the indicated Time-out period.

Graphical options The user will be able to change the foreground color, background color and font type of the Message of the Day.

Message of the Day Area to enter the Message of the Day.

Test The user will be able to view to test and view the Message of the Day in line of graphical mode. The result of the test will be indicated in the result field.

Propagate After applying the current settings the user is able to forward the Message of the day setting to another host. The result of the propagation will be indicated in the result field.

Buttons description The following buttons are available on the Message of the Day Administration window

Button	Description
Line	Select to display the line test.
Graphical	Select to display the graphical test
Update	Select to propagate the current settings to another host.
Apply	Select to store and activate current Message of the Day Administration
Cancel	Select to exit the screen without changes

□

Section: Managing Shutdown Broadcast

Overview

Purpose Perform one of the procedures provided to disable or enable the broadcast message sent to all connected ITM-SC Clients on shutdown.

□

Enabling Shutdown Broadcast

When to perform

When changing the properties of the shutdown broadcast message.

Before you begin

No prerequisites or precautions are needed when performing these procedures.

Related information

No related information is available.

Procedure

1 Log in as *i2kadmin* on the ITM-SC Server and enter:

```
$EMSAPPLDIR/bin/ems_param -i
```

Result:

This script invokes a menu driven tool which allows certain configurable parameters to be maintained.

2 Choose the number next to the *enable_shutdown_broadcast* parameter and press **ENTER**. If the parameter is not in the list press **ENTER**to go to the next page until the parameter is shown.

Result:

The following information is displayed:

```
Name : enable_shutdown_broadcast Enable
shutdown broadcast message. If TRUE, then
display a dialog on all connected clients
when the ITM-SC is shutdown.

Type : BOOLEAN

Range : TRUE or FALSE

Default : FALSE

Value : FALSE
```

3 Enter `TRUE` and select **ENTER**. Also `true`, `True`, `t` or **T**are allowed.

Result:

The following confirmation message is displayed: `Changed value of enable_shutdown_broadcast to TRUE Press <Enter> to continue..`

4 Press **ENTER**to continue

Result:

The opening menu will be displayed

5 Press q and **ENTER**to quit the script

END OF STEPS

□

Disabling Shutdown Broadcast

When to use When changing the properties of the shutdown broadcast message.

Before you begin No prerequisites or precautions are needed when performing these procedures.

Related information No related information is available.

Procedure

1 Log in as *i2kadmin* on the ITM-SC Server and enter:

```
$EMSAPPLDIR/bin/ems_param -i
```

Result:

This script invokes a menu driven tool which allows certain configurable parameters to be maintained.

2 Choose the number next to the *enable_shutdown_broadcast* parameter and press **ENTER**. If the parameter is not in the list press **ENTER**to go to the next page until the parameter is shown.

Result:

The following information is displayed:

```
Name : enable_shutdown_broadcast Enable
shutdown broadcast message. If TRUE, then
display a dialog on all connected clients
when the ITM-SC is shutdown.

Type : BOOLEAN

Range : TRUE or FALSE

Default : FALSE

Value : FALSE
```

3 Enter `FALSE` and select **ENTER**. Also `false`, `False`, `f` or **F**are allowed.

Result:

The following confirmation message is displayed:

```
Changed
value of enable_shutdown_broadcast to False
Press <Enter> to continue..
```

4 Press **ENTER**to continue

Result:

The opening menu will be displayed

5 Press q and **ENTER**to quit the script

END OF STEPS

□

Section: Managing NE Timing

Overview

Purpose

The procedures described in this section take care of the synchronization between the NEs and the ITM-SC. The NE time will be set to the ITM-SC time as close as possible. This is needed to prevent the corruption of Performance Monitoring data and to support the TCM feature.

□

Setting NE Time Synchronization Properties

When to perform

When changing the properties of automated synchronization between NE and ITM-SC.

Before you begin

No prerequisites or precautions are needed when performing these procedure.

Related information

The related concept is:

- NE Timing [10-12]

Parameters used in this procedure can be found at Parameters for Managing NE Timing [2-32].

Procedure

1 Select *Management —> NE Time Synchronization —> NE Time Synchronization*.

Result:

The *EMS — Time Synchronization* window is displaying the current properties.

2 Select `Edit` when changing the properties.

Result:

The *EMS — NE Time Synchronization* window is displayed.

3 Change the values and select `OK` to save them, otherwise select `Close` to exit without change.

Result:

The *EMS — NE Time Synchronization* window disappears.

4 Select `Close` to finish the procedure.

Result:

The *EMS — Time Synchronization* window disappears.

END OF STEPS

□

Viewing NE Time Synchronization Details per NE

When to perform

When checking the NE Time properties of an specific NE in respect to the ITM-SC timing.

Before you begin

No prerequisites or precautions are needed when performing these procedure.

Related information

The related concept is:

- NE Timing [10-12]

Parameters used in this procedure can be found at Parameters for Managing NE Timing [2-32].

Procedure

1 Select *Management —> NE Time Synchronization —> NE Time Synchronization- NE Details*.

Result:

The *EMS — NE Time Synchronization — NE Details* window is displayed.

2 Select the `Selection Dialog` button to select an NE.

Result:

The NE Selection Dialog window is listing all available NEs.

3 Select an NE and select `OK`.

Result:

The *EMS — NE Time Synchronization* window is updated with NE Name and NE Type information, together with the NE Timing characteristics of the NE at the time the Time synchronization was last run.

4 Select `Restart recording minimum round trip time` to update the values. Take some time to finish the operation.

Result:

All records of the minimum round trip time are removed before updated values are displayed.

5 Select `Close` to finish the procedure.

Result:

The *EMS — NE Time Synchronization — NE Details* window disappears.

END OF STEPS

□

Parameters for Managing NE Timing

Introduction

The fields needed to manage NE Timing are described below.

Time drift

Indicates the time difference between the NE time and the ITM-SC time

Round trip time

Indicates the time between a message send by the ITM-SC and receiving it back from the NE.

If the time drift is bigger than the value indicated by the Time Drift Allowed parameter then the NE clock will be set to the ITM-SC time.

Time drift allowed

Indicates the time drift allowed in an NE. If this value is exceeded the NE will be synchronized.

Time of day to start NE synchronization

Indicates the time at which the sequential synchronization of NEs begins, given as the local time for the ITM-SC client.

It is to be advised to select a time when the amount of management network traffic is at its lowest point.

The default time is 03:10, local time of the server.

Maximum variation allowed in message round trip times

Indicates the maximum variation allowed for a round trip to take.

If this value is exceeded an alarm will be generated to inform the user the NE could not be synchronized to the ITM-SC.

The default value is 1 second.

Number of queries sent to the NE

Indicates the number of time the ITM-SC sends a message requesting the NE time to each NE.

The default value is 3.

Offset added to minimum round trip times

The time added to the NEs minimum round trip time to determine the maximum allowed round trip time for the NE.

If the mean round trip time is bigger than this threshold value an alarm will be generated to inform the user the NE could not be synchronized to the ITM-SC.

The default value is 1 second.

Maximum time drift

The maximum time drift above which the NE time will be set without checking the maximum value and difference in round trip message time.

If the time drift exceeds this value then the NE clock is set without checking the message round times. This than occur when the NE is managed by the ITM-SC for the first time or when the time of the ITM-SC has changed.

The default value is 5 minutes.

Status Indicates the current synchronization status for the NE. Possible values are:

- Normal
- Excessive network load
- Network unstable
- Time drift still excessive

□

Lucent Technologies
Bell Labs Innovations

3 Provisioning Environment Setup

Overview

Purpose

This chapter describes how to prepare the ITM-SC environment for provisioning operators.

Contents

Subjects described in this chapter are:

- managing MEC files
- managing Card types

Abbreviations used

When Network Elements OLS 80G, ADM 4/1, ADM 16/1, ADM16/1c, AM 1 (Plus) and TM 1 are described WaveStar®OLS 80 G, WaveStar®ADM 4/1, WaveStar® ADM 16/1, WaveStar® ADM16/1 compact, WaveStar® AM 1 (Plus) and WaveStar® TM 1 are meant.

□

Section: Managing MEC Files

Overview

Purpose

An MEC file (Manufacturers Executable Code file) is operational software that is downloaded to the network element from the ITM-SC. Use this procedure to load or delete the MEC files on/from the ITM-SC.

□

Load MEC Files

When to use

When needing to provide the ITM-SC with the necessary software for upgrading NEs via the ITM-SC.

Before you begin

Before performing this procedure make sure:

- the device name and device host name are defined. This can be done via the menu *Tools* -> *Default Devices*.

Before performing this procedure consider the following:

- MEC file download is only applicable to ISM, SLM, PHASE, ADM 16/1, ADM 16/1 compact, OLS80G, AM-1 and TM-1 NEs.

Related information

The related procedure is:

- Delete MEC Files

The related concept is:

- MEC File Concepts [10-16]

Procedure

Follow these steps to load MEC files:

1 Select *Tools* -> *MEC Files*.

Result:

The *EMS - MEC File Information* window is displayed.

2 Select the appropriate *NE type*.

Result:

When selecting an entry for a PHASE NE this causes the list *Component files in software load* to be populated. A list of MEC files stored on the system are displayed in the *List of loaded files* window. Software files not available are greyed out.

3 Select `Edit`.

Result:

The *EMS - Edit MEC File Information* window is displayed.

4 Insert the MEC files tape/disc into the tape/disc drive, and select `Apply`.

5 Select `Search` from the operation menu. Select `Apply`.

Result:

A list of MEC files on the tape/disc is displayed in the *List of files on device* box.

6 Select `Load` from the operation menu.

7 Select the *file* to be loaded from this list.

8 Select `Apply`.

Result:

The MEC file is loaded into the ITM-SC and its name appears in the *List of loaded files* box.

9 Select `Close` (if you do not want to load another file).

Result:

The *EMS - Edit MEC File Information* window closes to complete the procedure.

END OF STEPS

□

Delete MEC Files

When to use

Whenever MEC files are not used anymore it is advised to remove them from the ITM-SC to free disk space.

Before you begin

Before performing this procedure consider the following:

- MEC file deletion is only applicable to ISM, SLM, PHASE, ADM 16/1, ADM 16/1 compact, OLS80G, AM-1 and TM-1 NEs.

Related information

The related procedure is:

- Load MEC Files

The related concept is:

- MEC File Concepts [10-16]

Procedure

Follow these steps to delete a loaded MEC file from the ITM-SC:

1 Select *Tools* -> *MEC Files*.

Result:

The *EMS - MEC File Information* window is displayed.

2 Select the appropriate *NE type*.

Result:

When selecting an entry for a Phase NE this causes the list *Component files in software load* to be populated. A list of MEC files stored on the system are displayed in the *List of loaded files* window. Software files not available are greyed out.

3 Select `Edit`.

Result:

The *EMS - Edit MEC File Information* window is displayed

4 Select `Delete` from the operation menu.

5 Select the MEC file to delete from the *List of loaded files* field.

6 Select `Apply`.

Result:

The selected MEC file is deleted from the list of *Loaded Files*.

7 If finished deleting select `Close`

Result:

The *EMS - Edit MEC File Information* window closes to complete the procedure.

8 Select `Close` to exit the *EMS - MEC File Information* window

END OF STEPS

□

Section: Managing Card Types

Overview

Purpose

The Card Type Inventory is a list that contains all possible Unit Types that can be used for the network shelf composition. It is possible to add card types having the same functionality as factory defined card types. These added card can be modified and deleted. Factory defined card types cannot be modified or deleted.

□

Listing Card Type Inventory

When to use To add a card which is having a different name than the factory defined cards but does have the same functionality.

Before you begin No prerequisites or precautions need to be considered when performing this procedure.

Related information Related procedures are:

- Adding a Card Type
- Modifying an Added Card Type
- Deleting an added Card Type

Procedure Follow these steps to list card types:

1 Select *Cards* -> *Inventory*.

Result:

The *EMS - Card Type Inventory* window is displayed, showing all factory defined card as well as customer added cards.

2 Select `Close`.

Result:

The *EMS - Card Type Inventory* window disappears.

END OF STEPS

□

Adding a Card Type

When to use To create an Added Card (a so-called user defined card).

Before you begin No prerequisites or precautions need to be considered when performing this procedure.

Related information Related procedures are:

- Listing Card Type Inventory
- Modifying an Added Card Type
- Deleting an added Card Type

Procedure Follow these steps to add a card type:

1 Select *Cards* -> *Inventory*.

Result:

The *EMS - Card Type Inventory* window is displayed.

2 Select `Edit`.

Result:

The *EMS - Edit Card Type Inventory* window is displayed.

3 Set the *Operation* mode to *Add*.

4 Select the *Physical Unit Type* from the list of *Factory Defined Cards*.

5 Fill in the *Physical Unit Type*.

6 Fill in the *Unit Item Code*.

7 Select the *Physical Unit Type* from the list of *Added Cards*. Select `Apply`.

Result:

The requested action is performed.

8 Select `Close`, to close the *EMS - Edit Card Type Inventory* window.

9 Select `Close` from the EMS - Card Type Inventory window.

Result:

The *EMS - Card Type Inventory* window closes to complete the procedure.

END OF STEPS

□

Modifying an Added Card Type

When to use To change the properties of an Added Card.

Before you begin No prerequisites or precautions need to be considered when performing this procedure.

Related information Related procedures are:

- Listing Card Type Inventory
- Adding a Card Type
- Deleting an added Card Type

Procedure Follow these steps to change a card type:

1 Select *Cards* -> *Inventory*.

Result:

The *EMS* - *Card Type Inventory* window is displayed.

2 Select `Edit`.

Result:

The *EMS* - *Edit Card Type Inventory* window is displayed.

3 Set the *Operation* mode to *Modify*.

4 Select the appropriate card from the list of *Added Cards*.

5 Modify the *Physical Unit Type*.

6 Modify the *Unit Item Code*.

7 Select `Apply` to apply the changes to the unit.

8 Select `Close`.

Result:

The EMS - Edit Card Type Inventory window closes.

9 Select `Close` from the *EMS - Card Type Inventory* window to close the window and complete the procedure.

END OF STEPS

□

Deleting and added Card Type

When to use

To remove Added Cards types.

Before you begin

Before performing consider the following precaution:

- do *not* delete factory defined cards as they are needed to create new card types.

Related information

Related procedures are:

- Listing Card Type Inventory
- Adding a Card Type
- Modifying an Added Card Type

Parameters used in this procedure can be found at Parameters for Managing Card Types [3-15]

Procedure

Follow these steps to delete a added card type:

1 Select *Cards* -> *Inventory*.

Result:

The *EMS - Card Type Inventory* window is displayed.

2 Select `Edit`.

Result:

The *EMS - Edit Card Type Inventory* window is displayed.

3 Set the *Operation* mode to *Delete*.

4 Select the appropriate card from the *List of Added Cards*.

5 Select `Apply`.

Result:

The card type is deleted.

6 Select `Close`.

Result:

The *EMS - Edit Card Type Inventory* window closes.

7 Select `Close` from the *EMS - Card Type Inventory* window to complete the procedure.

END OF STEPS

□

Parameters for Managing Card Types

Purpose

The parameters below are used when managing card types.

12NC/Item Code

The 12NC number, displayed when selected a ISM, SLM, RR, PHASE, ADM155c or ADM4/1 NE, is a numeric string of 11 digits.

If the NE Type is ADM16/1, ADM16/1 compact, OLS 80G, TM1, AM1, AM1 Plus or WDACS, this field will be replaced with *Item Code*, a alphanumeric string up to 9 characters.

Equiv. 12NC/Item Code

User description of the 12 NC/Item Code of the unit selected. The Equiv. 12NC number will be displayed when a ISM, SLM, RR, PHASE, ADM155c or ADM4/1 NE is selected.

If the NE Type is ADM16/1, ADM16/1 compact, OLS 80G, TM1, AM1, AM1 Plus or WDACS, this field will be replaced with *Equiv. Item Code*.

Unit 12NC

The Unit 12NC number is a numeric string of 11 digits.

Physical Unit Type

Description of the card selected

Equiv. Unit Type

User description of the Physical Unit Type selected.

Slot state/Unit state

Slot State is displayed as column header for all NEs except WDACS for which *Unit State* is displayed.

If the state is not applicable a “-” is displayed. The state is always *Assigned* for ADM155 / ADM4/1 and TM 1/AM 1 Baseboards.

Protection Function

Indicates either *Worker, Protecting* or “-”.

Hardware Actual 12NC/Item Code

Indicates the hardware 12 NC of the physical Unit

Serial Number

Will display the serial number of the unit. Applicable to OLS80G NEs only.

Interchange Marker (SSN)

Displays the interchangeability marker (series number). Applicable to OLS80G NEs only.

CLEI

Displays the Common Language Equipment Identifier. Applicable to OLS80G NEs only.

ECI

Displays the Equipment Catalog Item. Applicable to OLS80G NEs only.

Software Version Displays the software version. If not applicable, a “-” is displayed. Applicable to OLS80G NEs only.

Total Unit Type Count Displays the Total Unit Type Count for the selected unit.

□

Lucent Technologies
Bell Labs Innovations

4 Maintenance Environment Setup

Overview

Purpose

This chapter describes how to set up the ITM-SC environment for maintenance operators. Maintenance operators will be using the ITM-SC for fault localization and trouble solving. Therefore the maintenance environment should be in line with the maintenance philosophy agreed upon.

Maintenance philosophy

Implementing a consistent alarm/event behavior through all NEs and management components will decrease failure respond time. Therefore it is of high importance to implement the company’s maintenance philosophy.

Contents

Subjects described in this chapter are:

- configuring System Alarm Monitoring
- enabling Double Alarm Acknowledgement
- enabling Alarm Beeping
- changing Alarm Severity Color
- controlling EMS Alarms
- configuring All NE alarm control
- managing archives (ITM-SC, Event & Performance Monitoring)

Abbreviations used

When Network Elements OLS 80G, ADM 4/1, ADM 16/1, ADM16/1c, AM 1 (Plus) and TM 1 are described WaveStar®OLS 80 G, WaveStar®ADM 4/1, WaveStar® ADM 16/1, WaveStar® ADM16/1 compact, WaveStar® AM 1 (Plus) and WaveStar® TM 1 are meant.

□

Section: Configuring Systems Alarm Monitoring

Overview

Purpose To align the presentation of alarms (also called events) on the ITM-SC with the maintenance philosophy the system alarm monitor settings can be changed. These settings comprise the External Alarm Presentation (EAP), Fault Summary and Cyclic Check.

□

Configuring Systems Alarm Monitoring

When to use To change the System Alarm Monitoring settings.

Before you begin No prerequisites or precautions need to be considered when performin this procedure.

Related information The related concept is:

- Systems Alarm Monitoring Overview [10-18]

Parameters used in this procedure can be found at Parameters for Configuring Systems Alarm Monitoring [4-5].

Procedure Follow these steps to configure systems alarm monitoring:

1 Select *`Alarm Monitor Configure`* from the *Administration module*.

Result:

The *Systems Alarm Monitoring Information* window is displayed.

2 Select *`Edit`* .

Result:

The *Edit Systems Alarm Monitoring Information* window is displayed.

3 Select an *`operation`* .

Result:

Depending on the operation you select, some options will be greyed out on the window.

4 To add/remove ITM-SCs to/from the total list of monitored ITM-SC the *`Operation`* must be set to *`ITM-SC Host List`* .

5 To enable/disable the total monitor control choose monitoring *`On`* or *`Off`* .

6 When the Monitoring is *`On`* it is possible to include the *`Autonomous Events`* and events with a specific *`Severity`* .

Result:

When the *operation* is set to *External Alarm Presentation* (EAP) the following fields are highlighted: *Enable/disable list, Script Run Hold Off, Hold Off after Suppression, Screenlock Lapse* and *Beep on* .

7 When the *operation* is set to *Fault Summary* select *Yes* or *No* if you want to enable or disable the beep indicating the appearance of the Fault Summary Panel.

8 To enable/disable the feature selected in the *Operation box* the ITM-SC must be put in the right box in the *Feature Control* screen. Move the ITM-SC in the right box by first selecting first the appropriate *ITM-SCs* and than selecting the *arrow* .

9 Select *Apply* to apply the changes you have made.

10 When Systems Alarm Monitoring has not been active yet select *Alarm Monitor* in the *Provisioning and Maintenance* module to active Systems Alarm Monitoring.

Result:

The *Fault Summary Panel* will be displayed directly. The *EAP* window will only be displayed when a new alarm arrives.

END OF STEPS

□

Parameters for Configuring Systems Alarm Monitoring

Introduction

The parameters below are used to change the settings of the System Alarm Monitoring.

ITM-SC Host List

List host names of all ITM-SCs which can be monitored. Selecting the radio button will highlight the ITM-SC host list field.

Monitor Control

Enables or disables monitoring of all features for all ITM-SC on this workstation. Selecting the radio button will highlight the Monitor Control field.

External Alarm Presentation

Edit settings for the external alarm presentation. Selecting the radio button will highlight the External Alarm Presentation field and Feature Control field.

Fault Summary

Edits settings for the fault summary. Selecting the radio button will highlight the Fault Summary Field.

Host Name to be removed

Selecting the dialog button displays a list of ITM-SCs which can be monitored. Selecting an ITM-SC hostname out of this list and select OK will pass the hostname to the Edit screen for removal.

Host Name to be added

Enter the hostname of the ITM-SC to add.

Monitoring

Used to disable (off) or enable (on) monitoring control of all ITM-SC’s

Alarm Severities

Used to limit the amount of alarms by selecting:

- *Information*: showing information, deferred and prompt alarms
- *Deferred*: showing deferred and prompt alarms
- *Prompt*: showing only prompt alarms

Polling Interval

Sets the refresh time for the alarm monitor features. It indicates the time between each check for alarms on the monitored servers. Allowable range is between 1 and 15 minutes with a default of 5 minutes.

Include Autonomous Events

Indicates if also Autonomous Events are reported to the External Alarm Presentation. Instantaneous Alarms will be reported at default.

Enable Lists the ITM-SCs to which changes to the feature selected in the operation box have to be applied. Add an ITM-SC from the list by using the left arrow button (◀).

Disable Lists the ITM-SCs to which to selected feature or changes is not applicable.

Remove a ITM-SC from the list by using the right arrow button (▶).

Script Run Hold-Off Indicates the time between initial detection of an alarm and activation of the Alarm Raised script. This script can be found in the directory /etc/opt/itm/sc.

Valid entries are 0 - 999 minutes.

Hold Off after Suppression Indicates the time between a user has suppressed an alarm and next alarms will be notified to the workstation, displaying the EAP Suppression window once more. This value is not applicable to other workstations.

Valid entries are 0 - 999 minutes.

Screenlock Lapse If yes is selected the workstation will resume detecting alarms at screenlock activation even when the Suppress Hold Off period is not finished yet.

Fault Summary Field Within this field only the only the Beep feature can be adjusted. When no is selected, the acoustic signal is disabled.

□

Section: Configuring ITM-SC for Double Alarm Acknowledgment

Overview

Purpose Perform this procedure to configure the ITM-SC for Double Alarm Acknowledgment.

□

Configuring ITM-SC for Double Alarm Acknowledgment

When to use

When double alarm acknowledgment is to be implemented as part of the maintenance philosophy.

Before you begin

Before performing this procedure make sure

- latching is set for each alarm.To set latching perform the Setting Alarm Latching procedure as can be found in the *Sub-network controller Maintenance Guide* (SMG).

Before performing this procedure consider the following:

- Disabling the double alarm acknowledge feature is not supported.
- The double alarm acknowledgement will not work untill the ITM—SC it licensed to do so.

Related information

Related procedures are:

- Configuring ITM-SC for Alarm Beeping
- Configuring Systems Alarm Monitoring

The related concept is:

- Double Alarm Acknowledgment Concepts [10-19]

Procedure

1 Log in as *i2kadmin* on the ITM-SC and enter:

```
$EMSAPPLDIR/bin/ems_param -i
```

Result:

A menu driven tool is displayed. This tool will allow certain configurable parameters to be maintained.

2 Choose the number next to the *double_alarm_acknowledge* parameter and press **ENTER**. If the parameter is not in the list press **ENTER**to go to the next page until the parameter is shown.

Result:

The following information is displayed:

```
Name: double_alarm_acknowledge Should alarms
be double-acknowledged?

Type: BOOLEAN

Range: TRUE or FALSE

Default: FALSE
```

```
Value: FALSE
```

3 Enter `TRUE` and select **ENTER**. Also `true`, `True`, `t` or **T**are allowed.

Result:

The following confirmation message is displayed: `Changed value of double_alarm_acknowledge to TRUE Press <Enter> to continue..`

4 Press **ENTER**to continue.

Result:

The opening menu appears again.

5 Enter `q` and press **ENTER**to quit the script.

6 To enable the Double Alarm Acknowledgment feature license the ITM-SC for Double Alarm Acknowledgment. Refer to the *Subnetwork controller Administration Guide* (SAG) for the appropriate procedure.

END OF STEPS

□

Section: Enable ITM-SC for Alarm Beeping

Overview

Purpose Perform this procedure to enable the ITM-SC to use the alarm beeping feature. This alarm beeping feature is part of the ITM-SC's External Alarm presentation as described in the section *Configuring Systems Alarm Monitoring*.

□

Configuring ITM-SC for Alarm Beeping

When to use

When implementing the alarm beeping functionality as part of the maintenance philosophy.

Before you begin

Before performing this procedure make sure:

- That this procedure can only be performed at installation time.

Related information

Related procedures are:

- Configuring ITM-SC for Double Alarm Acknowledgment
- Configuring Systems Alarm Monitoring

Procedure

Follow these steps to enable the alarm beeping feature as comprised in the System External Alarm presentation.

1 Open a terminal screen and log in as *i2kadmin* on the ITM-SC.

2 Enter the following command:

```
$EMSAPPLDIR/bin/ems_param -i
```

Result:

A menu driven tool is displayed. This tool will allow certain configurable parameters to be maintained.

3 Choose the number next to the *alarm_beep_enabled* parameter and press **ENTER**. If the parameter is not in the list press **ENTER**to go to the next page until the parameter is shown.

Result:

The following information should be displayed:

```
Name : alarm_beep_enabled Should the alarm
beep feature be enabled ? i.e. should the
ITM-SC beep if there are any unacknowledged
alarms.

Type : BOOLEAN

Range: TRUE or FALSE

Default: FALSE

Value: FALSE
```

4 Enter `TRUE` and select **ENTER**. Also `true`, `True`, `t` or `T` are allowed.

Result:

The following confirmation message is displayed: `Changed value of alarm_beep_enabled to TRUE Press <Enter> to continue...`

5 Select **ENTER**to continue.

Result:

The opening menu will be displayed again.

6 If the alarm beep interval does not have to be changed press `q` and select **ENTER**to quit the script.

7 To change the alarm beep interval choose the number next to the parameter alarm_beep_interval and press **ENTER**. If you don't want to change the alarm beep interval proceed to Step 10.

Result:

The following information is displayed:

```
Name : alarm_beep_interval The interval
between alarm beeps (milliseconds).

Type : INTEGER

Range : 500 - 86400000

Default : 500

Value : 500
```

8 Enter the required value (in milliseconds) and press **ENTER**.

Result:

A confirmation message is displayed.

9 Press **ENTER**to continue.

Result:

The opening menu will be displayed again.

10 Press q and select **ENTER**to quit the script and complete the procedure.

END OF STEPS

□

Section: Setting EMS Event Parameters

Overview

Purpose Use this procedure to customize EMS Event parameters for each EMS Event which the ITM-SC can generate.

□

Setting EMS Event Parameters

When to use

To change the severities and report state of EMS related alarms.

Before you begin

Before perfoming this procedure consider the following precautions:

- Setting EMS Event Parameters can only be done for ITM-SC administrators or users with administration privileges.
- To prevent an event from being misinterpreted, setting the event parameters should always be in accordance with the maintenance philosophy.
- Changes to event severity information do not affect alarms currently raised on the ITM-SC, only new events will use the new severity and report status.

Related information

Related procedures are:

- Setting NE Event Parameters (ITM-SC Maintenance Guide (SMG))
- Setting NE Event Control Information (SMG)
- Setting SLM Regenerator Alarm Information (SMG)
- Setting WDACS Station Alarm Control (SMG)
- Setting Alarm Parameters for Existing Resources (SMG)
- Setting All NE Event Control (ITM-SC Administration Guide (SAG))
- Setting Manager Event Parameters (SMG)
- Setting EMS Event Control (SAG)

Related concepts are:

- Events [10-20]
- Event Characteristics [10-23]

Parameters used in this procedure can be found at Parameters for Setting EMS Event Parameters [4-17].

Procedure

Follow these steps to set the EMS Level Manager events severities and report state:

1 Select Event -> Event Parameter -> EMS from the top level menu.

Result:

The EMS - EMS Event Parameters window is displayed.

2 With the Factory Defaults button events can be set at once to the factory defaults.

Result:

A confirmation window will be displayed.

3 To set the severity per event, select an event from the list and select Edit.

Result:

The EMS - Edit EMS Event Parameters window for the selected alarm is displayed.

4 Set the Severity and the *Report* fields to the desired options.

5 Select OK in the EMS - Edit EMS Parameters window to confirm your selections.

Result:

The window closes and the EMS - EMS Event Parameters window is updated.

6 Select Close in the EMS - EMS Event Parameters window to close the window and complete the procedure.

END OF STEPS

□

Parameters for Setting EMS Event Parameters

Introduction

The fields used to change the EMS Level Manager Event parameters are described below.

Definition: EMS Event

To change the severities and report state of EMS related alarms.

Description

The description of the cause of the alarm.

Severity

Indicates the current severity of this alarm. This can be *Prompt, Deferred*, *Information* or *No Change.*

Report

Either Reported or Not Reported.

- *Reported* alarms are raised and reported on ITM-SC.
- *Not Reported*alarms are not displayed on the ITM-SC, and you will be unaware when an unreported alarm occurs.

□

Section: Setting EMS Event Control

Overview

Purpose Use this procedure to set latching on EMS Events and to control storage of all events.

□

Setting EMS Event Control

When to use To change the characteristics of the EMS Events as well as to control the event storage.

Before you begin No prerequisites or precaution need to be considered when performing this procedure.

Related information Related procedures are:

- Setting NE Event Parameters (ITM-SC Maintenance Guide (SMG))
- Setting NE Event Control Information (SMG)
- Setting SLM Regenerator Alarm Information (SMG)
- Setting WDACS Station Alarm Control (SMG)
- Setting Alarm Parameters for Existing Resources (SMG)
- Setting All NE Event Control (ITM-SC Administration Guide (SAG))
- Setting Manager Event Parameters (SMG)
- Setting EMS Event Parameters (SAG)

Related concepts are:

- Events [10-20]
- Event Characteristics [10-23]

Parameters used in this procedure can be found at Parameters for Setting EMS Event Control [4-21].

Procedure Follow these steps to set latching and to control the storage of EMS events:

1 Select Events -> EMS Event Control from the top level menu.

Result:

The EMS - NE Event Control Information window is displayed with the current settings.

2 Select Edit to change the settings. This button is only available for the “Supervisor”.

Result:

The EMS - Edit EMS Event Control Information window is displayed.

3 Change settings to customize EMS Event Control.

Result:

When enabling any of the options the number of events or hours is required.

4 Select OK to impose the new settings.

5 Select Close.

Result:

The EMS - Edit EMS Event Control Information window disappears.

6 Select Close.

Result:

The EMS - EMS Event Control Information window disappears.

END OF STEPS

□

Parameters for Setting EMS Event Control

Introduction

The parameters, described below, indicate the latching state and the event storage thresholds for all events.

Definition EMS Events

EMS events are those which report problems with the management system (ITM-SC) and so are not associated to any specific NE.

EMS Alarm Latching

When events are latched, all events must be both cleared and acknowledged before they are moved to the history list. When events are not latched, the events are moved to the history list when a fault is cleared. The options are Disabled or Enabled.

Current Event List Absolute Limit

The maximum number of events that can be stored in the current event list. The options are Disabled or Enabled. When enabled the minimum value is *25*, the maximum value is *99,999* and the default value is *10,000*.

Current Event List Warning Threshold

The number of events that can be stored in the current list before a management event warns you that the event list is nearing capacity. This event will only be cleared once the number of events has fallen to 75% of this threshold. The options are Disabled or Enabled. When enabled the minimum value is *25*, the maximum value is *99,999* and the default value is *8,000*.

History Alarm List Absolute Limit

The maximum number of events that can be stored in the history list. The options are Disabled or Enabled. When enabled the minimum value is *25*, the maximum value *80,000* and the default value is *20,000*.

History Alarm List Warning Threshold

The number of events that can be stored in the history list before a alarm notifies the user the event list is nearing capacity. This alarm can be cleared only when the number of events has fallen to 75% of this threshold. The options are Disabled or Enabled. When enabled the minimum value is *25*, the maximum value is *80,000* and the default value is *16,000*.

History Alarm List Deletion Time

The time (in hours) before events are automatically deleted from the history list. The options are Disabled or Enabled. When enabled the default value is *240*

□

Section: Setting All NE Event Control

Overview

Purpose Use this procedure to enable alarm latching and/or NE Alarm History Recovery for several or all NEs. Latching helps to ensure that alarms for network elements cannot be moved to the History Alarm List without being acknowledged. The user can set the latching status per Network Element or for all Network Elements at once. When the latter is selected the NE Alarm Control Information window will be displayed. When an ITM-SC has lost its association with an NE the events cannot be forwarded to the ITM-SC. Some NEs can hold their own event information. On recovery of association the ITM-SC downloads the event information to update its own alarm database. The NE can be enabled/disabled for this alarm recovery.

□

Setting All NE Event Control

When to use

To change latching and/or NE Alarm History Recovery settings for NEs.

Before you begin

Before performing this procedure consider the following:

- Alarm History Recovery is only available for ADM155 and ADM 4/1 NEs.

Related information

Related procedures are:

- Setting NE Event Parameters (ITM-SC Maintenance Guide (SMG))
- Setting NE Event Control Information (SMG)
- Setting WDACS Station Alarm Control (SMG)
- Setting SLM Regenerator Alarm Information (SMG)
- Setting Alarm Parameters for Existing Resources (SMG)
- Setting Manager Event Parameters (SMG)
- Setting EMS Event Parameters (ITM-SC Administration Guide (SAG))
- Setting EMS Event Control (SAG)

Related concepts are:

- Events [10-20]
- Event Characteristics [10-23]

Parameters used in this procedure can be found at Parameters for Setting All NE Event Control [4-25].

Procedure

Follow these steps to set alarm latching:

1 Select *Events -> Multi NE Alarm Control* from the top level menu.

Result:

The *EMS - Multi NE Event Control* window, showing the present settings, is displayed.

2 To set Latching and/or NE Alarm History Recovery for an individual NE, select *Individual NE alarm Control.*

Result:

The *EMS - NE Event Control Information* window is displayed. By means of the procedure described in procedure "Setting NE Alarm Control Information" individual NEs can be latched.

3 To set Latching and/or Alarm History Recovery for *ALL* NEs select `Edit`.

Result:

The *EMS - Edit All NE Event Control* window is displayed.

4 Set the Latching and Alarm History Recovery for all NEs to `On` or `Off`

5 Select `OK`.

Result:

The *EMS - Edit All NE Event Control* window closes.

6 Select `Close`.

Result:

The *EMS - Multi NE Event Control* window closes to complete the procedure.

END OF STEPS

□

Parameters for Setting All NE Event Control

Introduction

The fields needed during setting All NE Event Control are described below:

Latching state

The following information is displayed for the latching status:

Latching Status	**Displayed When...**
On for Some NEs	Latching has been previously set only on a per NE basis.
On for All NEs	Latching for all NEs has been previously set.
Off for All NEs	Latching for all NEs was not previously set.

NE Alarm History Recovery

Alarm History Recovery is only available to ADM155 and ADM 4/1 NEs. The following information is displayed for the NE Alarm History Recovery status:

NE Alarm Recovery Status	**Displayed when...**
On for Some NEs	NE Alarm History Recovery has been previously been enabled on a per NE basis.
On for All NEs	NE Alarm History Recovery for all NEs has been previously enabled.
Off for All NEs	NE Alarm History Recovery for all NEs was not enabled.

□

Section: Enabling Alarm Color Indication Modification

Overview

Purpose

Perform this procedure to allow a ITM-SC Client to use the alarm color resources on the ITM-SC Server. Normally the ITM-SC Client should use its own, default alarm color indications. By performing the *Configuring Colors for Alarm Severities* procedure the server will store the customized alarm color indication. By performing this procedure the ITM-SC Client will use this customized alarm color indication.

□

Enabling Alarm Color Indication Modification

When to use

When changing the alarm color indication as stored on the ITM-SC Server.

Before you begin

Before performing this procedure consider the following:

- A running ITM-SC Client will not be updated automatically. It should be restarted to take advantage of the updated colors.

Related information

No related information is available.

Procedure

1 Make sure the default ITM-SC Server is set to the desired server.

2 Login to an *ITM-SC Client*.

3 Execute a terminal window by selecting the *Lucent logo* at the VUE menu bar.

4 Log in as user *i2kadmin*.

5 Enter at the command line:

```
/opt/itm/sc/bin/ItmscChangeColours
```

6 Close the terminal window.

7 Repeat this procedure for each *ITM-SC Client*.

END OF STEPS

□

Section: Changing Alarm Color Indication

Overview

Purpose

Use this procedure to change the alarm notification color property on the network map. The highest alarm severity present in a Network Element is indicated by the color of the representing icon on the network map.

□

Changing Alarm Color Indication

When to use

To align the alarm severity indicating colors for icons on the network map with the company's maintenance philosophy.

Before you begin

Before performing this procedure make sure:

- each ITM-SC client is enabled for this change. To enable a ITM-Client perform the *Enabling Changing Alarm Color Indication* procedure.

Related information

The related procedure is:

- Enabling Changing Alarm Color Indication

Parameters used in this procedure can be found at Parameters for Changing Alarm Color Indication [4-31].

Procedure

Follow these steps to change the colors for alarm severities on the network map.

1 Open the ITM-SC Management menu and select the *Configure colors for Alarm Severities* icon.

Result:

The *Color Information Status* window is displayed.

2 Select `Edit`

Result:

The *Configure Color and Server Edit Definition* window is displayed.

3 Select *Configure*

4 Select one or more Servers which are to be configured

5 Select an *Alarm Severity* and `OK`

Result:

The *Edit Color Chart* window is displayed

6 Select a *new color* and *`OK`*

Result:

The *Edit Color Chart* window disappears

7 Select an other *Alarm Severity* to configure if necessary and repeat the previous step.

8 If finished select `Close`

Result:

The *Configure Color and Server Edit Definition* window disappear.

END OF STEPS

□

Parameters for Changing Alarm Color Indication

Introduction

Use these parameters, as described below, to configure the colors for alarm severities.

Sever Name

This field lists the stored ITM-SC Server names. Selecting a server name will populate the alarm severity fields with the current selected color.

Alarm Severity

When the server name is selected the color buttons will be populated with the current colors for each alarm severity. The color buttons will be greyed out if no ITM-SC Server is selected.

Color State

When default is selected the colors for alarm severities will be set to the default value for the list of selected ITM-SC Servers. When Configure is select the user is allowed to change the colors for alarm severities.

Server Name to be added to the list

This field allows the user to add a server name to the ITM-SC Server list.

Server Name to be removed from the list

This field allows the user to remove a server name from the ITM-SC Server list.

Default Color Settings

The default colors are detailed in the table below.

Severity	Color
Prompt	Red
Deferred	Yellow
Information	Orange

□

Section: Viewing Event Storage Capacity

Overview

Purpose Use this procedure to check the event store capacity of the ITM-SC. You can view the used and remaining capacity of current and historical logs. Events both include alarms and autonomous events.

□

Viewing Event Storage Capacity

When to use

To display the number of events stored on the ITM-SC in either the current or history event list. To change the settings of the event store capacity please refer to the Setting EMS Alarm Control Information procedure.These parameters can be set by an administrator only.

Before you begin

No prerequisites or precautions are needed when performing this procedure.

Related information

Related procedures are:

- Generating Event Reports
- Managing Event Archives

Related concepts are:

- Events [10-20]
- Event Characteristics [10-23]
- Event Storage and Archiving [10-27]

Parameters used in this procedure can be found at Parameters for Viewing Event Storage Capacity [4-34].

Procedure

Follow these steps to view the alarm store capacity.

1 Select Events -> EMS Event Store Capacity from the top level menu.

Result:

The EMS - Event Store Capacity window is displayed.

2 By selecting Print the information within this window will be put into a report. By means of the report browser a hardcopy print can be made.

3 Select Close to end viewing the EMS - Event Store Capacity.

Result:

The EMS - Event Store Capacity window closes to complete the procedure.

END OF STEPS

□

Parameters for Viewing Event Storage Capacity

Introduction

The parameters described below indicate information about the number of events stored, the warning threshold and absolute maximum for both the current and history event list.

System notifies when capacity reached

The system automatically notifies you when the event log exceeds a programmed capacity threshold (typically 75% full). Archiving historical information and/or deleting historical events can be performed before log space has been used and information is lost. When the current store reaches its full capacity, an instantaneous alarm is raised. This alarm, when acknowledged, changes its state to “Cleared” and the oldest 15% of the instantaneous and/or cleared latched persistent alarms waiting acknowledgment are automatically moved to the history store. If this occurs in the history store, the oldest 15% are deleted.

Warning Threshold

The number of events that can be stored before a EMS alarm is raised to inform you that the alarm list is nearing capacity. The alarm will only be cleared once the number of alarms has fallen to 75% of this threshold.

Absolute Limit

The maximum number of events that can be stored.

Total Number Present

The total number of events currently stored.

Unacknowledged

The total number of events that are not acknowledged.

% Occupancy

The percentage of the list that has been used.

□

Section: Managing ITM-SC Database Archives

Overview

Purpose

All ITM-SC Database archiving activity information is stored on the ITM-SC. By performing this procedure a clear insight is obtained about the last archives made. Furthermore archives on disk can be transferred to tape as well as old archives can be deleted.

□

Managing ITM-SC Database Archives

When to use To obtain information about the last archives made, clean up the disks and move archives on disk to tape.

Before you begin No prerequisites or precautions need to be considered when performing this procedure.

Related information Related procedures are:

- Backing Up the ITM-SC Database
- Restoring the ITM-SC Database
- Backing up the Entire ITM-SC System
- Restoring the Entire ITM-SC System

Parameters used in this procedure can be found at Parameters for Managing ITM-SC Database Archives [4-37].

Procedure Perform these steps to manage the ITM-SC Database Archives

1 Select *Database Archive* -> *Administration*

Result:

The *ITM-SC Archive Summary* window is displayed listing all pending or completed archives.

2 Select an *ITM-SC Database Archive*.

3 To move the selected Archive to tape select *Archive to Tape*

4 To delete a finished archive or to cancel a pending archive select `Delete`

5 Select `Refresh` to update the summary list with the last changes

6 Select `Close` to exit the procedure

Result:

The *ITM-SC Archive Summary* window will disappear.

END OF STEPS

□

Parameters for Managing ITM-SC Database Archives

Introduction

The following parameters can be found on the windows used to manage ITM-SC Database archives

Type

Displays the type of the archive performed. This will be either Immediate or Schedule.

Device

Indicates the device on which the archive is stored. This will be either Disk or Tape

Name

Indicates the archive filename as entered during archive creation

Status

Indicates whether problems where determined during archiving.

Button description

The following buttons are provided on the ITM-SC Database Archive Summary window.

Button	Description
Archive To Tape	This button will save a selected disk archive from the summary list to tape.
Delete	This button will delete a successfully completed disk archive, if one is selected. It also will cancel any outstanding archive requests, either to tape or disk.
Refresh	This button will refresh the summary list.

□

Section: Managing Event Archives

Overview

Purpose Use this procedure to manage event archives.

When to perform Procedures are provided to store events in a file, the event archive, write the archive to tape, stop a daily archive and to delete archives from the ITM-SC.

□

Create an Event Archive

When to use

When wanting to store events on the ITM-SC.

Before you begin

Before performing this procedure consider the following:

- Performing an immediate archive (option `now`) within 15 minutes of a scheduled Event Archive will postphone the scheduled Event Archive with 15 minutes.

Related information

The related procedures are:

- Viewing Event Storage Capacity (ITM-SC Maintenance Guide)
- Generating Event Reports (ITM-SC Maintenance Guide)
- Copy archive to the Default Device
- Cancel a Scheduled Archive
- Delete an Archive

The related concept is:

- Event Storage and Archiving [10-27]

Parameters used in this procedure can be found at Parameters for Creating an Event Archive [4-45].

Procedure

Follow these steps to create an event archive.

1 Select *Events* -> *Event Archive* from the top level menu.

Result:

The *EMS - Event Archive Information* window, showing the current archives, is displayed.

2 Select the *Create* menu item (under *Archive Menu*) to create an event archive.

Result:

The *EMS - Create Event Archive* window is displayed.

3 Enter the *Archive File Name*.

4 Enter the *Archive Description*.

5 Set the *Scheduled Archive* time and date.

- Select `Now` to start the archive immediately.
- Select `Daily at Specified Time` to select a daily time for the archive. If you select this option, you must enter the time in the Daily Archive Time field.

6 Select `OK`.

Result:

If selected the option to create a daily archive, a window will inform you if this request cannot be performed immediately. If so a new scheduled time for execution will be given.

If you submit another request for creating a daily archive before the new scheduled time, the latest request will replace the existing request

When selected the `Now` option the *EMS - Create Event Archive* window will close.

7 When necessary select `OK` to finish this procedure

END OF STEPS

□

Copy Event Archive to the Default Device

When to use When wanting to store an archived set of events on the default device.

Before you begin No prerequisites or precautions need to be considered when performing this procedure

Related information The related procedures are:

- Viewing Event Storage Capacity (ITM-SC Maintenance Guide)
- Generating Event Reports (ITM-SC Maintenance Guide)
- Create an Event Archive
- Cancel a Scheduled Archive
- Delete an Archive

The related concept is:

- Event Storage and Archiving [10-27]

Parameters used in this procedure can be found at Parameters for Creating an Event Archive [4-45].

Procedure Follow these steps to copy an archive to the default device.

1 Select *Events* -> *Event Archive* from the top level menu.

Result:

The *EMS - Event Archive Information* window, showing the current settings, is displayed.

2 Select the Archive you wish to transfer to the device and select the `Write to Device` option from the *Archive Menu* to write an event archive to tape.

Result:

A user confirmation window is displayed which prompts you to check that the media is present in the default device and warns that any existing files on the media will be overwritten.

3 Select `OK`.

4 Wait for the system to finish its data transfer. When writing the archive file to another device the original file remains on the ITM-SC.

5 Select *File -> Close in the EMS - Event Archive Information* window.

Result:

The window will disappear.

END OF STEPS

□

Cancel a Scheduled Archive

When to use When wanting to stop the automatic archiving of events.

Before you begin No prerequisites or precautions need to be considered when performing this procedure

Related information The related procedures are:

- Viewing Event Storage Capacity (ITM-SC Maintenance Guide)
- Generating Event Reports (ITM-SC Maintenance Guide)
- Create an Event Archive
- Copy archive to the Default Device
- Delete an Archive

The related concept is:

- Event Storage and Archiving [10-27]

Parameters used in this procedure can be found at Parameters for Creating an Event Archive [4-45].

Procedure Follow these steps to cancel a scheduled archive.

1 Select *Events* -> *Event Archive* from the top level menu.

Result:

The *EMS - Event Archive Information* window, showing the current settings, is displayed.

2 Select *Archive* -> *Cancel Daily Archive* to cancel the daily event archive.

Result:

A confirmation window is displayed.

3 Select `OK` to confirm this cancellation.

4 Select *File* -> *Close* in the *EMS - Event Archive Information* window.

Result:

The window will disappear.

END OF STEPS

□

Delete an Event Archive

When to use

When an EM Archive is not needed anymore it’s better to remove this archive from the system to free disk resources.

Before you begin

No prerequisites or precautions need to be considered when performing this procedure

Related information

The related procedures are:

- Viewing Event Storage Capacity (ITM-SC Maintenance Guide)
- Generating Event Reports (ITM-SC Maintenance Guide)
- Create an Event Archive
- Copy archive to the Default Device
- Cancel a Scheduled Archive

The related concept is:

- Event Storage and Archiving [10-27]

Parameters used in this procedure can be found at Parameters for Creating an Event Archive [4-45].

Procedure

Follow these steps to delete an archive:

1 Select *Events* -> *Event Archive* from the top level menu.

Result:

The *EMS - Event Archive Information* window, showing the current settings, is displayed.

2 Select the archive to be deleted and select *Archive Menu* -> *Delete*.

Result:

A user confirmation window is displayed.

3 Select `Yes` to confirm this deletion.

4 Select *File* -> *Close* in the *EMS - Event Archive Information* window.

Result:

The window will disappear.

END OF STEPS

□

Parameters for Creating an Event Archive

Introduction

The parameters needed to create an event archive are described below.

Archive File Name

Indicates the ID for the archive. Must follow DOS/UNIX naming rules with a maximum of 8 characters.

Archive File Size

The size of the created event archive will depend on the number of records stored as well as the content of the records. The size is indicated in kBytes. A displayed size of 0 indicates the file is less than 1 kByte.

Archive Description

Description of the archive. Maximum of 50 characters, including spaces. Must follow DOS/UNIX naming rules.

Schedule Archive

Selects either an instantaneous archive (now) or a pre-scheduled archive (daily at specified time). This specified time will be rounded up to the nearest 15 minutes (for example: quarter past, half past)

Daily Archive Time

Specifies the time an archive is made each day.

File directory and format

The PM Archive will be stored on the ITM-SC server or Stand-alone. It will be stored in twofold in the *var/spool/itm/sc/archive/alarmhist* directory. One file (*.ARC.txt) will in a tab separated ASCII format while the other (*.gz) will be in a gz compressed format. The *.gz file can be decompressed by the UNIX command `uncompress`. Other decompress programmes are widely available.

When performing the Copy Event Archive to the Default Device [4-41] procedure note that only a copy is made from the compressed archive file.

□

Section: Archiving PM Data

Overview

Purpose

The archiving of history data allows the user to obtain a long term, global view of the managed transport network. This data can be used for planning preventative maintenance strategies and assist in customer quality of service reports.

□

Create a PM Archive

When to use When wanting to store PM data for later use.

Before you begin Before performing this procedure make sure:

- the measurement, to store the PM data from, is finished.
- the place where the PM Archive data will be archived must be connected and operational (this place is defined at installation time)

Before performing this procedure consider the following precautions:

- It is not possible to create a PM Archive within 30 minutes of a scheduled Event Archive.
- When the previous prerequisites are not met, the procedures can still be performed up to a certain step but error notification is displayed.

Related information The related procedures are:

- Delete a PM Archive
- Copy a PM Archive to Default Device

Related concepts are:

- PM Data Storage and Recovery [10-28]
- PM Data Archiving [10-31]

Parameters used in this procedure can be found at Parameters for Archiving PM Data [4-53].

Procedure Follow these steps to create a PM Archive :

1 Select *Performance -> Archive List.*

Result:

The *EMS - PM Archive List* window is displayed.

2 Select *Archive -> Create.*

Result:

The *PM Archive Create* window is displayed.

3 Select the *Archive Filename* field and type the archive file name.

4 Select the *Description* field and type a description of the archive file.

5 Select the `Selection Dialog` button.

Result:

The *EMS - NE Multiple Selection Dialog* window is displayed. This window shows a list of nodes to select.

6 Select the Nodes for which data has to be archived.

7 In the PM Archive Create Window select the *Measurement Period*. This can be either *15 Minute Unidirectional*, *24 Hour Unidirectional* or/and *24 Hour Bidirectional*.

8 Select the archive timing of the data to be archived by entering First Measurement Period and Last Measurement Period.

9 Select the *TP* and TP and/or TCM in the Measurement Point box to filter the list

10 Click `Apply`.

Result:

If no TPs are selected a warning screen is displayed. The Archive is created.

11 Click `Close` to stop creating archives. To close the *EMS -PM Archive List window* select *File -> Close*.

END OF STEPS

□

Delete a PM Archive

When to use When a PM Archive is not needed anymore it's better to remove this archive from the system to free disk resources.

Before you begin Before performing this procedure make sure:

- the PM archiving procedure is completed. Do NOT delete a Performance Monitoring Archive while the archive operation (archive to device) is still in progress

Related information The related procedures are:

- Create a PM Archive
- Copy a PM Archive to Default Device

Related concepts are:

- PM Data Storage and Recovery [10-28]
- PM Data Archiving [10-31]

Parameters used in this procedure can be found at Parameters for Archiving PM Data [4-53].

Procedure Follow these steps to delete a PM Archive :

1 Select *Performance -> Archive List*.

Result:

The *EMS - PM Archive List* window is displayed.

2 Select the Archive to *delete*

Result:

The archive to delete is highlighted

3 Select *Archive -> Delete*

Result:

A confirmation window is displayed.

4 Click *Yes.*

Result:

The Archive is removed from the ITM-SC and the confirmation window disappears.

5 To close the *EMS -PM Archive List* window select *File* -> *Close*.

END OF STEPS

□

Copy a PM Archive to Default Device

When to use When wanting to export the PM data from the ITM-SC to the default device.

Before you begin Before performing this procedure make sure:

- the device name has been defined (see procedure Changing Default Device Names in the Subnetwork Administration Guide (SAG))
- the device is operational

Related information The related procedures are:

- Create a PM Archive
- Delete a PM Archive

Related concepts are:

- PM Data Storage and Recovery [10-28]
- PM Data Archiving [10-31]

Parameters used in this procedure can be found at Parameters for Archiving PM Data [4-53].

Procedure Follow these steps to write an archive to a device :

1 Select *Performance* -> *Archive List*.

Result:

The *EMS - PM Archive List* window is displayed.

2 Select the archive which must be written to the external device

Result:

The archive to move is highlighted

3 Select *Archive* -> *Write to Device*

Result:

A confirmation window is displayed.

4 Click *Yes*.

Result:

The Archive is copied from the ITM-SC to the external device and the confirmation window disappears.

5 Wait for the system to finish its data transfer. A transfer of around 200 Mb will take 2 minutes. To close the *EMS -PM Archive List* window select *File* -> *Close*.

END OF STEPS

□

Parameters for Archiving PM Data

Introduction

The parameters, as described below, give information about the PM Archives.

Network data logged

Performance Monitoring data for a TP is stored for a maximum of 31 days (31 bins of 24 hours are available) for later analysis and statistics.

Archive File Name

The user can choose an archive file name up to 32 characters and conform to DOS/UNIX naming rules.

Archive Description

A description can be added up to 50 characters and conform to DOS/UNIX naming rules.

Archive Size

Indicates the compressed size of the Archive file in Mbytes. A displayed size of 0 indicates the file is less than 1 Mbytes. This value is automatically generated

File directory and format

The PM Archive will be stored on the ITM-SC server or Stand-alone. It will be stored in twofold in the *var/spool/itm/sc/pm_archive* directory. One file (*.ARC.txt) will in a tab separated ASCII format while the other (*.gz) will be in a gz compressed format. The *.gz file can be decompressed by the UNIX command `uncompress`. Other decompress programmes are widely available.

When performing the Copy a PM Archive to Default Device [4-51] procedure note that only a copy is made from the compressed archive file.

Measurement Parameter

The list contains the measurement parameters available. By default all the counters are selected.

Archive Timing

The current time/date rounded backwards to the nearest reporting interval (15 minutes or 24 hours, depending on Measurement Period type) minus the database retention period.

For Normal Performance Monitoring the default Retention Date/Times are:

- 1 day for 15 minutes
- 31 days for 24 hour monitoring

For Extended Performance Monitoring the Retention Date/Times are:

- 7 days for 15 minutes monitoring
- 62 days for 24 hour monitoring

The date is displayed according: dd:mm:yy and the time according hh:mm.

Measurement Period For all NEs except the ADM 16/1 the 24 Hours Bidirectional option is greyed out For ADM 16/1 NEs, both the Unidirectional and Bidirectional options will be available. If the user attempts to deselect the only valid option it will remain selected.

TP Displays all available TP points for the selected NE. This selection can be any combination from 1 to all.

Measurement Points The user is able to select TP and TCM points. At default is both types of measurement points are selected.

□

5 ITM-SC Reliability

Overview

Purpose

This chapter describes tasks which will increase the reliability of the ITM-SC and its functionality. This can be done by adding extra hardware or creating a software backup of the ITM-SC.

Content

Subjects described in this chapter are:

- creating software backups
- adding hardware redundancy within the ITM-SC
- adding hardware outside the ITM-SC

Abbreviations used

When Network Elements OLS 80G, ADM 4/1, ADM 16/1, ADM16/1c, AM 1 (Plus) and TM 1 are described WaveStar®OLS 80 G, WaveStar®ADM 4/1, WaveStar® ADM 16/1, WaveStar® ADM16/1 compact, WaveStar® AM 1 (Plus) and WaveStar® TM 1 are meant.

□

Section: Backing up the Entire ITM-SC System

Overview

Purpose

The following procedures describe how to perform a backup of a complete ITM-SC. One procedure is provided to backup the server or stand-alone and one for a backup of a client.

The total backup will include Database, Unix and ITM-SC Configuration files.

□

Backing up an entire ITM-SC Server/Standalone

When to perform To prevent data begin lost on an ITM-SC Server or Standalone when the ITM-SC is to be installed again.

Before you begin No prerequisites or precautions are needed when performing this procedure.

Related information Related procedures are:

- Backing Up the ITM-SC Database
- Restoring the ITM-SC Database
- Managing ITM-SC Database Archives
- Restoring the Entire ITM-SC System

Related concepts are:

- ITM-SC Database [10-33]
- Archiving [10-34]

Procedure Follow these steps to back up the total ITM-SC server or stand-alone. Two clean tapes are required. Label them “Database Backup *hostname*” and “Server backup *hostname*”. Backup can be done on-line without stopping the ITM-SC.

1 Place a clean tape labelled “Database Backup *hostname*” in the tape drive of the ITM-SC Server/Stand-alone.

2 Log into a *Client ITM-SC* as an *administrative* user, and follow the *Backing Up ITM-SC Database* procedure

3 After a successful backup remove the tape and write protect it.

4 Place a clean tape labelled “*Server Backup*” in the tape drive of the Server/Stand-alone.

5 Login as *Root* via the *Unix Terminal* window.

6 Enter the following command: `itmsc_backup`. Press **ENTER**

7 After a successful backup remove the tape and write protect it.

8 Log out from *Root* to complete the procedure.

END OF STEPS

□

Backing up an entire ITM-SC Client

When to perform

To prevent data begin lost on an ITM-SC Client when the ITM-SC is to be installed again.

The total backup will include Database, Unix and ITM-SC Configuration files.

Before you begin

No prerequisites or precautions are needed when performing this procedure.

Related information

Related procedures are:

- Backing up an entire ITM-SC Server/Standalone
- Backing Up the ITM-SC Database
- Restoring the ITM-SC Database
- Managing ITM-SC Database Archives
- Restoring the Entire ITM-SC System

Related concepts are:

- ITM-SC Database [10-33]
- Archiving [10-34]

Procedure

Follow these steps to back up the total ITM-SC client. One clean tape is required. Label the tape “Client *hostname*”

1 Place the tape “Client *hostname*” in the tape drive of the client.

2 Login as *Root* via the *Unix Terminal* window.

3 Enter the following command: `itmsc_backup`. Press **ENTER**.

4 After a successful backup remove the tape and write protect it.

5 Log out from *Root* to complete the procedure.

END OF STEPS

□

Section: Backing Up the ITM-SC Database

Overview

Purpose To prevent total loss of the ITM-SC its data it is necessary a backup of the ITM-SC (Informix) database is made at regular intervals. Performing a backup is also called archiving.

□

Backing Up the ITM-SC Database

When to perform To prevent ITM-SC database information to get lost when the ITM-SC fails to restart the database or to freeze a specific NE setting.

Before you begin No prerequisites or precautions are needed when performing this procedure.

Related information Related procedures are:

- Restoring the ITM-SC Database
- Managing ITM-SC Database Archives
- Backing up the Entire ITM-SC System
- Restoring the Entire ITM-SC System

Related concepts are:

- ITM-SC Database [10-33]
- Archiving [10-34]

Parameters used in this procedure can be found at Parameters for Backing Up the ITM-SC Database [5-9].

Procedure Follow these steps to backup the ITM-SC database.

1 If a tape is used to backup, *label the tape with the appropriate hostname* and insert it in the tape drive.

2 Open the *ITM-SC Administration* menu and select the *Backup/Restore Database* icon.

Result:

The *ITM-SC Database Control* window is displayed.

3 Select `Backup`.

Result:

The *Create Database Archive* window is displayed.

4 Select a *Target Device* and enter an *Archive File Name*

5 Select the *host* where the tape or disk is mounted. In case of archiving to disk also the path must be entered. The default location is the default host where the backup is being done from.

6 Select either *Scheduled* or *Periodic* to set the *Archive Type*.

7 If a *scheduled* Archive Type is chosen, select *Now* for an instantaneous archive creation or *Later* to choose a more suitable time. If *Later* is chosen select a start time at the *When* field.

8 If a *periodic* Archive Type is chosen, select either *Daily* or *Weekly* and select a *Start Time*.

9 Select the number of retry attempts. This is needed in case the archive creation is cancelled due to a database lock.

10 Select `Apply`

Result:

The settings are activated.

11 Select `Close` to complete the procedure

Result:

The *Create Database Archive* window disappears

END OF STEPS

Error Messages

During the creation of a Database Archive the following errors can be displayed.

- *Destination not found*: Indicates there is either no tape drive or no tape in the drive.
- *Low Bandwidth*: Indicates the bandwidth is below the required speed of 1Mbit/s.
- *Archive Exists*: the name of the archive to be created already exist.

□

Parameters for Backing Up the ITM-SC Database

Archive Configuration options

The parameters displayed during the configuration of the archive are described below:

Target device

Defines whether archive files are stored on disk or tape. An Archive File Name is mandatory.

Archive type

Defines whether the archiving is performed once or periodically.

Schedule archive

This field of parameters will be highlighted when the Archive Type Scheduled. It allows to perform an instantaneous archive or to postpone the archive creation until a specified time and date. The specified time can be set by a quarter of an hour increments.

Periodic archives

This field of parameters will be highlighted when the Archive Type is set to Periodic. It allows to perform a daily or weekly archive. The time can be selected from the Start Time field by a quarter of an hour increments. For a weekly archive the date needs to be set as well.

Enter Number of Archive Retries

An archive can be cancelled due to an Database lock. (e.g. CTL busy or archive refused by the archive broker). This number indicates the amount of retries before the periodic archive is aborted. Valid entries are 1 up to 5 with a default value of 4.

□

Section: Disk Mirror Installation and Setup

Overview

Purpose

To increase the reliability of the ITM-SC Server, a second disk or a second pair of disks can be installed. The second disk or pair will maintain an exact copy of the primary one. When the primary disk fails the second will take over all processes active on the ITM-SC Server.

The disk mirroring for the ITM-SC Server is achieved by use of HP MirrorDisk/UX software, additional SCSI controller cards (optional) and additional disk drives.

□

Disk Mirror Installation

When to use

When installing a second disk to increase reliability.

Before you begin

To order to achieve full operational disk mirroring two procedures must be performed: *Disk Mirror Installation* and *Disk Mirror Setup*. Although the Disk Mirror Setup procedure can only be done when the Disk Mirror Installation procedure is performed successfully these two procedures can be performed individually.

When performing this procedure make sure:

- The system on which the disk mirroring software is being installed is a Large Network Management Server with the hardware of the Optional Mirroring Components already installed.
- ITM-SC is installed and configured according the ITM-SC Server Installation procedure.
- The PM archive disk is installed if the PM archive option is licensed.
- The Customer ID is known for the system.
- A Mirror U/X Codeword is available.
- The CD-ROM must be present for which the above Customer ID and Mirror U/X Codeword are valid.

Before performing this procedure consider the following:

- It is not possible to install an ITM-SC after disk mirroring has been set up.

Related information

The related procedure is:

- Disk Mirror Setup

Procedure

Follow these steps to install a second disk or pair of disks:

1 Login as *root*

2 Insert the Application Software CD-ROM into the CD-ROM drive.

3 To make a new directory enter the command:

```
mkdir /SD_CDROM
```

4 Enter the following command: `ioscan -fnC disk`

Result:

The output should will contain a line for the CD-ROM device. For example:

```
disk 2 8/16/5.2.0 sdisk CLAIMED DEVICE
TOSHIBA CD-ROM XM-5401 TA /dev/dsk/c1t2d0
/dev/rdsk/c1t2d0
```

5 Write down the device filename that starts with */dev/dsk/c*...... In the example above this will be *c1t2d0*.

6 Enter the following command: `mount /dev/dsk/<device filename> /SD_CDROM`. Replacing the `<device filename>` with the output from the `ioscan` command. In the example above this will be `c1t2d0`. For more details of the commands `ioscan`, `mkdir` and `mount` see the HP Manual.

7 To determine the bundle ID enter the following command:

```
swlist -d @ /SD_CDROM | grep <product number>
```

Result:

The bundle ID is the first word of the output displayed, usually the *<product number>* with a suffix. For example the bundle ID for product number *B2491A* is *B2491A_APZ*. Now the bundle ID is known.

8 Write down the *bundle ID*.

9 To licence and install the software enter the following command:

```
itmsc_mirror_install <bundle ID>/SD_CDROM
<bundle ID> <codeword>
```

Note: When typing the codeword into the command line it is necessary to omit any spaces there may be between the blocks of characters.

Result:

You will be requested for the Customer ID and HP Codeword.

10 Enter the Customer ID and HP codeword.

Result:

The command should then prompt with a warning message:

```
WARNING!!! When the software has been
installed the system will reboot!!! Do you
wish to continue (y/n [y])
```

11 Type `n` to terminate the command without installing the software. Type `y` to start the software installation process.

Result:

If `y` is selected the progress of the installation process will be logged to the screen. On successful completion of the software load the system will reboot. The setup of the mirrored disk can now be carried out. Disk Mirror Setup [5-14]

END OF STEPS

□

Disk Mirror Setup

When to use

When installing a second disk to increase reliability and the installation procedure is performed succesfully..

Before you begin

Before performing this procedure make sure:

- the Disk Mirror Installation procedure is performed succesfully..

Although the Disk Mirror Setup procedure can only be done when the Disk Mirror Installation procedure is performed successfully these two procedures can be performed individually.

Related information

The related procedure is:

- Disk Mirror Installation

Procedure

Follow these steps to setup and initialize a Mirrored Disk:

1 Login as *root*

2 Repeat the following steps for each *Volume Group* (disk) that is to be mirrored.

3 Determine the <bundle-ID> for HP MirrorU/X is the same as the <bundle-ID> obtained during the disk miroring installation.

After disk mirroring installation has been done, the <bundle-ID> can be obtained by command:

```
swlist | grep “HP MirrorU/X”
```

The bundle-ID is the first word of the output displayed, usually the <product number> wit a suffix. For example the bundle-ID for product number B2491A is B2491A_APZ.

Result:

The bundle ID is known.

4 Enter the following command: `itmsc_mirror_setup –b <bundle ID>`

Result:

The available Volume Groups are listed together with some details of the Logical Volumes contained and the physical disks used. Accordingly the ITM-SC will prompt the following message: `Select Volume Group to mirror (0 to abort):`

5 Enter the *Volume Group* to mirror.

Result:

A list of the available unused disks is displayed.

For example:

```
1 /dev/dsk/c0t5d0 4095 Mbyte SEAGATE
ST34371W.
```

Accordingly the ITM-SC will prompt the following message:

```
Select disk to mirror (0 to abort):
```

6 Select one of the available disks by entering the corresponding number.

Result:

A confirmation message is displayed.

For example:

```
Do you wish to add mirror disk
/dev/dsk/c0t5d0 to Volume Group /dev/vg00
(y/n [n])?
```

7 To terminate without any action taken enter `n`. To setup the mirroring as indicated by the confirmation message enter `y`.

Result:

It will take about *1 hour* to complete the synchronization of the new mirror disks.

8 To mirror another *Volume Group* repeat this procedure.

END OF STEPS

□

Section: Configuring a cold stand-by ITM-SC

Overview

Purpose

To increase the availability of the ITM-SC management system a so called ‘cold stand-by’ can be configured to backup the live ITM-SC. One cold stand-by ITM-SC will backup only one ITM-SC.

□

Configuring a cold stand-by ITM-SC

When to use

When adding an extra ITM-SC which acts as a cold stand-by.

Before you begin

Before performing this procedure make sure:

- the hardware configuration for the cold standby ITM-SC is the same as the live ITM-SC. For example same number of disks of the same size.
- the cold standby ITM-SC is connected to the same (Q-LAN) LAN0 as the live ITM-SC.
- the ethernet (TCP/IP) *LAN–1*connection on the cold stand-by ITM-SC is *NOT* connected to the same hub as the live ITM-SC. This will cause network conflicts because the stand-by ITM-SC will be installed using the same hostname and IP address as the live ITM-SC.

Before performing this procedure consider the following

- This procedure requires knowledge of ITM-SC administration, specifically the database backup and restore procedure. The recommended approach is to configure the cold stand-by ITM-SC and verify that it can manage the NEs. After configuration of the cold stand-by ITM-SC regular backups of the running ITM-SC and the database should be performed to tape.
- To ease the database backup configure the backup as periodic archive.

Related information

The related concept is:

- UPS Installation [10-35]

Procedure

Perform these steps to configure a cold stand-by:

1 Clean install the cold stand-by ITM-SC using the same procedure and software release used to install the live ITM-SC. Make sure the *hostname, IP address* and *NIS configuration* are the same as the live ITM-SC.

If the cold stand-by is a NIS Slave it will need to obtain its NIS information from the NIS master. To do so take into account the following prerequisites:

Before entering the `itmsc_server_setup` or `itmsc_standalone_setup` command:

- disconnect the live ITM-SC from *LAN–1*
- connect the cold stand-by ITM-SC to *LAN–1*.
- Restore the *LAN–1*connection to their original positions when the Informix serial number is entered.

2 After the installation has finished licence the cold stand-by ITM-SC for the same features that the live ITM-SC supports.

3 Make a backup of the licence file on the cold stand-by ITM-SC because it will be copied out when the ITM-SC configuration files are restored from the live ITM-SC. Log in as user *root* and enter the following commands:

- `. /opt/itm/sc/etc/itmsc_setup`
- `cd $EMSAPPLDIR`
- `cp authcodes /etc/opt/itm/sc`

4 Log onto the *live ITM-SC* as user *root*. Place a tape, not write protected and labelled *ITM-SC backup*, into the tape drive. Save the live ITM-SC files to tape by running the following command, note the ITM-SC will not need to be shutdown: `itmsc_backup`

Result:

The following message is displayed: `INFO: Start of itmsc_backup. Do you wish to use /etc/opt/itm/sc/SaveList (y/n[y])?`

5 Select `y` (yes) and press **ENTER**.

Result:

The files saved to tape will be displayed. This will take *half an hour*.

6 When all of the configuration files have been saved remove the tape from the tape drive and write protect it.

7 Insert a second tape, not write protected and labelled with *Informix Backup <hostname>* into the tape drive. Perform the Backing up the ITM-SC Database procedure described in the *Sub-network controller*

Administration Guide (SAG). After finishing this procedure remove the tape and write protect it.

8 Step 4 until Step 7 should be repeated on a regular basis to ensure that an up-to-date backup of the live ITM-SC is maintained. Step 4should be done when any new users, hosts or system alarm monitor configuration changes are made. This should not need to be done as frequently as Step 7, which can be configured as an automatic periodic archive.

9 In the event of a live ITM-SC failure or to test the cold stand-by ITM-SC configuration:

- log in as user root onto the cold stand-by ITM-SC
- Place the tape labelled ITM-SC back-up into the tape drive
- enter the following commands successively:
  - `init 3` (login again as user root)
  - `itmsc_restore`

Result:

After the `init 3` command the user is asked to log in again as user root. After the itmsc_restore command the following message will be displayed: `INFO: Start of itmsc_restore WARNING: The ITM-SC will be stopped and the files on the tape restored. Any existing data will be overwritten. Are you sure you want to continue (y/n [n])?`

10 Select `y` (yes) and press **ENTER**.

Result:

The saved configuration files will be restored from tape, this may take *half an hour*.

11 Log in as user root and restore the saved licence file by entering successively:

- `. /opt/itm/sc/etc/itmsc_setup`
- `cp /etc/opt/itm/sc/authcodes $EMSAPPLDIR`
- `init 4`

12 Remove the ITM-SC Backup tape and insert the tape labelled *Informix Backup <hostname>* into the tape drive of the cold stand-by ITM-SC. Follow the *Restoring ITM-SC Database* procedure as can be found in the *Sub-network controller Administration Guide* (SAG) and start the ITM-SC.

13 Remove the *LAN–1* (TCP/IP) connection from the live ITM-SC and place it into the *LAN–1* (TCP/IP) connection of the cold stand-by ITM-SC. If the live ITM-SC is running then stop it and the cold stand-by will take over management of the NEs.

14 When the live ITM-SC has been repaired it can be configured as the cold stand-by ITM-SC.

END OF STEPS

□

Section: Installing a Uninterruptible Power System (UPS)

Overview

Purpose

To increase the reliability of the ITM-SC, a Uninterruptible Power System (UPS) can provide power at times of power failure. The time a UPS can provide power to the ITM-SC system depend on the specifications of the UPS as well as the specifications of the equipment protected by the UPS.

□

Installing a Uninterruptible Power System (UPS)

When to use

When adding an UPS to increase reliability.

Before you begin

Before performing this procedure make sure that

- the server is a HP D230 or HP 380. Only these servers support UPS. It is however possible to connect the UPS to other server types but the UPS won't be fully monitored by the ITM-SC in that case.
- the ITM-SC Server is installed successfully.

Before performing this procedure consider the following:

- The alarm `UPS cannot communicate with the UPS monitor deamon` can only be raised at system start-up. Failure of the communication between UPS and ITM-SC will not be notified by the ITM-SC unless the ITM-SC is rebooted.

Related information

The related concept is:

- UPS Installation [10-35]

Procedure

Follow these steps to add UPS support:

1 Unpack the UPS device(s) and re-charge it for at least 24 hours. Connect the UPS device(s) to the serial port(s) on the workstation that will run the UPS daemon (take note of the serial port(s) and their associated */dev* entry).

2 Log into the ITM-SC system that is to run the UPS daemon as user *root*.

3 To start the installation process enter the command:

```
itmsc_ups_setup
```

Result:

The installation process retrieves the current UPS configuration. If a current UPS configuration is not present then a default configuration will be created. The UPS configuration is checked and then displayed. If an error is encountered during the configuration of the UPS then a warning will be displayed. Accordingly a prompt is displayed for setting the UPS time parameters.

4 Enter:

- D to select default values from a selection table (choose either 1, 2 or 3).
- O to enter manually values for the time parameters (enter Y or N to confirm that a time parameter is to be updated. Enter the new integer time value if Y).
- U to leave the time parameters at their current values. After the time values are set the user will be asked if more upstty entries are to be made.

5 After the time values are set a prompt is displayed asking if more *upstty* entries are to be made. Enter either:

- N to not add additional upstty entries.
- Y to add additional upstty entries:
  - select the serial port to add from the displayed list.
  - enter to add properties to the current upstty entry (select an option from the property list) or N to allocate no properties to the current upstty entry

Result:

After the additional upstty entries are complete a prompt is displayed for manipulating the lines.

6 If a line is to be manipulated (edit, move, delete or commented) then enter Y. Then enter the integer valued line number and the option.

7 When the configuration is set enter N to terminate line manipulation.

Result:

The installation process will invoke the UPS daemon and report the process identifier of the UPS daemon.

END OF STEPS

□

6 Geographic Redundancy

Overview

Objectives The geographic redundancy feature increases the reliability of network management.

Definition Geographic redundancy (GR) is a protection scheme in which a separate back-up ITM-SC can take over the management of network elements for a failed ITM-SC.

Outcome Several ITM-SC systems can be configured to work together in the geographic redundancy scheme to manage and protect management of several network elements selected by the user.

Intended use This chapter explains the concepts of geographic redundancy. After the concepts, procedures used for geographic redundancy are described.

Abbreviations used When Network Elements OLS 80G, ADM 4/1, ADM 16/1, ADM16/1c, AM 1 (Plus) and TM 1 are described WaveStar®OLS 80 G, WaveStar®ADM 4/1, WaveStar® ADM 16/1, WaveStar® ADM16/1 compact, WaveStar® AM 1 (Plus) and WaveStar® TM 1 are meant.

□

Section: Adding or Deleting a Peer ITM-SC

Overview

Purpose

The purpose of this procedure is to include or exclude peer ITM-SC systems in the geographic redundancy scheme. A peer ITM-SC system can act as a back-up and can take over the management of a network element if the primary ITM-SC fails. Under geographic redundancy, a maximum of 4 peer ITM-SC servers can be linked to a single ITM-SC. For example when the maximum of 4 peers has been reached and another peer has to be added, one of the 4 existing peers has to be delete first.

When to perform

Use this procedure to include or exclude ITM-SC systems to the geographic redundancy scheme. In other words to add or delete a peer ITM-SC.

Related procedures

Related procedures are:

- How to Display Protected Network Elements.
- How to Display Protecting Network Elements.

Prerequisites

Prerequisites for the procedure are:

- Make sure the ITM-SCs have a TCP/IP connection.
- The ITM-SC to be added should also have a connection to the same OSI-DCN.

Precautions

Pay attention to the following when adding a peer ITM-SC:

- Under geographic redundancy, a maximum of 4 peer ITM-SC servers can be linked to a single ITM-SC.
- The total number of protected and managed network elements may not exceed the ITM-SC designed limit of 200 equivalents (GR Equivalents Maximum).

□

Add or Delete a Peer ITM-SC

The purpose of the following procedure steps is to add or delete a peer ITM-SC:

1 Select *Management* --> *Geographic Redundancy* --> *Manager Information.*

Result:

The *EMS* - *Geographic Redundancy Manager Information* Window appears.

2 Select `Add Peer ITM-SC` or `Delete Peer ITM-SC`.

Result:

The *EMS* - *Geographic Redundancy Add Peer* window or the *EMS* - *Geographic Redundancy Delete Peer* window appears.

3 To add a peer ITM-SC fill in the *ITM-SC Name* that needs to be added to the GR scheme and click `Apply`.

To delete a peer ITM-SC select the *ITM-SC Name* that needs to be deleted from the GR scheme and click `Apply`.

Repeat this step to add or delete another peer ITM-SC.

Result:

The ITM-SC is added to or deleted from the GR scheme.

4 Click the `Close` button to exit the *EMS* - *Geographic Redundancy Add Peer* window or *EMS* - *Geographic Redundancy Delete Peer* window.

Result:

The window disappears and the *EMS* - *GR Manager Information* window appears. The added peer ITM-SCs will now be displayed too.

5 Click the `Close` button to exit the *EMS* - *GR Manager Information* window.

Result:

The *EMS* - *GR Manager Information* window disappears.

END OF STEPS

Parameters for Adding or Deleting a Peer ITM-SC

ITM-SC Name The name of the peer ITM-SC connected to the host ITM-SC.

Location The location of the ITM-SC server.

Link Status Contains the status of the peer to peer Link between the two ITM-SCs. The values are described in the table below:

Link Status	Description
Link Established	The link exists and is running correctly.
Link Not Established	The ITM-SCs are currently attempting to set up the link for the first time.
Link Failed Version Check	A link cannot be established because the two ITM-SC managers are running different versions of the software, or they use different versions of the ITM-SC database.

Resynch State

Resynch State	Description
Resynching	Resynching database.
Normal	Database is stable.

□

Section: Adding Network Elements to the Geographic Redundancy Scheme

Overview

Purpose

To increase the reliability of network management, network elements can be added to the geographic redundancy Scheme.

When to perform

When the management of a network element has to be protected, it has to be added to the geographic redundancy scheme.

Related procedures

Related procedures are:

- Provision a Network Element from a template.
- Create a pre-provisioned Network Element.
- View Network Element Status.
- Provisioning the Data Communications Channel.
- Performing the Data Communications Test.

Prerequisites

Prerequisites for the procedure are:

- The NE to be added should be provisioned.
- The NE to be added should be reachable by this ITM-SC in the OSI-DCN.

Precautions

Pay attention to the following:

- When the static value is chosen for the connection type, make sure the filled in DCN parameters are correct!
- The total number of protected and managed network elements may not exceed the ITM-SC designed limit of 200 network element equivalents (GR Equivalents Maximum).
- A network element which is part of the Primary Domain of an ITM-SC can not also be part of the Protecting Domain of the same ITM-SC.
- A network element may only have two peers assigned to manage it. The two peer ITM-SCs are said to be the network element's Primary and Secondary ITM-SCs. This is because in the geographic redundancy Scheme an ITM-SC may have several peers but a network element will only have two ITM-SC assigned to manage it. It is important to note that the two ITM-SCs can NOT manage the network element at the same time.

□

Add Network Elements to the Geographic Redundancy Scheme

Follow these steps to appoint selected network elements to a secondary ITM-SC, adding them to the geographic redundancy scheme

1 Select *Management* --> *Geographic Redundancy* --> *NE Information*.

Result:

The *EMS - GR Network Element Information* window appears.

2 Click `Add`.

Result:

The *EMS - GR Add Protection* window appears.

3 Select the secondary ITM-SC from the list of *ITM-SC names* that act as peers to the ITM-SC.

Result:

The secondary ITM-SC is selected.

4 Select the network element from the list of names to be added to the selected peer ITM-SC and to be included in the geographic redundancy scheme.

Result:

The Secondary Gateway Address prompt window for that network element appears. When a network element has a diamond symbol next to it, the Secondary Gateway Address prompt window contains the address data that has been entered.

5 Set the Secondary Management connection as desired.

Result:

The Secondary Management parameters are set.

6 Click `OK` to confirm the current selections.

Result:

The Secondary Gateway Address prompt window disappears and the network element is provisioned for the secondary ITM-SC selected. On the Geographic Redundancy Add Protection window, this network element is marked with a “diamond” symbol.

7 Click `Apply`.

Result:

The selected network elements are placed within the geographic redundancy protection scheme, using the selected secondary ITM-SC.

8 Click `Close` to exit the *EMS - GR Add Protection* window.

Result:

The *EMS- GR Add Protection* window disappears.

9 Click `Close` to exit the *EMS - GR Network Element Information* window.

Result:

The *EMS - GR Network Element Information* window disappears.

END OF STEPS

□

Parameters for Adding Network Elements to the Geographic Redundancy Scheme

NE Name Displays the name of the network element.

Protection Domain

Protection Domain	Description
Show All NEs	Shows all network elements.
Show Protected NEs	Shows the network elements that are in the protected domain for the host ITM-SC and in the protecting domain for the highlighted peer ITM-SC.
Show Protecting NEs	Shows the network elements that are in the protecting domain for the host ITM-SC and in the protected domain for the highlighted peer ITM-SC.
Show Not Protected NEs	Shows the not protected network elements.

Management status Filter option to view network elements with a specific management status. The values are described in the table below:

Management status	Description
Show All States	Shows all network elements.
Show Expecting Management	Shows the network elements which the ITM-SC is currently attempting to manage.
Show actively Managed	Shows the network elements which the ITM-SC is currently managing.
Show no control	Shows the network elements which the ITM-SC is neither managing or expected to be managing.

Setup Status (Primary ITM-SC) Explains in which state the geographic redundancy of the network element is at any time. The setup statuses for the primary ITM-SC are

described in the table below:

Setup Status (Primary ITM-SC)	**Description**
Not Protected	This NE is not in the geographic redundancy scheme.
Protected	This NE is in the geographic redundancy scheme and is currently protected by a secondary ITM-SC.
Protected Disabled	This NE is in the geographic redundancy scheme, but the protection has been disabled. Protection can be re-enabled from the GR NE Information Screen.

Setup Status (Secondary ITM-SC)

Explains in which state the geographic redundancy of the network element is at any time. The setup statuses for the secondary ITM-SC are described in the table below:

Setup Status (Secondary ITM-SC)	**Description**
Protecting	This NE is in the geographic redundancy scheme and this ITM-SC is its secondary ITM-SC.
Protecting Disabled	This NE is in the geographic redundancy scheme, but the protection has been disabled. Protection can be re-enabled from the GR NE Information Screen.

Peer ITM-SC

Lists the names of the hosts with which the named NE (in the NE Name column) has peer to peer links.

Management Status

Explains the management status between the ITM-SC and the network element. The values are described in the table below:

Management Status	**Description**
Expecting Management	This ITM-SC is currently attempting to manage the NE.
Actively Managing	This ITM-SC is currently managing the NE.
No Control	This ITM-SC is neither managing or expected to be managing this NE.

Switch Status

Explains whether a switch has taken place and if so what type of switch. The values are described in the table below:

Switch Status	**Description**
Auto (Link Loss)	An automatic switch has taken place. The switch was caused by a failure of the peer to peer Link.
Auto (Assoc Loss)	An automatic switch has taken place. The switch was caused by a failure of association of between the primary ITM-SC and the NE.
Manual Switch	The user of the primary ITM-SC has performed a manual switch to the secondary ITM-SC.
No Switch	No switch has taken place. The primary ITM-SC has control of the NE.

Resynch State

Contains the resynch state for the communication between two ITM-SCs. The values are described in the table below:

Resynch State	**Description**
Resynching	Resynching database.
Normal	Database is stable.

Connection type

Controls network management data routing. The values are described in the table below:

Connection type	**Description**
Dynamic	Management data is routed dynamically. The ITM-SC chooses the most suitable Intermediate System (IS) on the Q-LAN through which it communicates with this network element.
Static	The management data route is forced. The management system uses a user-defined network element (Ethernet) address to select one Intermediate System (IS) via which the ITM-SC communicates with a node. This network element is referred to as the Gateway network element.

NE Connected Determines how the network element is connected. The values are described in the table below:

NE Connected	Description
Via Gateway	The network element is connected via a gateway node through which it is managed by the ITM-SC.
on LAN	The ITM-SC manages the network element directly through a Q-LAN connection.

Gateway Format Determines the format of the gateway via which this network element is managed. The values are described in the table below:

Gateway Format	Description
Ethernet	12 Hexadecimal digits.
Short	2 Hexadecimal digits.

Gateway Ethernet Address Address of the gateway via which this network element is managed. The format depends on setting of Gateway Format field.

□

Section: Removing Network Elements from the Geographic Redundancy Scheme

Overview

Purpose

Use this procedure to remove network elements from the geographic redundancy scheme. These network elements can not be protected by a Peer ITM-SC anymore.

When to perform

With geographic redundancy, a maximum of 200 network element equivalents can be managed by an ITM-SC. If this maximum has been reached, a network element that does not participate (anymore) in the geographic redundancy scheme of this ITM-SC has to be deleted to make it possible for another network element to join the Geograhic Redundancy scheme.

Related procedures

View Network Element Status.

Prerequisites

None.

Precautions

After removing network elements from the geographic redundancy scheme, these network elements can not be protected by a Peer ITM-SC anymore.

□

Remove Network Elements from the Geographic Redundancy Scheme

Follow these steps to remove selected network elements from the geographic redundancy Scheme.

Procesdures

1 Select *Management* --> *Geographic Redundancy* --> *NE Information*.

Result:

The *EMS - Geographic Redundancy Network Element Information* window appears.

2 Click `Remove`.

Result:

The *EMS - Geographic Redundancy Remove Protection* window appears.

3 Select the network element from the list of names to be removed. Multiple network elements can be selected at once on this window. Only one remove request needs to be made.

Result:

The selection of the network elements to be removed from the GR scheme is made.

4 Click the `OK` button.

Result:

When the protection for the selected NEs is removed successfully, the window will automatically disappear from the screen.

5 Select `Close` to exit the *EMS - GR Network Element Information* window.

Result:

The *EMS - GR Network Element Information* window disappears.

END OF STEPS

□

Parameters for Removing Network Elements from the Geographic Redundancy Scheme

NE Name Displays the name of the network element.

Protection Domain The protection domain is a filter option to view specific network elements of the protection domain. The values are described in the table below:

Protection Domain	**Description**
Show All NEs	Shows all network elements.
Show Protected NEs	Shows the network elements that are in the protected domain for the host ITM-SC and in the protecting domain for the highlighted peer ITM-SC.
Show Protecting NEs	Shows the network elements that are in the protecting domain for the host ITM-SC and in the protected domain for the highlighted peer ITM-SC.
Shows the not protected network elements.	Show Not Protected NEs

Management status Filter option to view network elements with a specific management status. The values are described in the table below:

Management status	**Description**
Show All States	Shows all network elements.
Show Expecting Management	Shows the network elements which the ITM-SC is currently attempting to manage.
Show actively Managed	Shows the network elements which the ITM-SC is currently managing.
Show no control	Shows the network elements which the ITM-SC is neither managing or expected to be managing.

Setup Status (Primary ITM-SC) Explains in which state the geographic redundancy of the network element is at any time. The setup statuses for the primary ITM-SC are

described in the table below:

Setup Status (Primary ITM-SC)	Description
Not Protected	This NE is not in the geographic redundancy scheme.
Protected	This NE is in the geographic redundancy scheme and is currently protected by a secondary ITM-SC.
Protected Disabled	This NE is in the geographic redundancy scheme, but the protection has been disabled. Protection can be re-enabled from the GR NE Information Screen.

Setup Status (Secondary ITM-SC)

Explains in which state the geographic redundancy of the network element is at any time. The setup statuses for the secondary ITM-SC are described in the table below:

Setup Status (Secondary ITM-SC)	Description
Protecting	This NE is in the geographic redundancy scheme and this ITM-SC is its secondary ITM-SC.
Protecting Disabled	This NE is in the geographic redundancy scheme, but the protection has been disabled. Protection can be re-enabled from the GR NE Information Screen.

Peer ITM-SC

Lists the names of the hosts with which the named NE (in the NE Name column) has peer to peer links.

Management Status

Explains the management status between the ITM-SC and the network element. The values are described in the table below:

Management Status	Description
Expecting Management	This ITM-SC is currently attempting to manage the NE.
Actively Managing	This ITM-SC is currently managing the NE.
No Control	This ITM-SC is neither managing or expected to be managing this NE.

Switch Status Explains whether a switch has taken place and if so what type of switch. The values are described in the table below:

Switch Status	Description
Auto (Link Loss)	An automatic switch has taken place. The switch was caused by a failure of the peer to peer Link.
Auto (Assoc Loss)	An automatic switch has taken place. The switch was caused by a failure of association of between the primary ITM-SC and the NE.
Manual Switch	The user of the primary ITM-SC has performed a manual switch to the secondary ITM-SC.
No Switch	No switch has taken place. The primary ITM-SC has control of the NE.

Resynch State Contains the resynch state for the communication between two ITM-SCs. The values are described in the table below:

Resynch State	Description
Resynching	Resynching database.
Normal	Database is stable.

□

Section: Enabling or Disabling Protection of Network Elements

Overview

Purpose

Purpose of enabling protection of network elements: To increase the overall reliability of network management, network elements can be protected by a peer ITM-SC.

Purpose of disabling protection of network elements: To disable management protection of network elements which participate in the geographic redundancy scheme. In case of a failure in the primary ITM-SC, the secondary ITM-SC will not take over.

When to perform

Enabling protection of network elements: To include a network element in the geographic redundancy scheme from which it temporary has been excluded. In that case protection has to be set to enabled again to make it possible for a peer ITM-SC to take over management in case of a failure in the primary ITM-SC.

Disabling protection of network elements: When a network element no longer has to be protected within the geographic redundancy scheme.

Related procedures

Related procedures when enabling the protection of network elements:

- View Network Element Status.
- Provisioning the Data Communications Channel.
- Performing the Data Communications Test.

Prerquisites

Related procedures when disabling the protection of network elements:

- View Network Element Status.
- Display Protected Network Elements.

Prerequisites when enabling the protection of network elements are:

- The Ne to be added should be provisioned.
- The Ne to be added should be reachable by this ITM-SC in the OSI-DCN.

Precautions

Pay attention to the following when enabling the protection of network elements: The total number of protected and managed network elements may not exceed the ITM-SC designed limit of 200 equivalents (GR Equivalents Maximum).

Pay attention to the following when disabling the protection of network elements: After disabeling the protection of a network element, the secondary ITM-SC will NOT take over management in case of a failure in the primary ITM-SC.

□

Enable or Disable Protection of Network Elements

Follow these steps to enable or disable the protection of selected network elements:

Procedures

1 Select *Management* --> *Geographic Redundancy* --> *NE Information*.

Result:

The main *EMS - GR Network Element Information* window appears.

2 Click `Enable` or `Disable`.

Result:

The *EMS - GR Amend Protection* window appears.

3 Select one or more network elements from the list of network element names for which GR protection should be enabled or disabled.

Result:

The network elements for which GR protection should be enabled or disabled are selected.

4 Click `OK` to confirm the enabling or disabling of the selected network elements.

Result:

If all the selected NEs are enabled or disabled successfully, the GR Amend Protection window disappears.

5 Click `Close` to exit the *EMS - GR Network Element Information* window.

Result:

The *EMS - GR Network Element Information* window disappears.

END OF STEPS

□

Parameters for Enabling or Disabling Protection of Network Elements

Protection Domain

The protection domain is a filter option to view specific network elements of the protection domain. The values are described in the table below:

Protection Domain	Description
Show All NEs	Shows all network elements.
Show Protected NEs	Shows the network elements that are in the protected domain for the host ITM-SC and in the protecting domain for the highlighted peer ITM-SC.
Show Protecting NEs	Shows the network elements that are in the protecting domain for the host ITM-SC and in the protected domain for the highlighted peer ITM-SC.
Show Not Protected NEs	Shows the not protected network elements.

Management status

Filter option to view network elements with a specific management status. The values are described in the table below:

Management status	Description
Show All States	Shows all network elements.
Show Expecting Management	Shows the network elements which the ITM-SC is currently attempting to manage.
Show actively Managed	Shows the network elements which the ITM-SC is currently managing.
Show no control	Shows the network elements which the ITM-SC is neither managing or expected to be managing.

NE Name

Displays the name of the network element.

Setup Status (Primary ITM-SC)

Explains in which state the geographic redundancy of the network element is at any time. The setup statuses for the primary ITM-SC are

described in the table below:

Setup Status (Primary ITM-SC)	Description
Not Protected	This NE is not in the geographic redundancy scheme.
Protected	This NE is in the geographic redundancy scheme and is currently protected by a secondary ITM-SC.
Protected Disabled	This NE is in the geographic redundancy scheme, but the protection has been disabled. Protection can be re-enabled from the GR NE Information Screen.

Setup Status (Secondary ITM-SC) Explains in which state the geographic redundancy of the network element is at any time. The setup statuses for the secondary ITM-SC are described in the table below:

Setup Status (Secondary ITM-SC)	Description
Protecting	This NE is in the geographic redundancy scheme and this ITM-SC is its secondary ITM-SC.
Protecting Disabled	This NE is in the geographic redundancy scheme, but the protection has been disabled. Protection can be re-enabled from the GR NE Information Screen.

Peer ITM-SC Lists the names of the hosts with which the named NE (in the NE Name column) has peer to peer links.

Management Status Explains the management status between the ITM-SC and the network element. The values are described in the table below:

Management Status	Description
Expecting Management	This ITM-SC is currently attempting to manage the NE.
Actively Managing	This ITM-SC is currently managing the NE.
No Control	This ITM-SC is neither managing or expected to be managing this NE.

Switch Status Explains whether a switch has taken place and if so what type of switch. The values are described in the table below:

Switch Status	Description
Auto (Link Loss)	An automatic switch has taken place. The switch was caused by a failure of the peer to peer Link.
Auto (Assoc Loss)	An automatic switch has taken place. The switch was caused by a failure of association of between the primary ITM-SC and the NE.
Manual Switch	The user of the primary ITM-SC has performed a manual switch to the secondary ITM-SC.
No Switch	No switch has taken place. The primary ITM-SC has control of the NE.

□

Section: Displaying Protected Network Elements

Overview

Purpose

This procedure displays the network elements that are protected in the geographic redundancy scheme by a specific peer ITM-SC. The current protection switch status is also displayed.

When to perform

Use this procedure to view the above mentioned information about the network elements that are protected by a peer ITM-SC in the geographic redundancy scheme.

Related procedures

None.

Prerquisites

None.

Precautions

None.

□

Display Protected Network Elements

Follow these steps to list the ITM-SC NEs that protected by a peer ITM-SC:

Procedures

1 Select *Management* --> *Geographic Redundancy* --> *Manager Information*.

Result:

The *EMS* - *GR Manager Information* window appears.

2 Select the peer *ITM-SC Name* for which to display the list of protected network elements.

Result:

A selection is made.

3 Click `Protected NE View`.

Result:

The *EMS* - *GR Network Element List* window appears.

4 Click `Close` to exit the *EMS* - *GR Manager Information* window.

Result:

The *EMS* - *GR Manager Information* window disappears.

5 Click `Close` to exit the *EMS* - *GR Network Element List* window.

Result:

The *EMS* - *GR Network Element List* window disappears.

END OF STEPS

□

Parameters for Displaying Protected Network Elements

ITM-SC Name The name of the peer ITM-SC connected to the host ITM-SC.

Location The location of the ITM-SC server.

Link Status Contains the status of the peer to peer Link between the two ITM-SCs. The values are described in the table below:

Link Status	Description
Link Established	The link exists and is running correctly.
Link Not Established	The ITM-SCs are currently attempting to set up the link for the first time.
Link Failed Version Check	A link cannot be established because the two ITM-SC managers are running different versions of the software, or they use different versions of the ITM-SC database.

Resynch State Contains the resynch state for the communication between two ITM-SCs. The values are described in the table below:Contains the resynch state for the communication between two ITM-SCs. The values are described in the table below:

Resynch State	Description
Resynching	Resynching database.
Normal	Database is stable.

NE Name Displays the name of the network element.

Switch Status Explains whether a switch has taken place and if so what type of switch. The values are described in the table below:

Switch Status	Description
Auto (Link Loss)	An automatic switch has taken place. The switch was caused by a failure of the Peer to Peer Link.
Auto (Assoc Loss)	An automatic switch has taken place. The switch was caused by a failure of association of between the Primary ITM-SC and the NE.

Switch Status	Description
Auto Switch	The user of the Primary ITM-SC has performed a manual switch to the Secondary ITM-SC.
No Switch	No switch has taken place. The Primary ITM-SC has control of the NE.

□

Section: Displaying Protecting Network Elements

Overview

Purpose

This procedure displays the network elements owned by a peer ITM-SC that are being protected by this ITM-SC. The current protection switch status is also displayed.

When to perform

If you want to view which network elements are being protected by this ITM-SC and what the current protection switch status is.

Related procedures

None.

Prerquisites

None.

Precautions

None.

□

Display Protecting Network Elements

Follow these steps to list the ITM-SC NEs that are protected by a peer ITM-SC:

Procedures

1 Select *Management* --> *Geographic Redundancy* --> *Manager Information*.

Result:

The *EMS - GR Manager Information* window appears.

2 Select the peer *ITM-SC Name* for which to display the list of protecting network elements.

Result:

A selection is made.

3 Click `Protecting NE View`.

Result:

The *EMS - GR Network Element List* window appears.

4 Click `Close` to exit the *EMS - GR Network Element List* window.

Result:

The *EMS - GR Network Element List* window disappears.

5 Click `Close` to exit the *EMS - GR Manager Information* window.

Result:

The *EMS - GR Manager Information* window disappears.

END OF STEPS

□

Parameters for Displaying Protecting Network Elements

ITM-SC Name The name of the peer ITM-SC connected to the host ITM-SC.

Location The location of the ITM-SC server.

Link Status

Contains the status of the peer to peer Link between the two ITM-SCs. The values are described in the table below:

Link Status	Description
Link Established	The link exists and is running correctly.
Link Not Established	The ITM-SCs are currently attempting to set up the link for the first time.
Link Failed Version Check	A link cannot be established because the two ITM-SC managers are running different versions of the software, or they use different versions of the ITM-SC database.

Resynch State Contains the resynch state for the communication between two ITM-SCs. The values are described in the table below:

Resynch State	Description
Resynching database.	Resynching
Normal	Database is stable.

NE Name Displays the name of the network element.

Switch Status Explains whether a switch has taken place and if so what type of switch. The values are described in the table below:

Switch Status	Description
Auto (Link Loss)	An automatic switch has taken place. The switch was caused by a failure of the Peer to Peer Link.
Auto (Assoc Loss)	An automatic switch has taken place. The switch was caused by a failure of association of between the Primary ITM-SC and the NE.

Switch Status	Description
Manual Switch	The user of the Primary ITM-SC has performed a manual switch to the Secondary ITM-SC.
No Switch	No switch has taken place. The Primary ITM-SC has control of the NE.

□

Section: Transferring Network Element Control to the Secondary ITM-SC

Overview

Purpose

Use this procedure to transfer network element management to the secondary ITM-SC. The primary ITM-SC will no longer be actively managing this network element.

When to perform

Network element management can be transferred to the secondary ITM-SC when the primary ITM-SC can not be used to continue managing the network element. This can be the case when maintenance has to be done that will disable the primary ITM-SC or management communication between the primary ITM-SC and the network element.

Related procedures

Related Procedures are:

- Display Protected Network Elements.
- Display Protecting Network Elements.

Prerequisites

None.

Precautions

None.

□

Transfer Network Element Control to the Secondary ITM-SC

Follow these steps to transfer control of selected network elements to their secondary ITM-SCs:

Procedures

1 Select *Management* --> *Geographic Redundancy* --> *NE Information*.

Result:

The *EMS - Geographic Redundancy Network Element Information* window appears.

2 Click `Switch`.

Result:

The *EMS - Geographic Redundancy Manual Transfer* window appears.

3 Select one or more network elements from the list of names for which control will be transferred to the secondary ITM-SC.

Result:

A selection is made.

4 Click `OK` to confirm the switch request for the selected network elements.

Result:

If control of all selected network elements has been transferred successfully to the secondary ITM-SC, the *EMS - Geographic Redundancy Manual Transfer* window disappears.

5 Click `Close` to exit the *EMS - Geographic Redundancy Network Element Information* window.

Result:

The *EMS - Geographic Redundancy Network Element Information* window disappears.

END OF STEPS

□

Parameters for Transferring Network Element Control to the Secondary ITM-SC

Protection Domain

The protection domain is a filter option to view specific network elements of the protection domain. The values are described in the table below:

Protection Domain	Description
Show All NEs	Shows all network elements.
Show Protected NEs	Shows the network elements that are in the protected domain for the host ITM-SC and in the protecting domain for the highlighted peer ITM-SC.
Show Protecting NEs	Shows the network elements that are in the protecting domain for the host ITM-SC and in the protected domain for the highlighted peer ITM-SC.
Show Not Protected NEs	Shows the not protected network elements.

Management status

Filter option to view network elements with a specific management status. The values are described in the table below:

Management status	Description
Show All States	Shows all network elements.
Show Expecting Management	Shows the network elements which the ITM-SC is currently attempting to manage.
Show actively Managed	Shows the network elements which the ITM-SC is currently managing.
Show no control	Shows the network elements which the ITM-SC is neither managing or expected to be managing.

NE Name

Displays the name of the network element.

Setup Status (Primary ITM-SC)

Explains in which state the geographic redundancy of the network element is at any time. The setup statuses for the primary ITM-SC are

described in the table below:

Setup Status (Primary ITM-SC)	**Description**
Not Protected	This NE is not in the geographic redundancy scheme.
Protected	This NE is in the geographic redundancy scheme and is currently protected by a secondary ITM-SC.
Protected Disabled	This NE is in the geographic redundancy scheme, but the protection has been disabled. Protection can be re-enabled from the GR NE Information Screen.

Setup Status (Secondary ITM-SC)

Explains in which state the geographic redundancy of the network element is at any time. The setup statuses for the secondary ITM-SC are described in the table below:

Setup Status (Secondary ITM-SC)	**Description**
Protecting	This NE is in the geographic redundancy scheme and this ITM-SC is its secondary ITM-SC.
Protecting Disabled	This NE is in the geographic redundancy scheme, but the protection has been disabled. Protection can be re-enabled from the GR NE Information Screen.

Peer ITM-SC

Lists the names of the hosts with which the named NE (in the NE Name column) has peer to peer links.

Management Status

Explains the management status between the ITM-SC and the network element. The values are described in the table below:

Management Status	**Description**
Expecting Management	This ITM-SC is currently attempting to manage the NE.
Actively Managing	This ITM-SC is currently managing the NE.
No Control	This ITM-SC is neither managing or expected to be managing this NE.

Switch Status Explains whether a switch has taken place and if so what type of switch. The values are described in the table below:

Switch Status	Description
Auto (Link Loss)	An automatic switch has taken place. The switch was caused by a failure of the peer to peer Link.
Auto (Assoc Loss)	An automatic switch has taken place. The switch was caused by a failure of association of between the primary ITM-SC and the NE.
Manual Switch	The user of the primary ITM-SC has performed a manual switch to the secondary ITM-SC.
No Switch	No switch has taken place. The primary ITM-SC has control of the NE.

Resynch State Contains the resynch state for the communication between two ITM-SCs. The values are described in the table below:

Resynch State	Description
Resynching	Resynching database.
Normal	Database is stable.

□

Section: Returning Network Element Control to the Primary ITM-SC

Overview

Purpose

Use this procedure to return network element control to the primary ITM-SC. The secondary ITM-SC will no longer be actively managing this network element.

When to perform

When the secondary ITM-SC has been managing the network element and the primary ITM-SC is available again to resume the managing of this network element.

Related procedures

Related Procedures are:

- Display Protected Network Elements.
- Display Protecting Network Elements.

Prerquisites

None.

Precautions

None.

□

Return Network Element Control to the Primary ITM-SC

Follow these steps to select one or multiple network elements and direct them to send a message to their respective secondary ITM-SCs to return control to the primary ITM-SC:

Procedures

1 Select *Management* --> *Geographic Redundancy* --> *NE Information*.

Result:

The *EMS - Geographic Redundancy Network Element Information* window appears.

2 Click `Retrieve`.

Result:

The *EMS - Geographic Redundancy Return Control* window appears.

3 Select one or more network elements from the list of names from which the control information should be displayed and changed.

Result:

A selection is made.

4 Click `OK` to confirm the receive control request for the selected network elements.

Result:

If control for all selected network elements is received successfully, the *EMS - Geographic Redundancy Return Control* window disappears.

5 Click `Close` to exit the *EMS - Geographic Redundancy Network Element Information* window.

Result:

The *EMS - Geographic Redundancy Network Element Information* window disappears.

END OF STEPS

□

Parameters for Returning Network Element Control to the Primary ITM-SC

Protection Domain

The protection domain is a filter option to view specific network elements of the protection domain. The values are described in the table below:

Protection Domain	**Description**
Show All NEs	Shows all network elements.
Show Protected NEs	Shows the network elements that are in the protected domain for the host ITM-SC and in the protecting domain for the highlighted peer ITM-SC.
Show Protecting NEs	Shows the network elements that are in the protecting domain for the host ITM-SC and in the protected domain for the highlighted peer ITM-SC.
Show Not Protected NEs	Shows the not protected network elements.

Management status

Filter option to view network elements with a specific management status. The values are described in the table below:

Management status	**Description**
Show All States	Shows all network elements.
Show Expecting Management	Shows the network elements which the ITM-SC is currently attempting to manage.
Show actively Managed	Shows the network elements which the ITM-SC is currently managing.
Show no control	Shows the network elements which the ITM-SC is neither managing or expected to be managing.

NE Name

Displays the name of the network element.

Setup Status (Primary ITM-SC)

Explains in which state the geographic redundancy of the network element is at any time. The setup statuses for the primary ITM-SC are described in the table below:

Setup Status (Primary ITM-SC)	Description
Not Protected	This NE is not in the geographic redundancy scheme.
Protected	This NE is in the geographic redundancy scheme and is currently protected by a secondary ITM-SC.
Protected Disabled	This NE is in the geographic redundancy scheme, but the protection has been disabled. Protection can be re-enabled from the GR NE Information Screen.

Setup Status (Secondary ITM-SC)

Explains in which state the geographic redundancy of the network element is at any time. The setup statuses for the secondary ITM-SC are described in the table below:

Setup Status (Secondary ITM-SC)	Description
Protecting	This NE is in the geographic redundancy scheme and this ITM-SC is its secondary ITM-SC.
Protecting Disabled	This NE is in the geographic redundancy scheme, but the protection has been disabled. Protection can be re-enabled from the GR NE Information Screen.

Peer ITM-SC

Lists the names of the hosts with which the named NE (in the NE Name column) has peer to peer links.

Management Status

Explains the management status between the ITM-SC and the network element. The values are described in the table below:

Management Status	Description
Expecting Management	This ITM-SC is currently attempting to manage the NE.
Actively Managing	This ITM-SC is currently managing the NE.

Management Status	Description
No Control	This ITM-SC is neither managing or expected to be managing this NE.

Switch Status

Explains whether a switch has taken place and if so what type of switch. The values are described in the table below:

Switch Status	Description
Auto (Link Loss)	An automatic switch has taken place. The switch was caused by a failure of the peer to peer Link.
Auto (Assoc Loss)	An automatic switch has taken place. The switch was caused by a failure of association of between the primary ITM-SC and the NE.
Manual Switch	The user of the primary ITM-SC has performed a manual switch to the secondary ITM-SC.
No Switch	No switch has taken place. The primary ITM-SC has control of the NE.

Resynch State

Contains the resynch state for the communication between two ITM-SCs. The values are described in the table below:

Resynch State	Description
Resynching	Resynching database.
Normal	Database is stable.

□

Section: Editing the Gateway Address

Overview

Purpose

Use this procedure to edit the parameters for the management communication between the network element and the secondary ITM-SC.

When to perform

When the management communication between the network element and the secondary ITM-SC has to be routed differently.

Related procedures

Related procedures are:

- Provision a Network Element from a Template.
- Create a pre-provisioned Network Element.
- View Network Element Status.
- Provisioning the Data Communications Channel.
- Performing the Data Communications Test.

Prerquisites

Prerequisites for the procedure are:

- The NE must be provisioned.
- The NE must be reachable by this ITM-SC in the OSI-DCN.

Precautions

Pay attention to the following:

- When the static value is chosen for the connection type, make sure the filled in DCN parameters are correct!
- The secondary gateway address can only be edited on the secondary ITM-SC when the Management Control Status of the NE is *Expecting Management* and the peer link is down.

Note

The gateway address can be changed on the primary ITM-SC by removing the NE from the GR protection scheme and adding the NE again with different parameters.

□

Edit the Gateway Address

Follow these steps to edit the Gateway Address of selected network elements:

Procedure

1 Select *Management* --> *Geographic Redundancy* --> *NE Information*.

Result:

The *EMS - GR Network Element Information* window appears.

2 Select `Gateway`.

Result:

The *EMS - GR Edit Gateway Address* window appears.

3 Select the network element for which the Gateway Address needs to be changed.

Result:

The *EMS - Edit GR Network Element Address* window for that NE appears.

4 Set the Secondary Management connection as desired.

Result:

The Secondary Management parameters are set.

5 Click `OK` to confirm the current selections.

Result:

The *EMS - Edit GR Network Element Address* window disappears and the network element is provisioned for the secondary ITM-SC selected. On the Geographic Redundancy Add Protection window, this network element is marked with a diamond symbol.

6 Click `Close` to exit the *EMS - GR Network Element Information* window.

Result:

the *EMS - GR Network Element Information* window disappears.

END OF STEPS

□

Parameters for Editing of the Gateway Address

Protection Domain

The protection domain is a filter option to view specific network elements of the protection domain. The values are described in the table below:

Protection Domain	Description
Show All NEs	Shows all network elements.
Show Protected NEs	Shows the network elements that are in the protected domain for the host ITM-SC and in the protecting domain for the highlighted peer ITM-SC.
Show Protecting NEs	Shows the network elements that are in the protecting domain for the host ITM-SC and in the protected domain for the highlighted peer ITM-SC.
Show Not Protected NEs	Shows the not protected network elements.

Management status

Filter option to view network elements with a specific management status. The values are described in the table below:

Management status	Description
Show All States	Shows all network elements.
Show Expecting Management	Shows the network elements which the ITM-SC is currently attempting to manage.
Show actively Managed	Shows the network elements which the ITM-SC is currently managing.
Show no control	Shows the network elements which the ITM-SC is neither managing or expected to be managing.

NE Name

Displays the name of the network element.

Setup Status (Primary ITM-SC)

Explains in which state the geographic redundancy of the network element is at any time. The setup statuses for the primary ITM-SC are

described in the table below:

Setup Status (Primary ITM-SC)	Description
Not Protected	This NE is not in the geographic redundancy scheme.
Protected	This NE is in the geographic redundancy scheme and is currently protected by a secondary ITM-SC.
Protected Disabled	This NE is in the geographic redundancy scheme, but the protection has been disabled. Protection can be re-enabled from the GR NE Information Screen.

Setup Status (Secondary ITM-SC)

Explains in which state the geographic redundancy of the network element is at any time. The setup statuses for the secondary ITM-SC are described in the table below:

Setup Status (Secondary ITM-SC)	Description
Protecting	This NE is in the geographic redundancy scheme and this ITM-SC is its secondary ITM-SC.
Protecting Disabled	This NE is in the geographic redundancy scheme, but the protection has been disabled. Protection can be re-enabled from the GR NE Information Screen.

Peer ITM-SC

Lists the names of the hosts with which the named NE (in the NE Name column) has peer to peer links.

Management Status

Explains the management status between the ITM-SC and the network element. The values are described in the table below:

Management Status	Description
Expecting Management	This ITM-SC is currently attempting to manage the NE.
Actively Managing	This ITM-SC is currently managing the NE.
No Control	This ITM-SC is neither managing or expected to be managing this NE.

Switch Status Explains whether a switch has taken place and if so what type of switch. The values are described in the table below:

Switch Status	Description
Auto (Link Loss)	An automatic switch has taken place. The switch was caused by a failure of the peer to peer Link.
Auto (Assoc Loss)	An automatic switch has taken place. The switch was caused by a failure of association of between the primary ITM-SC and the NE.
Manual Switch	The user of the primary ITM-SC has performed a manual switch to the secondary ITM-SC.
No Switch	No switch has taken place. The primary ITM-SC has control of the NE.

Resynch State Contains the resynch state for the communication between two ITM-SCs. The values are described in the table below:

Resynch State	Description
Resynching	Resynching database.
Normal	Database is stable.

Connection type Controls network management data routing. The values are described in the table below:

Connection type	Description
Dynamic	Management data is routed dynamically. The ITM-SC chooses the most suitable Intermediate System (IS) on the Q-LAN through which it communicates with this network element.
Static	The management data route is forced. The management system uses a user-defined network element (Ethernet) address to select one Intermediate System (IS) via which the ITM-SC communicates with a node. This network element is referred to as the Gateway network element.

NE Connected Determines how the network element is connected. The values are described in the table below:

NE Connected	Description
Via Gateway	The network element is connected via a gateway node through which it is managed by the ITM-SC.
on LAN	The ITM-SC manages the network element directly through a Q-LAN connection.

Gateway Format Determines the format of the gateway via which this network element is managed. The values are described in the table below:

Gateway Format	Description
Ethernet	12 Hexadecimal digits.
Short	2 Hexadecimal digits.

Gateway Ethernet Address Address of the gateway via which this network element is managed. The format depends on setting of Gateway Format field.

□

7 Management Communication of the ITM-SC

Overview

Purpose

This chapter describes taks to set or change the address of the ITM-SC in a network.

Abbreviations used

When Network Elements OLS 80G, ADM 4/1, ADM 16/1, ADM16/1c, AM 1 (Plus) and TM 1 are described WaveStar®OLS 80 G, WaveStar®ADM 4/1, WaveStar® ADM 16/1, WaveStar® ADM16/1 compact, WaveStar® AM 1 (Plus) and WaveStar® TM 1 are meant.

□

Section: Maintaining Network Addresses

Overview

Purpose The purpose of this procedure is to set the network address of the ITM-SC within the management data communications network (DCN).

□

Maintain Network Addresses

When to perform

The ITM-SC is connected to the data communications network thus must belong to an area. The label of an area, the area ID of the ITM-SC, is set by the administrator of the ITM-SC. Use this procedure to assigning the ITM-SC to an area.

Before you begin

Before performing this procedure make sure:

- a DCN plan available
- the ITM-SC Area is known

Before performing this procedure consider the following:

- In case the DCN is divided into areas make sure you assign the ITM-SC to an area with at least one level 2 node in it. Otherwise there is no connectivity between the ITM-SC and the NEs in the other areas in the DCN.
- This procedure can only be performed when the ITM-SC application is stopped (shutdown).
- Whenever the area ID is incorrect NE management will fail.

Related information

Related procedures are:

- Change general NE information
- Create a MIB image from an NE
- Provision an NE from template
- Create a pre-provisioned NE

The related concept is:

- Overview of Maintaining Network Addresses [10-37]

Parameters used in this procedure can be found at Parameters for Maintaining Network Addresses [7-5].

Procedure

Follow these steps to set the network address of the ITM-SC within the DCN:

1 Click the *DCN Data* icon from the *ITM-SC Administration* menu.

Result:

The *ITM-SC DCN Data Information* window appears.

2 Click `Edit`.

Result:

The *ITM-SC DCN Data Edit* window appears.

3 Select the desired *NSAP format*.

Result:

The NSAP format is selected.

4 Depending on the chosen NSAP format fill in the *Area ID* or *Area Address*.

Result:

The *Area ID* or *Area Address* is filled in.

5 Click `OK` to confirm the current changes.

Result:

The changes are now stored.

END OF STEPS

□

Parameters for Maintaining Network Addresses

SID The SID (System ID) is taken from the Ethernet address of the OSI LAN card or one of the OSI LAN cards when more LAN cards are present.

NSAP Format The NSAP address of the ITM-SC is its DCN wide identifier which uniquely identifies the ITM-SC in the network. The different formats are described in the table below. The default value is Fixed 20 bytes.

NSAP format	Description
Fixed 20 byte	40 hexadecimal digits.
Fixed 10 byte	20 hexadecimal digits.
Flexible	Else (16 - 40 hexadecimal digits).

Area The Area indicates the area to which the ITM-SC belongs and thus its logical location in the network.

The Area is indicated for the

- *fixed 20* byte NSAP format in 4 hexadecimal digits (2 bytes)
- *fixed 10* byte NSAP format in 4 hexadecimal digits (2 bytes)
- *flexible NSAP* format in 2 - 26 hexadecimal digits (1-13 bytes). Note that only an even number of digits is allowed.

OSI Stack Mode Displays the OSI stack mode which can be:

- Single LAN ES-IS (one LAN card is present)
- Single LAN, IS-IS (more LAN cards are present)
- Multi LAN, IS-IS (more LAN cards are present)

□

8 Trouble Clearing

Overview

Purpose This chapter provides help when the ITM-SC system is halted or interrupted in its normal operation. Tasks to investigate the cause of the problems such as viewing events, ITM-SC Logs and Operator Logs are provided as well.

Content Subjects described in this chapter are:

- restoring the ITM-SC database
- performing a MIB upload and download
- viewing events
- using ITM-SC Log and Operator Log files

Abbreviations used When Network Elements OLS 80G, ADM 4/1, ADM 16/1, ADM16/1c, AM 1 (Plus) and TM 1 are described WaveStar®OLS 80 G, WaveStar®ADM 4/1, WaveStar® ADM 16/1, WaveStar® ADM16/1 compact, WaveStar® AM 1 (Plus) and WaveStar® TM 1 are meant.

□

Section: Restoring the ITM-SC Database

Overview

Purpose This procedure describes how to restore the ITM-SC database.

□

Restoring the ITM-SC Database

When to use To restore the ITM-SC its database as saved on disk.

Before you begin Before performing this procedure make sure:

- The ITM-SC application is stopped (shutdown)
- The INFORMIX password is known. The default password is the same as the root password. This password can be changed by performing the procedure as described in the Sub-network Installation Guide (SIG)

Before performing this procedure consider the following precaution:

- Do NOT close the restore window while a database archive process is still in progress, wait until the operation is finished.

Related information Related procedures are:

- Backing Up the ITM-SC Database
- Managing ITM-SC Database Archives
- Backing up the Entire ITM-SC System
- Restoring the Entire ITM-SC System

The related concept is:

- ITM-SC Database [10-33]

Procedure Follow these steps to restore the ITM-SC database:

1 Select the *Backup/Restore Database* icon from the *ITM-SC Administration* menu.

Result:

The *ITM-SC Database Control* window is displayed.

2 Select `Restore`.

Result:

The ITM-SC restore process starts. A HP-UX Terminal window is displayed with the following lines:

`Do you want automatic association after the database has been restored (y/n [n])?` is displayed.

3 Select either `y` or `n`.

y(es) means that on association, the MIB Image in the ITM-SC is re synchronized with the NE's MIB. Any changes made to the NE since the ITM-SC database archive was made will be automatically copied into the ITM-SC MIB Image. This does not affect the NE so is NOT traffic affecting.

n(o) means that the network will be restored back to the database that existed when the last database archive was made. Each NE has to be forced back to it's previous condition by downloading the MIB Image into each NE. Depending on the changes that have been made to each NE since the last database archive was made, this can affect the operation of the NE. The download could potentially affect traffic.

Result:

The message `Do you want to restore old Alarm and PM data? (y/n [n]):` is displayed.

4 Select either `y` or `n`.

Result:

The user is asked the following:

```
Do you wish to specify a remote host to
restore from? (y,n[n])
```

5 Select either `y` or `n`.

Result:

If selecting y(es) a list of remote hosts will be displayed.

6 If selected y(es) the previous step, enter a corresponding number to the host to restore from.

Result:

The user is asked to restore from disk. Tape is default.

7 Select either `y` or `n`.

Result:

The user is asked if to specify the directory where the archive is held. A list of archives is displayed.

8 Select a file to restore. Wait the system to finish the operation

Result:

The database is being restored.

9 When the message `Press <return> to Continue...` is displayed, press **RETURN**.

10 Enter `Exit` to complete the procedure.

Result:

The HP-UX Terminal window closes.

END OF STEPS

□

Section: Restoring the Entire ITM-SC System

Overview

Purpose The following procedures describe how to restore a previously saved configuration on server/stand-alone and client completely. Two procedures are provided: one for restoring the server/stand-alone and one for restoring the client.

□

Restore Entire ITM-SC System on Server/Standalone

When to use

To restore a Server or Stand-alone ITM-SC as saved. This includes all necessary data.

Before you begin

Before performing this procedure make sure:

- The ITM-SC is stopped (shutdown)
- the correct password, hostname and IP address are used. This will be essential because this procedure will restore host file and password information.
- the same release of the IMT-SC and the same NIS configuration are used.

Related information

Related procedures are:

- Restore Entire ITM-SC System on Client
- Backing Up the ITM-SC Database
- Restoring the ITM-SC Database
- Managing ITM-SC Database Archives
- Backing up the Entire ITM-SC System

The related concept is:

- ITM-SC Database [10-33]

Procedure

Follow these steps to restore the server/standalone. The ITM-SC does not need to be licensed because this will be restored automatically.

1 Follow the clean install procedure and install the ITM-SC in the same way that is was initially configured.

2 Restore the Informix database by the Restoring the ITM-SC Database procedure.

3 Login as *Root* via the *UNIX Terminal* window.

4 Place the tape labelled “Server Backup *hostname*” into the tape drive of the server/standalone and enter the following command: `itmsc_restore`. Press **ENTER**.

Result:

After the files have been copied from tape the ITM-SC will automatically restart.

5 Remove the tape and log out from *Root* to complete the procedure.

END OF STEPS

□

Restore Entire ITM-SC System on Client

When to use

To restore a Client ITM-SC as saved. This includes all necessary data.

Before you begin

Before performing this procedure make sure:

- The same release of the IMT-SC and the same NIS configuration should be used.
- the correct password, hostname and IP address are used. This will be essential because this procedure will restore host file and password information.

Related information

Related procedures are:

- Restore Entire ITM-SC System on Server/Standalone
- Backing Up the ITM-SC Database
- Restoring the ITM-SC Database
- Managing ITM-SC Database Archives
- Backing up the Entire ITM-SC System

The related concept is:

- ITM-SC Database [10-33]

Procedure

Follow these steps to restore the client. The Client ITM-SC does not have to be stopped.

1 Follow the clean install procedure and install the ITM-SC in the same way that is was initially configured.

2 Login as *Root* via the *Unix Terminal* window.

3 Place the tape “Client *hostname*” into the tape drive of the client and enter the following command: `itmsc_restore`. Press **ENTER**.

4 After the files have been copied from tape remove the tape and log out from *Root* to complete the procedure.

END OF STEPS

□

Section: Performing a MIB Upload

Overview

Purpose The purpose of this procedure is to upload the Management Information Base (MIB) of a provisioned network element to the ITM-SC.

□

Perform a MIB Upload

When to use

Use this procedure to synchronize the databases when a difference between the MIB image of the ITM-SC and the MIB of the network element is expected. The MIB image of the ITM-SC is overwritten with the MIB contents of the network element.

Before you begin

Before MIB upload can start, the following prerequisites must be met:

- The network element must have a valid MIB.
- On the ITM-SC a MIB image must be present.

Before performing this procedure consider the following precaution

- The MIB image in the ITM-SC will be overwritten by the MIB of the network element.

Related information

Related procedures are:

- Creating network element.
- View network element status: To monitor the status of the association to the network elements.
- Backup / restore: After a restore, when the automatic association option is not chosen. The user then has the option for MIB download or MIB upload for each network element individually.
- Manage Associations.

Procedure

To perform a MIB upload follow this procedure:

1 Select *Management* --> *MIB Upload*.

Result:

The *EMS - MIB Upload* window appears.

2 To select a provisioned NE or to switch to another provisioned NE, click the Selection Dialog Button. A list of possible NEs then appears in the *EMS- NE Selection Dialog* window. Select the desired NE and click `OK`

Result:

The *EMS - MIB Upload* window appears again with the selected NE displayed in it.

3 Click `Apply`.

Result:

A confirmation window appears to warn the user about the consequences of this action and to ask to continue or not.

4 Click `Yes.`

Result:

In the message box Operation Started is displayed. If the MIB upload is executed the message Operation Successful will be displayed. Otherwise Operation Failed will be displayed.

5 Click `Close.`

Result:

The *EMS* - *MIB Upload* window disappears.

END OF STEPS

□

Section: Performing a MIB Download

Overview

Purpose The purpose of this procedure is to download the Management Information Base (MIB) image of a provisioned network element from the ITM-SC database to the network element.

□

Perform a MIB Download

When to use

Use this procedure:

- To synchronize the network elements and ITM-SCs database when the MIB of the network element is corrupted.
- After an ITM-SC restore.

The specified node's MIB image in the ITM-SC is downloaded to the network element, overwriting the network element MIB with the data defined in the ITM-SC database.

Before you begin

Before the MIB download can start, the following prerequisites must be met:

- The network element must have a MIB.
- On the ITM-SC a MIB image must be present.

Pay attention to the following:

- The MIB in the network element will be overwritten by the MIB image of the ITM-SC.
- A MIB download causes the network element to reset. This results in a temporary loss of association with this network element. The association state will be “Maintaining” (see: View Network Element Status) until the network element is back up again and the association has been (automatically) re-established.
- A MIB download can be traffic affecting when the MIB and the MIB image differ!

Related information

Related procedures are:

- Disable association.
- Creating a Network Element.
- View Network Element status.
- Backup / restore: After a restore, when the automatic association option is not chosen. The user then has the option for MIB download or MIB upload for each network element individually.
- Manage Associations.

Procedure

To perform a MIB download follow this procedure:

1 Select *Management* --> *MIB Download*.

Result:

The *EMS - MIB Download* window appears.

2 To select a provisioned NE or switch to another provisioned NE, click the Selection Dialog Button. A list of possible NEs then appears in the *EMS- NE Selection Dialog* window. Select the desired NE and click `OK.`

Result:

The *EMS - MIB Download* window appears again with the selected NE displayed in it.

3 Click `Apply`.

Result:

A confirmation window appears to warn the user about the consequences of this action and to ask to continue or not.

4 Click `Yes`.

Result:

In the message box “Operation Started” is displayed. If the MIB upload is executed the message “Operation Successful” will be displayed. Otherwise “Operation Failed” will be displayed.

5 Click `Close`.

Result:

The *EMS - MIB Download* window disappears.

END OF STEPS

□

Section: Using the Event Lists

Overview

Purpose

Use this procedure to view the current and historical events of the network and to acknowledge the current events of the network. You can also delete historical events from the history alarm list and generate a report for displaying or printing.

□

Using the Event Lists

When to use

To evaluate alarms by filtering and sorting the events in every possible way.

Before you begin

Before performing this procedure make sure:

- when wanting to the display the autonomous event list, the ITM-SC is licensed for ADM 155– ADM4/1 NE management

When performing this procedure consider the following:

- If events are described Alarms and Autonomous Events are meant.
- Alarms are displayed through the Alarm List window while the Autonomous Events are displayed through the Autonomous Event List window.

Related information

Related procedures are:

- Viewing Event Details
- Acknowledging Events
- Deleting History Events
- Configuring the Event Lists
- Customizing Alarm Summary Filters
- Viewing Alarm Statistics

The related concept is:

- Event Display [10-26]

Parameters used in this procedure can be found at Parameters for Using the Event Lists [8-20].

Procedure

Follow these steps to list the Event lists.

1 To view the alarms select Events -> Alarm List from the top level menu. To view the Autonomous alarms select Events -> Autonomous Event List from the top level menu or the Auto-Event button in the main EMS - Menu window .

Result:

The *EMS - Alarm List* or *EMS - Autonomous Event List* window is displayed.

2 To see the time the alarm/autonomous event was raised or cleared and a cause description for the alarm instead of the code, select `Show Time`.

Result:

The list is updated with time, date and cause information.

3 Select `Current` to display the events that are still present in the network.

4 Select History Alarms to update the list with an overview of events that are not present any more in the network and are moved to the history list.

5 Select Both to update the list with an overview of both the Current and History events.

6 When you want to filter the list by *Location*, *NE type*, *NE name*, *Status*, *Level*, *Category*, *Severity*, *Source* or *Time Frame* please proceed to *Configuring the Event List* procedure.

7 When you want to acknowledge or delete an alarm please proceed to the Acknowledge Events or Deleting Events procedure.

8 Click Selection dialog button in the *Alarms/Autonomous Events are being sorted by* field to sort the events.

Result:

The Alarm Sorting Dialogue or Autonomous Event Sorting Dialogue is displayed.

9 Select the first key, and second key when necessary.

10 Click `Apply` to activate the sorting criteria. Select `Close`.

Result:

The Sorting dialog window disappears.

11 Click `Apply` to change the selections for this event list only.

12 Click `Close`.

Result:

The *EMS - Event List* window or *EMS - Autonomous Event List* window closes.

END OF STEPS

□

Parameters for Using the Event Lists

Introduction

Events are divided into two categories:

- Alarms, these are also called instantaneous events
- Autonomous events.

The options and buttons, as described below, provide possibilities to display additional event information and to select multiple events for further actions.

Access to the Event Lists

The Alarm Lists can be accessed via

- the top level menu
- a double click on a node (the alarm list will be filtered by that node)
- the node pop-up menu by selecting the node by using the right mouse button (the alarm list will be filtered by that node)

The Autonomous Event List can be accessed via:

- the top level menu
- the autonomous event button on the network map.

Display

You can switch the listing of events between displaying the *Current*, *History* or *Both*, by using the options on the left-hand side of the window. It is possible to display the time the events were raised by clicking on the Show Time option on the right-hand side of the window. The time will then replace the *Description* in the Alarm List or Autonomous Event List window. Select *Show Time* to display the Description field again.

Show Time

Shows the time raised, time cleared and cause of the event. Replaces the Description column in the Alarm List or Autonomous Event List window. The date convention used is dd/mm/yy and the convention for time is hh:mm:ss

Select All

Selects all event in the Alarm List or Autonomous Event List window.

De-select All

Clears all selections in the Alarm List or Autonomous Event List window.

Details

Displays details about the selected event. Please refer to the Viewing Alarm Details procedure.

Operation

The options to choose for further action are: acknowledge and delete. When event latching is enabled the alarm must be acknowledged before the alarm moves to the history list upon clearance. Deletion is only possible to history events. Please refer to the Acknowledging Events and the Deleting History Events procedures

□

Section: Managing ITM-SC Log Files

Overview

Purpose

Use this procedure to manage the records of system (ITM-SC) related actions which are performed in history.

□

View ITM-SC Log Files

When to use To investigate or evaluate system related actions.

Before you begin No prerequisites or precautions are needed when performing this procedure

Related information The related procedure is:

- Delete ITM-SC Log Files

The related concepts is:

- ITM-SC Log File Management [10-39]

Procedure Follow these steps to view the ITM-SC Log Files.

1 Select *Log File Administration* from the *ITM-SC Administration* menu.

Result:

The *ITM-SC Log Files* window is displayed.

2 In the *Filter* field, type the name of the log file to view. The use of wild cards such as “*” is permitted.

3 Select *Filter*.

Result:

The list of log files is updated.

4 Select the log file to view from the list.

Result:

The selected log file is highlighted.

5 Select *View*.

Result:

A text editor window is displayed, allowing to view data logged in the selected log file. The file is read only.

6 Select *File* -> *Exit* in the text editor to stop viewing data.

Result:

The view data window closes.

7 Select `Close` to complete the procedure.

Result:

The *ITM-SC Log Files* window will disappear

END OF STEPS

□

Delete ITM-SC Log Files

When to use When deleting the stored ITM-SC log files to free disk resources.

Before you begin No prerequisites or precautions are needed when performing this procedure

Related information The related procedure is:

- View ITM-SC Log Files

The related concepts is:

- ITM-SC Log File Management [10-39]

Procedure Follow these steps to delete ITM-SC Log Files.

1 Select the *Log File Administration* icon from the *ITM-SC Administration* menu.

Result:

The *ITM-SC Log Files* window is displayed.

2 Move the cursor to the *Filter* field and type the Log File name. The use of wild cards such as "*" is permitted.

3 Select *Filter*.

Result:

The list of log files is updated.

4 Select the log file to delete from the list.

Result:

The selected log file is highlighted.

5 Select `Delete`

Result:

The *Delete Log Files* window is displayed.

6 Select `Yes`.

Result:

The log file is removed from the list of Log Files.

7 Select `Close` to exit from the Log Files window.

END OF STEPS

□

Section: Managing Operator Log Files

Overview

Purpose

The Operator Log shows the actions and operations done on the ITM-SC by a user. This can be necessary when tracking down actions done on the ITM-SC. A history of the operations are maintained for all users.

These procedures manage all operations that can be performed on Operator Logs

□

Enabling or Disabling the Operator Log

When to use To enable or disable Operator Logging.

Before you begin No prerequisites or precautions are needed when performing this procedure

Related information Related procedures are:

- Controlling the Operator Log
- Displaying the Operator Log
- Create an Operator Log Archive
- Copy Operator Log Archive to Default Device
- Delete an Operator Log Archive

The related concept is:

- Operator Logs [10-40]

Parameters used in this procedure can be found Parameters for Managing Operator Log Files [8-34]

Procedure Perform this procedure to enable or disable Operator Logging

1 Select *File* -> *Logging* -> *Operator Logs* -> *Operator Log Status*.

Result:

The *Operator Logging Control Information* window is displayed, indicating the current Operator Logging status.

2 Select `Edit`.

Result:

The *Edit Operator Logging Control* window is displayed.

3 Change the *Operator Logging status* to *Enable* or *Disable* and select `OK`.

Result:

The *Edit Operator Logging Control* window will disappear and the Operator Logging status is changed.

4 Select `Close` to complete the procedure.

Result:

The *Operator Logging Control Information* window will disappear.

END OF STEPS

□

Controlling the Operator Log

When to use

To increase the security of the ITM-SC this procedure can be used to restrict a user its view of attributes in the Operator Log List. The Operator Log List displays all records created by the user. Attributes of the records are: host and node name, date and time of an operation, operation details and the result of an operation.

Before you begin

Before performing this procedure consider the following precaution:

- Only the ITM-SC Administrator can control the Operator Logs for all users.

Related information

Related procedures are:

- Enabling or Disabling the Operator Log
- Displaying the Operator Log
- Create an Operator Log Archive
- Copy Operator Log Archive to Default Device
- Delete an Operator Log Archive

The related concept is:

- Operator Logs [10-40]

Parameters used in this procedure can be found Parameters for Managing Operator Log Files [8-34]

Procedure

To edit or change the user restriction the following procedure has to be performed.

1 Select *File* -> *Logging* -> *operator logs*->*Operator Log Control*.

Result:

The *EMS* - *Operator Log Control* window is displayed.

2 Select a user with the `selection dialog` button.

Result:

A selection dialog window is displayed.

3 Select the *Filter* items that you want to edit or change. When the Filter Item is highlighted the selected user will not see this field in the Operator Log List window.

4 Select `Apply`.

Result:

The Operator Log List is updated for the user specified according to the changes made in the *EMS - Operator Log Control* window. The window closes to complete the procedure.

END OF STEPS

□

Displaying the Operator Log

When to use To investigate or evaluate the users actions and the ITM-SC response.

Before you begin No prerequisites or precautions are needed when performing this procedure

Related information Related procedures are:

- Enabling or Disabling the Operator Log
- Controlling the Operator Log
- Create an Operator Log Archive
- Copy Operator Log Archive to Default Device
- Delete an Operator Log Archive

The related concept is:

- Operator Logs [10-40]

Parameters used in this procedure can be found Parameters for Managing Operator Log Files [8-34]

Procedure Follow these steps to view and filter the Operator Log List:

1 Select *File -> Logging -> Operator Logs->Operator Logs*.

Result:

The *EMS - Operator Log List* window is displayed. This window will display the user initiated events. The filtering options are displayed in the top of the window. When no filters are applied all operations are displayed.

2 To filter select the `selection dialog` button.

Result:

The *EMS - Operator Log List Filter Options* window is displayed.

3 Select the appropriate *filter*.

4 After completing all *Filter* options, select `OK`.

Result:

All operations/actions in the Operator Log List are filtered according to the Filter Options. If a filter is being used this is indicated by a positive indication in the box adjacent to the filter type.

5 To suppress *attributes* select an attribute.

Result:

The *EMS - Operator Log List* window is updated automatically.

6 To sort select *Primary Sort* and choose an attribute out of list. A *Secondary Sort* is optional.

Result:

The *EMS - Operator Log List* window is updated automatically.

7 To close the *EMS - Operator Log List* window select `close`.

Result:

The *EMS - Operator Log List* window disappears.

END OF STEPS

□

Parameters for Managing Operator Log Files

Introduction

Parameters in the *Operator Log List User Display Restrictions* window and the *Operator Log List* window are described below.

Host Name

The host ID from which the operation was attempted.

Date and time

When operation took place.

Node name

Name of NE or Node the action was submitted to.

Result

Type of result. This can be `started`, *`failed`* or *`finished`* .

Additional information

Supplies additional information.

Sorting Criteria

To sort the Operator Log List use:

- Primary Sort
- Secondary Sort

The list is sorted first using the Primary Sort criteria. If two or more records are equal to the Primary Sort criteria, the system applies the Secondary Sort will be applied.

Display Suppression

Select the appropriate item in the Operator Log List window. The window will be automatically refreshed to show the items not suppressed.

Refresh

The Operator Log List will not be automatically updated when new Operator Logs are created. Select in the Operator Log List to view new records.

Button description

Buttons on the Operator Log List window are detailed in the table below.

Button	Function
Refresh	The Operator Log List will not be automatically updated when new Operator Logs are created. Select in the Operator Log List to view new records.

Button	Function
Dialogue	When the Dialog Button is selected, a window is displayed. Only one user name, host and node can be chosen as filter option at a time. Several Operation options can be selected as filter. To prevent a maximum of 30.000 records to be displayed the default Date/Time setting is set to 7 days.

□

Section: Managing Operator Log Archives

Overview

Purpose

The archiving of operator log information allows the user to obtain a long term, global view of the ITM-SC its users. This data can be used for planning preventative maintenance strategies and assist in customer quality of service reports.

Deleting old Operator Logs will free system resources prevent the system of being halted due to limited disk space.

□

Create an Operator Log Archive

When to use

When storing Operator Log Files for later use.

Before you begin

No prerequisites or precautions are needed when performing this procedure.

Related Information

Related procedures are:

- Enabling or Disabling the Operator Log
- Controlling the Operator Log
- Displaying the Operator Log
- Copy Operator Log Archive to Default Device
- Delete an Operator Log Archive

The related concept is:

- Operator Logs [10-40]

Parameters used in this procedure can be found Parameters for Managing Operator Log Archives [8-42]

Procedure

Follow these steps to create an Operator Log Archive:

1 Select *File* -> *Logging* -> *Operator Logs* -> *Archive*.

Result:

The *EMS - Operator Log Archive Information* window is displayed.

2 Select *Archive* -> *Create*.

Result:

The *EMS - Create Operator Log Archive* window is displayed.

3 Enter the *Archive File Name* and an *Archive Description* and select `OK`.

Result:

All records of the current Operator Logs are archived to a history file.

4 Select *File* -> *Close* to complete the procedure.

Result:

The *EMS - Operator Log Archive Information* window disappears

END OF STEPS

□

Copy Operator Log Archive to Default Device

When to use When copying created Operator Log Archive to the default device for external use.

Before you begin Before performing this procedure make consider the following:

- On a co-resident configuration both ITM-SC and ITM-NM modules will access the same tape drive.

Related Information Related procedures are:

- Enabling or Disabling the Operator Log
- Controlling the Operator Log
- Displaying the Operator Log
- Create an Operator Log Archive
- Delete an Operator Log Archive

The related concept is:

- Operator Logs [10-40]

Parameters used in this procedure can be found Parameters for Managing Operator Log Files [8-34]

Procedure Follow these steps to write a created Operator Log Archive to the default device:

1 Select *File* -> *Logging* -> *Operator Logs* -> *Archive*.

Result:

The *EMS - Operator Log Archive Information* window is displayed.

2 Select an *Operator Log Archive*.

3 Select *Archive* -> *Write to Device*.

Result:

The user to asked to check if the media (e.g. tape) is present in the default device.

4 Wait for the system to finish its data transfer. A transfer of around 200 Mb will take 2 minutes.

Result:

The selected Operator Log Archive is copied to the default device.

END OF STEPS

□

Delete an Operator Log Archive

When to use

When removing archived Operator Logs to free disk resources.

Before you begin

No prerequisites or precautions are needed when performing this procedure.

Related Information

Related procedures are:

- Enabling or Disabling the Operator Log
- Controlling the Operator Log
- Displaying the Operator Log
- Create an Operator Log Archive
- Copy Operator Log Archive to Default Device

The related concept is:

- Operator Logs [10-40]

Parameters used in this procedure can be found Parameters for Managing Operator Log Files [8-34]

Procedure

Follow these steps to archive operator logs:

1 Select *File* -> *Logging* -> *Operator Logs* -> *Archive.*

Result:

The EMS - Operator Log Archive Information window is displayed.

2 Select the file to delete and select *Archive* -> *Delete*.

Result:

The file is deleted.

3 Select *File* -> *Close* to exit the *EMS - Operator Log Archive Information* window and complete the procedure.

END OF STEPS

□

Parameters for Managing Operator Log Archives

Introduction

Parameters as used when performing Operator Log Archive tasks are described below.

Archive Filename

The Filename the user gives to an Operator Log archive for identification. This can be up to 8 characters long and must be according to the UNIX/DOS naming rules.

File directory and format

The Operator Log Archive will be stored on the ITM-SC client or Stand-alone. It will be stored in twofold in the *var/spool/itm/sc/archive/<server name>/operlog/* directory. One file (*.txt) will in a tab separated txt format while the other (*.gz) will be in a gz compressed format. The *.gz file can be decompressed by the UNIX command `uncompress`. Also other decompress programmes are widely available.

If performing the Copy Operator Log Archive to Default Device procedure is performed the compressed archive file is copied.

Archive Description

Using an archive description support identifying the right archive. Up to 50 characters, including spaces, can be used.

Size

Indicates the compressed size of the Operator Log Archive file in kBytes.

□

9 ITM-SC Upgrade

Overview

Purpose

This chapter provides tasks to perform a software upgrade of the ITM-SC.

Abbreviations used

When Network Elements OLS 80G, ADM 4/1, ADM 16/1, ADM16/1c, AM 1 (Plus) and TM 1 are described WaveStar®OLS 80 G, WaveStar®ADM 4/1, WaveStar® ADM 16/1, WaveStar® ADM16/1 compact, WaveStar® AM 1 (Plus) and WaveStar® TM 1 are meant.

□

Section: Starting and Stopping the ITM-SC

Overview

Purpose Perform this procedure for example to start the ITM-SC after shutdown or initial installation. When for example the ITM-SC database has to be restored it is necessary to stop the ITM-SC.

□

Starting and Stopping the ITM-SC

When to use Use this procedure to start or stop the ITM-SC application.

Before you begin No prerequisites or precautions are needed when performing this procedure.

Related information No related information is available.

Procedure Follow these steps to start or stop the ITM-SC application:

1 Open the *ITM-SC Administration* menu.

2 Select the *System Administration* icon.

Result:

The *ITM-SC System Control* window is displayed.

3 Select `Start` or `Stop`.

Result:

The *Start System* window or *Stop System* window is displayed.

4 Select `Yes`.

Result:

If the `Start` option was chosen then after a while all the ITM-SC processes are activated. To prevent interference with the system processes wait for the system to start!

If the `Stop` option was chosen then after a while all running ITM-SC processes are stopped. Wait for the system to stop!

5 Select `Exit` to complete the procedure.

Result:

The *ITM-SC System Control* window closes.

END OF STEPS

□

Section: ITM-SC Maintenance Upgrade

Overview

Purpose

This procedure will install a new version of the ITM-SC software. This procedure will automatically upgrade the help files and on-line documentation. This can be done locally or remotely.

□

Local ITM-SC Maintenance Upgrade

When to use

When upgrading the ITM-SC to a new version of the same release on a local system. This procedure will automatically upgrade the help files and on-line documentation.

Before you begin

Before performing this procedure make sure:

- *not* to use this procedure for upgrading additional languages. Please perform the ITM-SC foreign Language Install procedure.

Consider the following recommendation:

- It is recommended the ITM-SC configuration files and Informix database are backed up before performing an upgrade. This can be done by following the *Backing Up of the Entire ITM-SC System* procedure as described in the Administration Guide (AG).

Related information

The related procedure is:

- Local ITM-SC Maintenance Upgrade

Procedure

Follow these steps to perform a *local* ITM-SC Maintenance upgrade:

1 Insert the ITM-SC installation tape for the required hardware platform into the tape drive.

2 Hardware platforms with less than the standard hard disk space requirement may need a HP-UX patch cleanup program to be loaded and run. Enter the following command as user root to perform the patch cleanup:

```
cleanup -F
```

3 Answer `y` (yes) to the prompts to trim logs and remove patch backups.

4 To perform the actual upgrade enter the following command:

```
itmsc_maintenance_upgrade [source location]
```

(The default source location is */dev/rmt/0m*)

Result:

After the upgrade the machine will automatically reboot.

5 The reboot can be suppressed using the `-nr` (noreboot) switch. The use of this switch is not recommended.

6 If upgrading a client or stand-alone machine, from the CDE login screen select *Options* -> *Command Line Only* and press **ENTER**.

7 Login as *root*.

8 After the new release of the ITM-SC is installed enter:

```
itmsc_switch_release
```

Result:

This command will configure and start the new release. A list of available releases is displayed and the user is prompted to select the release to switch to.

9 Choose a release by typing a number as indicated by the list.

Result:

The ITM-SC will be stopped and restarted as necessary.

END OF STEPS

□

Remote ITM-SC Maintenance Upgrade

When to use

When upgrading the ITM-SC to a new version of the same release on a remote system. This procedure will automatically upgrade the help files and on-line documentation.

Before you begin

Before performing this procedure make sure:

- *not* to use this procedure for upgrading additional languages. Please perform the ITM-SC foreign Language Install procedure.

Consider the following recommendation:

- It is recommended the ITM-SC configuration files and Informix database are backed up before performing an upgrade. This can be done by following the *Backing Up of the Entire ITM-SC System* procedure as described in the Administration Guide (AG).

Related information

The related procedure is:

- Local ITM-SC Maintenance Upgrade

Procedure

Follow these steps to perform a Remote Maintenance upgrade. This will be done via a depot:

1 Enter the command below to make sure the system containing the software depot can be accessed across the network:

```
/etc/ping <IP address of machine containing
depot>
```

Result:

The ping command should display regular successful communication time messages. An example is shown below:

```
PING <IP address>: 64 byte packet 64 bytes
from <IP address>: icmp_seq=0. time=2. ms 64
bytes from <IP address>: icmp_seq=1. time=1.
ms ----<hostname> PING Statistics---- 2
packets transmitted, 2 packets received, 0%
packet loss
```

2 Perform the ITM-SC Maintenance Upgrade procedure using the remote depot. To do so enter:

```
itmsc_maintenance_upgrade –s <ip of depot
machine>:/depot
```

END OF STEPS

□

10 Concepts

Overview

Purpose In this chapter some concepts of ITM-SC administration are explained.

Section Each section describes one of more concepts of each previous chapter. However not all of these, so called, tasks-chapters do have a concept description.

Abbreviations used When Network Elements OLS 80G, ADM 4/1, ADM 16/1, ADM16/1c, AM 1 (Plus) and TM 1 are described WaveStar®OLS 80 G, WaveStar®ADM 4/1, WaveStar® ADM 16/1, WaveStar® ADM16/1 compact, WaveStar® AM 1 (Plus) and WaveStar® TM 1 are meant.

□

Section: Security Management

Overview

Purpose

This section gives the reader detailed information about the User Administration on the ITM-SC.

Intended Use

Readers not familiar with User Administration is advised to read this entire section. For detailed information on User Roles refer to the *User Roles* concept. For information about using the ITM-SC for CIT Access restriction refer to the *CIT Access* concept.

□

Security Management Overview

Introduction

To prevent illegal access and to provide customized access the ITM-SC User must be provided with the appropriate privileges. These privileges are twofold: functionality and NE accessibility. The functionality will restrict the user in the actions he can perform on an NE while the NE accessibility will give him only access to the NE he is entitled to manage.

The functionality restriction is comprised in the User Roles and User Class feature while the NE accessibility is comprised within the Access Domains.

Objective

To provide each user with the privileges which are necessary to perform the job correctly.

Initial User ID Creation

In order to access the ITM-SC, users must have both a user ID and password. Initially the user must be assigned to one of the User Classes. Accordingly the user will have access to all NEs currently managed by the ITM-SC.

Optional: User Roles and Access Domains

Initially the user's functionality will be directed by the User Class and will have access to all NEs currently managed by the ITM-SC. Customized restriction of functionality and accessibility can be done by assigning the user to a User Role (created by the ITM-SC administrator) and an Access Domain. However this is not mandatory.

System Administrator assigns user ID and password

The ITM-SC Administrator assigns the user ID, password, and the User Class. The ITM-SC Administrator is one of the three User Classes.

Maximum logins

Up to 100 login names can be created. With the appropriate licenses, up to 10 users can use the ITM-SC simultaneously.

User Classes

There are four User Classes. These are listed below:

User Class	User Privileges
Not Defined	Has access to the UNIX operating system of the ITM-SC only.

User Class	User Privileges
Administrator	Performs administrative functions. This includes the ability to: • administer user privileges. • backup and restore the database. • manage Log Files. • set system devices. The ITM-SC default Administrator *i2kadmin* login name cannot be changed or deleted.
Supervisor	Performs ITM-SC provisioning functions. This includes the ability to: • retrieve all alarm information and acknowledge these alarms • view administration information • view and modify configuration information.
Operator	Performs functions which includes to ability to: • retrieve all alarm information and acknowledge these alarms • view administration information • view configuration information.

User Roles

User Roles allow the user to have customized functionality. All the functionality of the ITM-SC can be divided into function groups, e.g. PM, licenses, alarms etc. A user has an access level for each functional group. The three access levels are described below.

Access Level	Description
Edit	The user does have read and write access to the parameters within the function group
Information	The user can only view the parameters within the function group
Disabled	The user cannot access the function group

Maximum User Roles

In addition to the 4 User Classes, 5 User Roles can be created by the ITM-SC Administrator. To enable the User Roles the Extended User Class license key has to be enabled.

Access Domain

The user can be restricted to a number of NEs which he/she can manage. This is called an Access Domain. An Access Domain is a collection of one or more Access Groups. Access Groups are groups of NEs and/or Nodes. The user is able to perform functions on the NEs in the Access Domain as defined by his/her User Role/Class.

Example on Access Domains

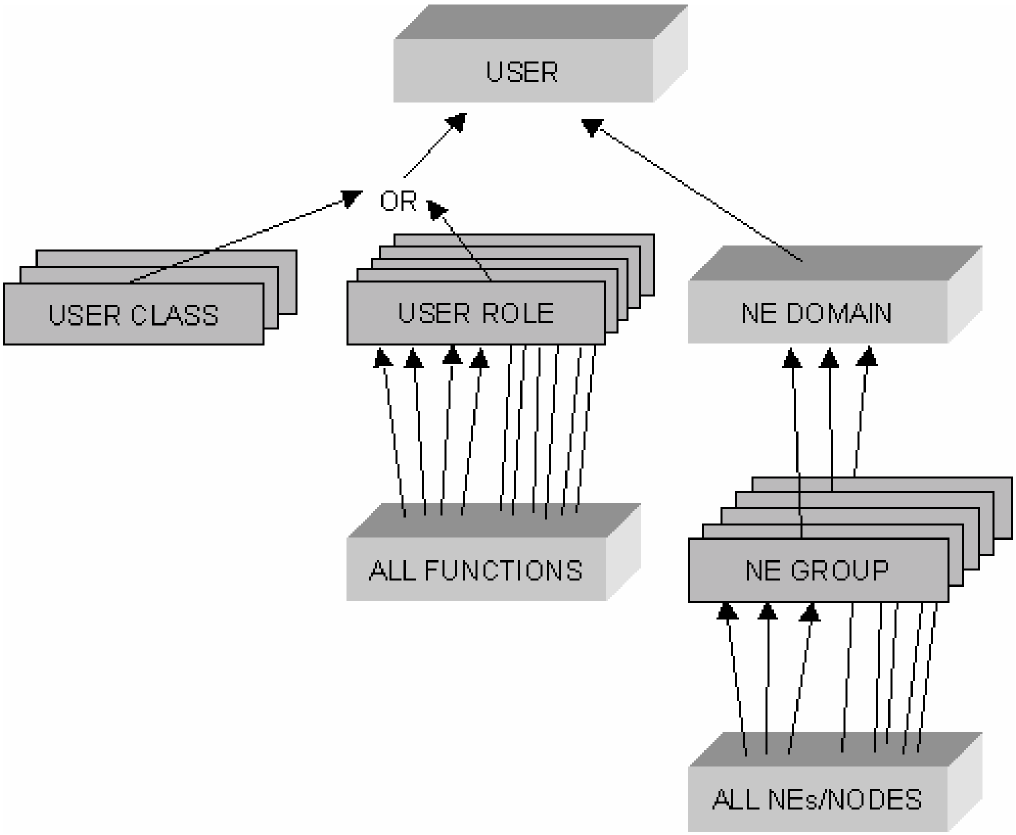
Due to his capabilities Mister X has to be assigned only to ISM Network Elements. Therefore in each of the e.g. two available regions all ISMs are grouped together in the Access groups: ISMnorth, ISMsouth. The Access Domain Mister X is assigned to consist out of the Access Groups: ISMnorth and ISMsouth.

Multiple use of User Roles and Access Groups

A User Role/Class can be used for several users. Also Access Groups can be used in several Access Domains as well. An Access Domain is user specific. It is possible to assign the same Access Groups to 2 different Access Domains. As a result both users can access the same NEs.

Graphical Outline

In following graphical outline the components of user administration are displayed.



□

User Roles

Overview

When the aimed privileges of a user cannot be met by one of the User Classes, the user has to be assigned to a User Role. First this User Role has to be created by the ITM-SC Administrator.

Definition

A User Role is a collection of privileges. A privilege consists of a function and access level.

Objective

To customize the privileges of the ITM-SC users.

Example

Whenever a person is only entitled to perform ITM-SC Network Maintenance the following settings can be made:

Function	Access Level
Performance Monitoring	Edit
Alarm Management	Information
Equipment Management	Disabled
Traffic Management	Disabled
Report Management	Edit
Geographic Redundancy	Disabled
Protection Management	Edit
Network Setup	Disabled

Default User Roles

The User Classes (Administrator, Supervisor and Operator) are provided as default User Roles. These default User Roles cannot be changed. The privileges are indicated below where E, D and I mean Edit, Disabled and Information respectively.

Feature	Administrator	Supervisor	Operator
Core Feature	E	E	E
Report Management	E	E	I
Report Timing	E	E	I
Report Definition	D	E	E
Template Management	E	E	D
Templates Timing	D	E	D
Templates Protection	E	E	D
Card Management	E	D	D
User Roles	E	D	D

Feature	Administrator	Supervisor	Operator
Pre-provisioning	D	E	D
EMS Administration	E	D	D
Traffic Management	D	E	I
Operator Logs	E	I	I
Operator Log Archive	E	I	I
Equipment Management	D	E	I
Alarms	D	E	I
Alarm Archive	E	E	I
EMS Alarm Control	E	E	I
Geographic Redundancy	D	E	I
Performance	E	E	I
Performance Monitoring	D	E	I
Performance Set Up Monitoring	D	E	I
Performance Archiving	E	E	I
Confirmation Required	D	E	D
Licensing	E	I	I
Alarm Summary	E	E	E
Map	I	E	I
Enhanced Alarm Map	D	E	I
Sub-Network Manager	D	E	I
CIT Access Feauture	E	E	I
Access Groups Feature	E	I	I
Protection	D	E	I

Number of User Roles

In total 5 User Roles can be created.

Administrating User Roles

The User Role’s functionality and its assigned users can only be changed by the ITM-SC Administrator or any other person which entitled, by means of a User Role, to change these settings.

When a user is not assigned to one of the user roles the privileges will be assigned according the users classes Administrator, Supervisor or Operator.

A user can be assigned to one only 1(one) User Role at a time.

□

CIT Access

Overview

To restrict the NE access via a CIT the ITM-SC Supervisor and ITM-SC Administrator are able to control NE access for CIT users. This access control is done by the ITM-SC.

Definition

CIT Access means managing an NE by means of a CIT.

CIT User Roles

The CIT Users are divided into three CIT (User) Roles: Admin, Config and View. Each CIT Role does have its own set of privileges as detailed in the table below.

CIT User Role	Privilege
View	The CIT User is allowed to monitor the NE
Config	The CIT User is allowed to provision the NE
Admin	The CIT User has Config capability, and is allowed to administer the password, lock flag and inactivity time out.

ITM-SC Control

The ITM-SC Administrator and ITM-SC Supervisor are able to change the privileges of CIT users by changing the CIT Roles. They are also able to disconnect the access of any CIT to an NE at once.

Association Loss

When the association is lost between the ITM-SC and an NE the privileges, as set for the CIT Roles, will be ignored. Each CIT Role will have access to the NE any without restriction.

□

Section: ITM-SC System Administration

Overview

Purpose This section is used to give the reader detailed information about

- ITM-SC License keys.
- the synchronization of time on the NE and the EMS.

□

License Key

Purpose

License Keys increase the functionality of the ITM-SC. Each module of the ITM-SC application available is enabled by a separate license keys. Before you can enable any of the modules you first need to obtain valid license keys from your provider. To apply for a license key the Host ID of the ITM-SC is needed.

Important! If the License keys are not entered properly, the ITM-SC will NOT be accessible for the other users.

Available Licenses

Licenses have to be entered to the system to activate the modules or to enable a specific amount of NEs and/or users to collaborate with the ITM-SC.

- Base Software
- Maximum Users allowed
- Maximum number of ADM 4/1s (including ADM 155c)
- Maximum number of ISMs
- Maximum number of SLMs
- Maximum number of PHASEs (except LXC 16/1)
- Maximum number of LXC 16/1s
- Maximum number of RRs
- Maximum number of OLS80Gs
- Maximum number of ADM 16/1s (including compact version)
- Maximum number of AM1/TM1/AM1 Plus
- Maximum number of WDACSs
- Northbound TMAG interface (needed in deployments with WS-NMS)
- Northbound G7 2.0 Interface
- Northbound TMF CORBA interface
- Performance Monitoring Archive
- Geographic Redundancy
- Extended User Classes
- Tandem Connection Monitoring

ADM 155c

In order to license the ITM-SC for ADM155c NEs, it is sufficient to license the ADM4/1 instead.

□

NE Timing

Purpose

This feature synchronizes the internal clocks of all Network Elements (NEs) and the Element Management System within the management domain of that EMS as closely as possible to one another. This is needed to prevent the corruption of Performance Monitoring data and to support the TCM feature.

Previously all NEs were sent the time by the EMS but took no account of the time taken by the message to pass from the EMS to each NE. This resulted in the NEs being set to times that varied depending on the network topography and the traffic on the network.

ITM-SC and WaveStar® SNMS

The NE Timing Synchronization mechanism is implemented in both ITM-SC and WaveStar® SNMS. All NEs supported by these EMSs do support NE Timing Synchronization as well.

Automatic

The NE Timing Synchronization mechanism is run automatically every 24 hours, preferably at a period where the Management Network traffic is low. Each managed NE is scheduled to be synchronized sequentially by the EMS. To avoid the possibility of a particular NE being continuously synchronized at the time when PM data was being retrieved, the EMS shall start each synchronization cycle with a random NE.

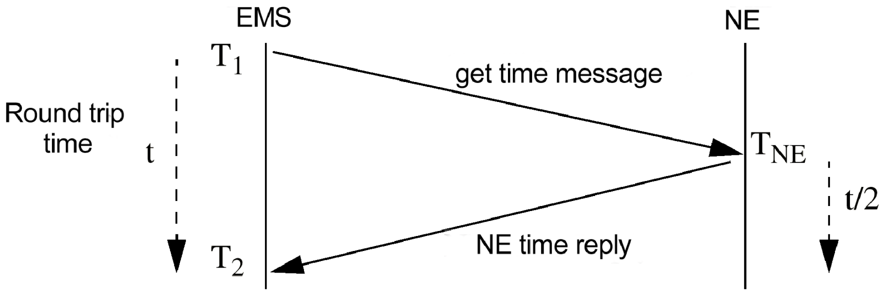
Definitions

Time drift Time difference between the NE time and the ITM-SC time

Round trip time Time between a message send by the ITM-SC and receiving it back from the NE

Measure round trip time

The round trip time, t, between sending a message and receiving the reply (T_2 -T_1 in the graphic below) shall be calculated a configurable number of times (indicated by the *Number of queries sent to NE* parameter) and the mean and maximum difference (maximum time minus minimum time) for the round trip time will be determined. The messages that are used to determine the round trip time are also used to request the NEs internal time to process the message (T $_{NE}$ in the diagram below), which is returned in the replies to the EMS.



The mean round trip time shall be checked against the maximum value allowed for the NE to determine if the traffic on the network is low.

If the mean round trip time is less than this threshold value then there are currently no significant delays being experienced by a message being sent to this NE. The threshold value is derived from the minimum round trip time recorded for this NE plus a user define offset.

Set NE Time

After the round trip time is determined the NE Time will be set to the EMS Time if:

- the mean round trip time is less than the minimum round time found in the latest added with an offset as indicated by the *Offset added to minimum round trip times*parameter. This will indicate no significant delays are being experienced by a message being sent to this NE.
- the variation of round trip times found (T_{max} — T_{min}) is less than indicated by the *Maximum variation allowed* parameter. This will indicate the path between NE and EMS is stable and is not fluctuating due to traffic on the network.
- the time drift measured is higher than the allowed difference as indicated by the *Time drift allowed in an NEs clock* parameter.

If the NE time is to be set the NE clock shall be sent a message indicating the current time plus the calculated offset (half of mean round trip time).

Check NE Time

Once the NEs clock has been set the time drift of the NEs clock is again determined to check whether the re-synchronization has been performed correctly. The message with the NEs time is received either as a response to setting the NEs clock or as a reply to a specific request to get the time from the NE.

The drift of the NEs clock is again determined using half the mean message round trip time previously calculated.

Fault generation

There are three possible places where a fault may cause the mechanism to fail:

- If the mean round trip time is greater than a user specified maximum. (network is experiencing some delays)
- If the maximum difference in the round trip times is greater than the user defined value. (network is unstable)
- If the NEs clock drift still exceeds the user defined threshold even after it has been adjusted by the EMS.

□

Section: Provisioning Environment Setup

Overview

Purpose This section provides background information about the MEC files on the ITM-SC.

□

MEC File Concepts

File Formats

There are three types of files to be considered which are used for software download.

- MEC File
- Software Load File
- TAR File

MEC File

A MEC File contains the actual software that will be run by the NE

Software Load File

This type of file contains a list of hardware and software IDs for use in NEs which require a MEC file per processor. Software Load Files are only available to PHASE NEs.

TAR File

A TAR File is used to combine the Software Load File and the MEC Files it contains into a single file. This will make copying between tape and ITM-SC easier. TAR Files are only available to PHASE NEs.

For PHASE NEs the MEC files that make up the software load are displayed, with an indication as to whether the MEC file is loaded (greyed out if not loaded).

Multiple MECs may be required

A complete version of software for an NE may require a single MEC or multiple MECs. The name of the MEC corresponds to the ID code of the software.

MEC file naming

The MEC files are considered present if a file of the given name, or a file whose name starts with the given name exists (for example: if the list gives the name as *12345678* and file *12345678A* is present, the MEC file is considered present).

If more than one MEC exists on the system which complies with the Software (S/W) ID the one with the highest value will be used (for example: S/W ID=123456701, MEC Files present: 1234567011 and 1234567012, than 1234567012 is used).

□

Section: Maintenance Environment Setup

Overview

Purpose

This section is used to give the reader detailed information about:

- Systems Alarms Monitoring
- Event characteristics and presentation
- Archiving of Event and Performance Monitoring data

Intended use

Readers not familiar with one of the topics above are advised to read the respective section before performing any task.

□

Systems Alarm Monitoring Overview

Background

Systems Alarm Monitoring is a group of features which can be used to monitor a number of ITM-SC applications (servers) at the same time. System Alarm Monitoring provides all alarm information for the entire management network via one workstation.

Alarm monitoring benefits multi server

Although a multi-service configuration benefits the most from the alarm monitoring feature it can also be used for stand-alone configurations.

Features of alarm monitoring

The three different features that comprise Systems Alarm Monitoring are:

- Systems External Alarm Presentation (EAP)
- Systems Fault Summary (FS)
- Cyclic check.

All features must be enabled by the workstation configured to monitor the ITM-SC servers. This enable/disable setting only affects the workstation on which the settings are made, so each workstation can have its own setting. Systems EAP and Systems FS must be licensed.

Initial Start of Systems Alarm Monitoring

Systems Alarm Monitoring must be activated initially by selecting the Alarm Monitor icon in the Provisioning and Maintenance module. The Fault Summary Panel will be displayed directly. The EAP window will only be displayed when a new alarm arrives. When Systems Alarm Monitoring is active it can only be stopped by entering the configuration window and change the setting accordingly.

License keys independent

Note that the (server dependent) licence key is however independent of the workstations. In this way an ITM-SC Server can be monitored by every workstation.

□

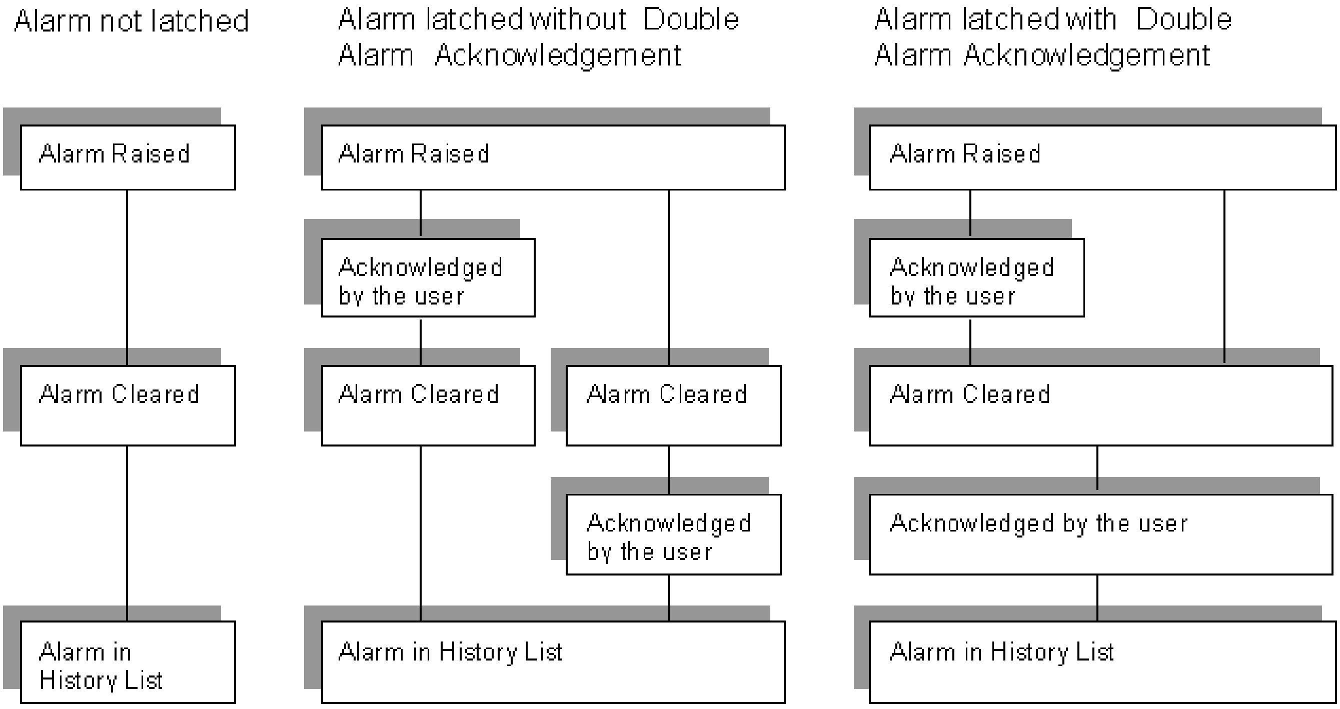
Double Alarm Acknowledgment Concepts

Background

If double alarm acknowledgment is implemented, cleared and latched alarms must be acknowledged before they are moved to the history list. Even when the alarm was acknowledged before clearance it is necessary to acknowledge it once more before it is moved to the history list. This is displayed in the right column of the picture below.

Without Double Alarm Acknowledgment cleared alarms which are already acknowledged will go to the history list directly. This is displayed in the middle column of the picture below.

Double Alarm Acknowledgment is to prevent the user to miss any clearance of alarms.



Not latched alarms

Alarms which are not latched can go to the history list without acknowledgment. This is displayed in the left column of the picture above.

□

Events

Event Management

Maintenance can be performed by using the ITM-SC. Two groups of maintenance activities are provided: *preventive* and *corrective* activities. ITM-SC's provides a bundle of corrective maintenance features that are described all together as *Event Management*. Corrective maintenance identifies a failure after it occurs. It is necessary to locate the failure as soon as possible to solve the problem or to prevent (further) signal disruption. The user is supplied with information about the location, nature, probable cause and severity of the event. All these parameters will determine the strategy of solving the problem.

Introduction

An event can be all kind of defects, failures and alarms on Network Elements, lines or paths, unit insertion or removal, etc. The ITM-SC is to support the collection of alarm/fault information from each individual NE, and provide capabilities for maintaining the ITM-SC view in line with the NE status. NE alarm notifications are forwarded to the Network Level (NL) immediately after being received. The information transferred to the NL includes all alarm information available in the ITM-SC.

Events

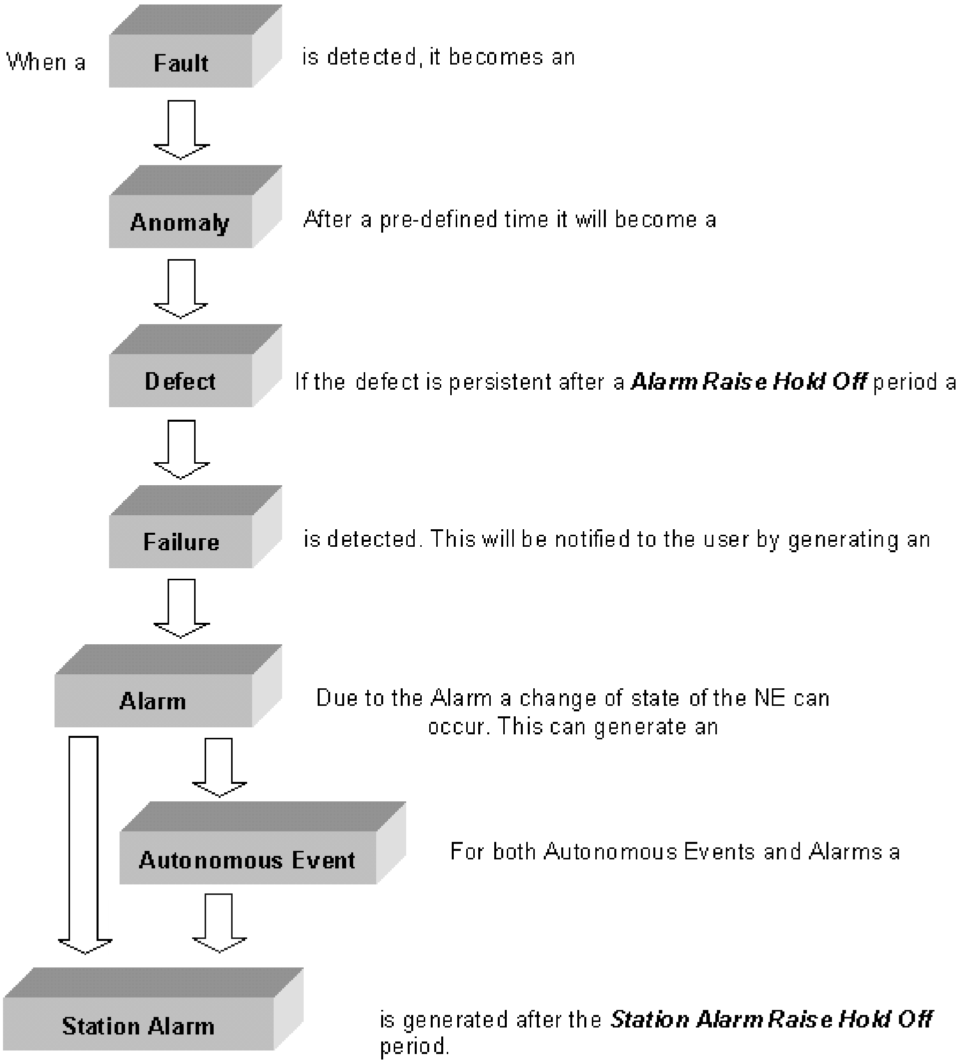
The description of the events are stated below

Event	Description
Fault	Something has broken or degraded to the point where some requirements can not be met. Faults exist whether we detect them or not.
Anomaly	The smallest discrepancy we can observe in the working of some item. Maintenance actions are not initiated on a single occurrence of anomalies. Anomalies are used as input for defect detections.
Defect	The density of an anomaly is increased to a level where the ability to perform a required function is interrupted. A defect may result in consequent actions.
Failure	The defect persisted long enough to have confidence that the condition is permanent. This implies by definition that there is a fault which we have now detected. A failure is defined as the detected termination of the ability to perform a required function, so it is an event, not a state.

Event	Description
Alarm	A human observable indication that draws the attention to a detected failure. Alarms may be delayed after the detection of failures. These are also called instantaneous events.
Autonomous Event	An autonomous event is an event that does not interfere with the network performance. For example the crossing threshold of the event storage can be an autonomous event.
Station Alarm	Discrete contact on the NE to enable a physical warning such as bell or light on the NE or within the vicinity.

Flow of events

The events stated before succeed each other in the flow chart below. Both Raise Hold off periods can be adjusted by the user. The station alarm is a visual or audible indication near the NE itself.


When a
Fault
is detected, it becomes an
Anomaly
After a pre-defined time it will become a
Defect
If the defect is persistent after a ***Alarm Raise Hold Off*** period a
Failure
is detected. This will be notified to the user by generating an
Alarm
Due to the Alarm a change of state of the NE can occur. This can generate an
Autonomous Event
For both Autonomous Events and Alarms a
Station Alarm
is generated after the ***Station Alarm Raise Hold Off*** period.

Persistent or Instantaneous alarms

Alarms can be persistent or instantaneous. Persistent means that a fault condition exists until the fault is cleared in the system. An instantaneous alarm is a one-off events and does not have a persisting fault condition and so does not have an associated severity. Instantaneous alarms are for example protecting switch events.

□

Event Characteristics

Introduction

In order to bring the alarm behavior in line with the maintenance philosophy all alarms can be configured. The characteristics of an alarm will determine:

- *if* an alarm or autonomous event will appear
- *when* the alarm or autonomous event will appear
- *how* the alarm or autonomous event will appear
- *how* the alarm or autonomous event will disappear when the problem is *solved*.

Event Status

Alarms/autonomous events can have three different statuses. These are described below.

Status	Description
Raised	The event is still present. It has not yet been acknowledged.
Acknowledged	The event has been noticed and confirmed by the user but the cause of the alarm may not yet have been removed.
Cleared	The cause of the event has been removed.

Report State

Whether the alarm/autonomous event will be notified to the user depends on the alarm report state.

Report State	Description
Reported	Raised events will be reported on the ITM-SC.
Not Reported	Raised events will not be displayed on the ITM-SC, you will be unaware of the occurrence of these alarms.

Severity

Events are classified according to their impact on the service of the Network Element or the ITM-SC (management alarms) itself. The attribute which defines the class of an event is called severity. At the management system the alarm severity of events can be set. The NE alarm severity settings are sent to the selected Network Element. The initial definitions of the available alarm severities are detailed in the table below.

Severity	Initial definition
Prompt	Immediate maintenance action is required because a primary system service is being affected.
Deferred	Maintenance action is required but may be deferred because no primary system service is being affected.
Info	Maintenance information: no maintenance action is required at this NE.

An instantaneous alarm is a one-off events and does not have a persisting fault condition and so does not have an associated severity. Instantaneous alarms are for example protecting switch events.

ADM 155c & ADM4/1 Severities

The ADM 155c and ADM4/1 NEs have a different set of severities. These specific severity levels are mapped into the standard manager severity definitions (Prompt, Deferred, Info) according the table below..

Then ADM 155c / ADM 4/1 severity...	is displayed on the ITM-SC as..
Critical	Prompt
Major	Prompt
Minor	Deferred
Warning	Info
Indeterminate	Info
Not alarmed	Not Reported

Alarm Control

When a defect is detected within an NE or ITM-SC the user will be notified of this defect via an alarm after the Raise Hold Off period. This period is used to make sure the defect really exist within the NE or ITM-SC. When the defect is solved the alarm will be cleared after the Clear Hold Off period. This period is used to make sure the problem is solved and prevents the alarm reporting to blink on and off repetitively.

Alarm latching

When latching is enabled the alarm/autonomous event must be acknowledged before the alarm moves to the history list upon clearance. When alarm latching is not enabled acknowledgement is still possible. But these alarms/autonomous events will go directly to the history list upon clearance whether acknowledged or not.

Clearance Acknowledgement

When Clearance Acknowledgement is licensed an alarm or autonomous event, which is initially latched, can only go to the history list after its clearance has been acknowledged. The alarms which have been acknowledged in the raised state remain after clearance in the current alarm list; they only go to the history list when their clearance has been explicitly acknowledged by the user.

Alarms latched on default

All alarms (instantaneous events) are latched on default. This is to make sure the alarm will be notified by the user. So they are moved to the History List only after they have been acknowledged.

Acknowledgments effective only on ITM-SC

Acknowledgments are only effective on the ITM-SC. Interaction with the network element or the NL is not expected or required in order to acknowledge alarms. Acknowledgment of alarms applies to the ITM-SC and NE created alarms.

Maintenance Philosophy

Within Event Management many parameters can be customized. It is expected to bring these parameters in line with the maintenance philosophy. Please obtain a consistent implementation of this philosophy in order to avoid confusion about solving problems within the transmission network.

□

Event Display

Introduction

When alarms or autonomous events are raised in an NE or ITM-SC they are brought to the attention of the user by autonomous reports. These reports are displayed on several windows on the ITM-SC. The several display types are described below.

Display type	**Displays...**
Network Map	the highest severity of all alarms on a NE by means of the NE icon turning into a color.
Alarm List	all alarms (instantaneous events) available. This list can be customized by a filter.
Autonomous Event List	all autonomous events available. This list can be customized by a filter
Alarm Summary	displays last alarm or autonomous event arrived as well as the total amount of alarms sorted out by severity and raised/acknowledged status. This list can be customized by a filter.
Alarm Statistics	the amount of NE alarms per NE

Filtering

A raised event, for example a card is pulled out, normally causes an immediate alarm notification on the alarm message display line of the management system. It is possible however (by means of the alarm filter option) to filter out various alarm/autonomous event messages from the alarm message display line. For example the user may not be interested in summary messages for alarms of the “INFO” severity class. The user may filter alarm messages for display by alarm severity, type and acknowledgment status. Note that this filtering only affects immediate alarm reporting. The total number of alarms for each severity is updated whatever the setting of the alarm filter, and alarms are entered into the current alarm list. This number can be viewed at any time.

Events can be sorted

Alarms in alarm or autonomous events can be sorted in their respective lists by the following parameters: number, alarm time, severity, probable cause, NE type, NE name and card type. Two sorting keys are available to provide a sorted list which is first sorted by another parameter. The settings can be stored as default.

Alarm acknowledgment information

When an alarm/autonomous event has been acknowledged, the Operator ID and the Acknowledgment time and date are added to the event record. This can be seen in the Details window.

□

Event Storage and Archiving

Introduction

All alarms and autonomous events present on the ITM-SC will be stored in either the current event list or history event list. Eventually every alarm or autonomous event in the current event list will end up in the history event list upon clearance.

Reports

Selections of the current and/or history event list can be printed to a report. This report can be viewed by the report browser. This can be used to store a specific situation.

Storage

Because events in the history list are not automatically deleted the amount of alarms have to be controlled. A warning signal is given when a certain threshold is exceeded. It is possible to delete the events automatically after they have resided in the history list after a configurable time.

Archiving

It is possible to store all the alarm and autonomous event data into an Event Archive. An Event Archive can be written to an external device such as tape or disk for further analysis.

Scheduled archive

It is possible to select either an instantaneous archive or a scheduled archive. This scheduled archive will be performed daily at a the specified time. This specified time will be rounded up to the nearest 15 minutes (for example: quarter past, half past).

Scheduled versus manual archiving

When a scheduled archive is set for a specific time, manual initiated creation of event archives (instantaneous archive) can be performed up to 15 minutes before the scheduled archive. When the manual creation is performed within these 15 minutes the scheduled archive will be postponed 15 minutes accordingly.

Furthermore it is not possible to create an PM Archive within 30 minutes before a scheduled Event Archive. Because the creation of an PM Archive can take a maximum of 30 minutes to complete. The request will be rejected with the message: `Not authorized by archive broker`.

File directory and format

The PM Archive will be stored on the ITM-SC server or Stand-alone. It will be stored in twofold in the *var/spool/itm/sc/archive/alarmhist* directory. One file (*.ARC.txt) will in a tab separated ASCII format while the other (*.gz) will be in a gz compressed format. The *.gz file can be decompressed by the UNIX command `uncompress`. Other decompress programmes are widely available.

□

PM Data Storage and Recovery

Bins

Once the data is collected over the selected accumulation periods (15 minutes, or 24 hours) and that directionality is selected for a given termination point, the system stores the performance results in registers, called bins.

A bin contains performance data information for each termination point such as:

- Timestamp;
- Elapsed time;
- Suspect indication which is a data flag to indicate that the data stored in the bin is incomplete or invalid.

Resetting the NE clock has no effect on the timestamp of the recent 15 minutes and 24 hour bin.

Each TP can have two current bins, one for a 15–minutes measurement period and one for a 24 hour measurement period. The latter can be either uni- or bidirectional, when applicable for the specific NE.

When a measurement period has elapsed, the data will be moved from the current bin on an NE to a so-called historic bin on the NE.

The number of historic bins depend on the NE type, as is displayed below.

NE type	Number of 15 minutes unidirectional historic bins	Number of 24 hours unidirectional historic bins (or bidirectional when applicable)
ADM 155C	15	1
OLS80G	32	6
any other NE	16	1

The unidirectional and bidirectional 24 hours bins store performance data over a span of a current 24 hours period. At the end of the current 24 hours period, the data is timestamped and sent to the 24 hours historic bin, and the current 24 hours bin is reset to zero. The 24h measurement period will always start at the next full hour. The 15–minutes measurement period will always start at the next full quarter.

The unidirectional 15 minutes bins accumulates performance data over a span of 15 minutes periods. At the end of a current 15 minutes period, the data is timestamped and transferred to the first of the fifteen available 15–minutes historic bins. When all the 15 minutes history bins are full, the eldest history bin is overwritten by the new information to be transferred.

Viewing Current bins

Via both the ITM-SC and ITM-CIT the values of the currently running PM measurements can be displayed.

On the ITM-SC refer to the procedure *Displaying Current Measurements*.

Interval (Bin) suppression

In the event that the current bin data is all zero and that the system indicator is not set, while the `actual` number of consecutive suppressed intervals is lower than the `maximum number` of consecutive suppressed intervals, then the current interval can be suppressed. This means that the data would not be transferred to the next available, or recent bin. The default value for the maximum number of consecutive suppressed intervals is zero, but can be provisioned per termination point for each accumulation period.

Interval (Bin) suppression is only available at the ITM-CIT.

Reset of PM counters

The ITM-CIT as well as the ITM-SC offer the possibility to reset the parameters counter for uni— and/or bidirectional monitoring in order to assist with maintenance activities. When the management system sends this request to the NE, the bin content is reset for the current 15 minutes bins and the content of the current 24 hours bins associated with a termination point.

Resetting the counters has the following consequences:

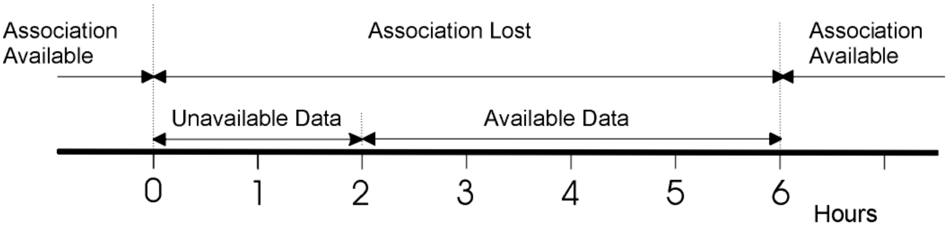
- Elapsed time is reset to zero
- PM counters value (BBE, ES, SES, UAS, UAP) are reset to zero
- UAPlog counter is NOT affected
- Suspect indication is set.
  Refer to the procedure *Reset Digital Counters* on the ITM-SC.

Data Recovery Following Loss of Association

If the association between ITM-CIT or ITM-SC and the NE fails, the CIT/SC regains information about the lost time by reading the NE bins for the relevant interval. If the association fails for a longer period of time the NE may not be able to store sufficient information for a full recovery.

Example of Loss of Association

In the example below the association with the management system has been lost for 6 hours. Because this NE does have sixteen 15 minutes unidirectional bins only 4 hours of data can be recovered.



On connection

While performance monitoring is active the network element will store its most recent data in its bins. On connection with the ITM-CIT and ITM-SC will retrieve all data as present in the bins.

□

PM Data Archiving

ITM-SC Storage capacity

ITM-SC will has the ability to store the raw (the data as sent by the NE) PM data for any configured termination points. This information can be passed on to the ITM-SNM on request. The storage and pruning of data takes place with no intervention from the user.

The volume of data stored depend upon the variation of data generated by the monitored NEs.

Under full network loading the amount of data that can be stored per TP, as a *minimum* is indicated in the table below. To enable the extended storage feature the ITM-SC has to be licensed accordingly.

PM Measurement Period	Number of measurements (bins) stored	Total time stored
Default Storage		
15 minutes (unidir)	96	24 hours
24 hours (uni/bidir)	31	31 days
Extended Storage		
15 minutes (unidir)	672	7 days
24 hours (uni/bidir)	62	62 days

Archiving of PM Data

Because the amount of PM data stored on the ITM-SC is limited (for example 1 month for the 24 hours unidirectional measurement period, without a extended storage license), it is possible to transfer the stored PM data to tape. The archiving of history data allows the user to obtain a long term view of the managed network.

Note that only historic PM data can be archived. The current bins are not available for archiving but can be viewed by using the *Displaying Current Measurements* procedure.

File directory and format

The PM Archive will be stored on the ITM-SC Server or Stand-alone. It will be stored in twofold in the *var/spool/itm/sc/pm_archive* directory. One file (*.ARC.txt) will in a tab separated ASCII format while the other (*.gz) will be in a gz compressed format. The *.gz file can be decompressed by the UNIX command `uncompress`. Other decompress programmes are widely available.

Important! It is not possible to create a PM Archive within 30 minutes of a scheduled Event Archive. This is due to the fact the PM Archive creation process can take a maximum of 30 minutes.

□

Section: ITM-SC Reliability

Overview

Purpose This section provides background information about the databases in the ITM-SC and archiving them.

□

ITM-SC Database

Background

The total software of the ITM-SC can be divided in 4 types of files. Every type has different functionality. They are listed below.

Type	Functionality
System Files	These are the files which remain unaltered when the configuration of the ITM-SC is changed.
Database (Informix)	The database holds all of the configuration data (e.g. MIB) for each of the nodes managed. Also the User Roles and Alarm Stores are within the database.
Unix Configuration File	Stores user information such as password, ID and
ITM-SC Configuration File	Stores system configuration information

Use ITM-SC software

All operations performed on the database should be performed through the ITM-SC. Any attempt to manually modify the database may result in a complete loss of management and could lead to traffic disruption.

Co-resident configuration

On a co-resident configuration both ITM-SC and ITM-NM modules will access the same tape drive on the co-residence server.

□

Archiving

Frequency of backups

If a large number of changes are being made to the managed network (adding new nodes, cross connections etc.), it is recommended that a database backup be made at least once a day. If very few changes are being made, it will not be necessary backing up the same data every day. When archiving more often, note that there is sufficient time for a fault to be identified before all of the tapes contain data with the same ‘error’.

Archiving done on-line

Archiving can be done on-line so there is no loss of management control due to stopping the ITM-SC application. Two options are provided: a scheduled and unscheduled or ad-hoc archive.

Advantage of scheduled archive

The scheduled archive options offers an automatic backup of the Database. Parameters such as time and cycle can be adjusted to perform a customized automatic backup. Whenever a MIB of an NE is locked or an Controller of an NE is busy no backup can be made. After a while the ITM-SC retries to make a backup. The number of retries can be adjusted before automatic archiving is stopped.

Immediate archive

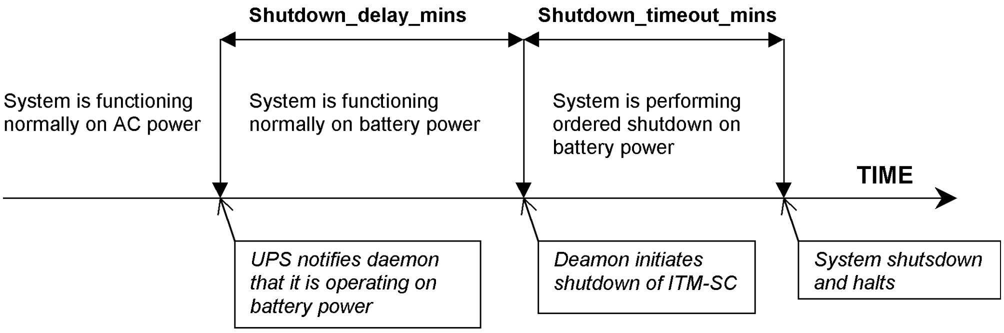
You can initiate an scheduled (immediate) archive to perform an immediate backup. An immediate archive is faster compared to a schedules one because the ITM-SC must be stopped. No system process will interrupt a immediate archive.

□

UPS Installation

Parameters

During the installation the user is asked to set the shutdown delay time and the shutdown time-out time. The shutdown delay time is the period between AC failure and start of the ITM-SC shutdown sequence. The shutdown time-out time is the period between start of the ITM-SC shutdown sequence and the actual shutdown of the UPS. This is detailed in the picture below.


Shutdown_delay_mins
Shutdown_timeout_mins
System is functioning normally on AC power
System is functioning normally on battery power
System is performing ordered shutdown on battery power
TIME
UPS notifies daemon that it is operating on battery power
Deamon initiates shutdown of ITM-SC
System shutsdown and halts

If the AC power is restored before the shutdown_delay_mins period is elapsed, then the system will not be shut down.

□

Section: Management Communication of the ITM-SC

Overview

Purpose This section provides some detailed background about the network address of the ITM-SC.

□

Overview of Maintaining Network Addresses

DCN addresses

The ITM-SC system has two addresses in the DCN:

- Ethernet address
- NSAP address

Ethernet address

The Ethernet address is the unique 6-byte address of a Network Element. Sometimes it is also referred to as the hardware or physical address of the node. The Ethernet address has only local meaning on the Q-LAN and can not be used for routing purposes. It does not contain the information on where the node is in the data communications network. This is also called the System ID (SID).

NSAP address

The Network Service Access Point (NSAP) address is used by the network protocol for location information. The NSAP address of a node is its DCN wide identifier which uniquely identifies the node in the network.

About the ITM-SC

The ITM-SC is normally an end-system (ES) in the DCN. End-systems do not perform routing of data. However the ITM-SC will be an IS when more than one LAN interface is used for OSI communication. In order to restrict the amount of routing data being exchanged the entire data communications network can be divided into areas. In this way the traffic data will be routed from one area to another.

□

Section: Trouble Clearing

Overview

Purpose This section is used to give the reader detailed information about:

- ITM-SC Log Files
- Operator Logs.

Intended use Readers not familiar with one of the topics above are advised to read the respective section before performing any task.

□

ITM-SC Log File Management

Purpose of log file

The ITM-SC Log File records all system related actions such as starting and stopping the ITM-SC.

Log messages may be filtered

Log messages may be “throttled” to enable repeated messages (such as continuous server retry messages) to be filtered and replaced by the first message sent and the subsequent number of retries in a given period.

Log files may be compressed or expanded

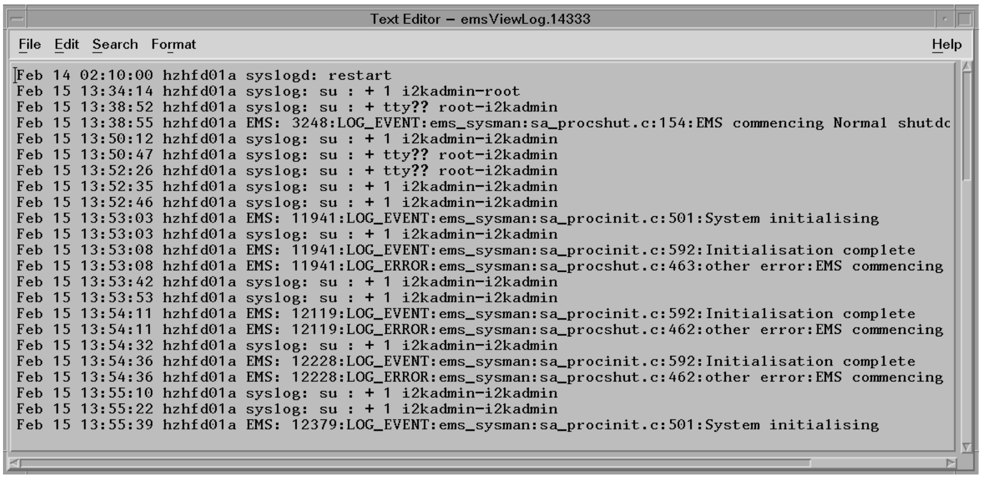
Each Log File may be compressed or expanded. An expanded mode Log File contains messages with all available information about their type, content, source and time of sending. Compressed format logs contain a more abbreviated form.

ITM-SC administrator only

Only an ITM-SC Administrator is able to perform Log File management functions.

Example

An example of the ITM-SC Log Files is displayed below.



```
Feb 14 02:10:00 hzhfd01a syslogd: restart
Feb 15 13:34:14 hzhfd01a syslog: su : + 1 i2kadmin-root
Feb 15 13:38:52 hzhfd01a syslog: su : + tty?? root-i2kadmin
Feb 15 13:38:55 hzhfd01a EMS: 3248:LOG_EVENT:ems_sysman:sa_procshut.c:154:EMS commencing Normal shutdc
Feb 15 13:50:12 hzhfd01a syslog: su : + 1 i2kadmin-i2kadmin
Feb 15 13:50:47 hzhfd01a syslog: su : + tty?? root-i2kadmin
Feb 15 13:52:26 hzhfd01a syslog: su : + tty?? root-i2kadmin
Feb 15 13:52:35 hzhfd01a syslog: su : + 1 i2kadmin-i2kadmin
Feb 15 13:52:46 hzhfd01a syslog: su : + 1 i2kadmin-i2kadmin
Feb 15 13:53:03 hzhfd01a EMS: 11941:LOG_EVENT:ems_sysman:sa_procinit.c:501:System initialising
Feb 15 13:53:03 hzhfd01a syslog: su : + 1 i2kadmin-i2kadmin
Feb 15 13:53:08 hzhfd01a EMS: 11941:LOG_EVENT:ems_sysman:sa_procinit.c:592:Initialisation complete
Feb 15 13:53:08 hzhfd01a EMS: 11941:LOG_ERROR:ems_sysman:sa_procshut.c:463:other error:EMS commencing
Feb 15 13:53:42 hzhfd01a syslog: su : + 1 i2kadmin-i2kadmin
Feb 15 13:53:53 hzhfd01a syslog: su : + 1 i2kadmin-i2kadmin
Feb 15 13:54:11 hzhfd01a EMS: 12119:LOG_EVENT:ems_sysman:sa_procinit.c:592:Initialisation complete
Feb 15 13:54:11 hzhfd01a EMS: 12119:LOG_ERROR:ems_sysman:sa_procshut.c:462:other error:EMS commencing
Feb 15 13:54:32 hzhfd01a syslog: su : + 1 i2kadmin-i2kadmin
Feb 15 13:54:36 hzhfd01a EMS: 12228:LOG_EVENT:ems_sysman:sa_procinit.c:592:Initialisation complete
Feb 15 13:54:36 hzhfd01a EMS: 12228:LOG_ERROR:ems_sysman:sa_procshut.c:462:other error:EMS commencing
Feb 15 13:55:10 hzhfd01a syslog: su : + 1 i2kadmin-i2kadmin
Feb 15 13:55:22 hzhfd01a syslog: su : + 1 i2kadmin-i2kadmin
Feb 15 13:55:39 hzhfd01a EMS: 12379:LOG_EVENT:ems_sysman:sa_procinit.c:501:System initialising
```

□

Operator Logs

Overview

The Operator Log will show all actions and operations done by an ITM-SC user on the ITM-SC. Each action and attempted operation is recorded in the operator log as a record.A history of the operations are maintained for all users. This can be usefull when track down actions done on the ITM-SC.

Fields in log record

Each record for an action or operation contains the following attributes:

Attribute	Meaning
User Name	Login ID of person who performs the action
Host Name	The host ID from which the operation was attempted.
Node name	Name of NE or Node the action was submitted to.
Operation code	Type of operation.
Operation result	Type of result. This can be for example *`failed`* or *`passed`* .
Additional information	Supplies additional information.
Date and time	When operation took place.

Privileges

The ITM-SC Administrator can view all records stored on the system, regardless of the user who created them. The ITM-SC Administrator also can determine which attribute remains invisible for a user. This can be set differently for each user. The administrator can also store records onto external devices, such as diskettes.

The ITM-SC Supervisor and ITM-SC Operator will be able to view records created by their own operations only. The attributes they can view can be limited, due to extra control options, by the administrator.

Control options

The ITM-SC Administrator can restrict a user to display a limited set of attributes of their records. The hostname, date-time, node-name, result and additional information attributes can be hidden to the user.

Filter and sort options

All ITM-SC users can read records which match only his or her own operator ID. This set of records can be filtered and sorted to limit the number of Operator Log records. Also attributes can be suppressed to hide unwanted information.

□

11 Using the ITM-SC Interface

Overview

Purpose Using the ITM-SC interface provides information on how to use the Integrated Transport Management-Subnetwork Controller (ITM-SC).

Objectives To customize or change settings of the ITM-SC Interface according to the users needs.

Outcome Be able to work with the ITM-SC Interface.

Intended Use This chapter contains four sections. The first section described the HP-Vue specific subjects. The other sections describe the subjects which are more ITM-SC specific, such as Module description, general ITM-SC tasks and the Network Map.

Each section starts with a conceptual explanation and, if available, this is followed by a procedure.

□

Section: HP-Vue Specific Subjects

Overview

Purpose This section describes the more HP-Vue specific subjects such as:

- Buttons and Mouse usage.
- The general software modules.

□

Front Panel

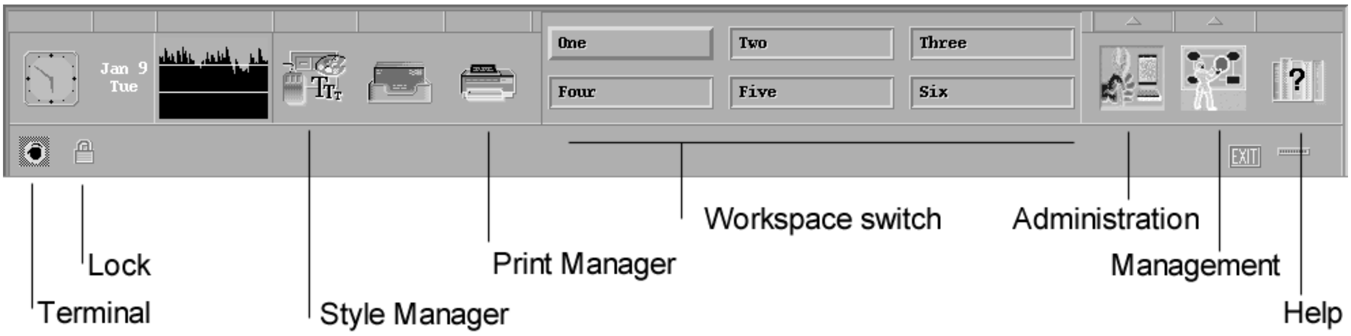
About the ITM-SC Front Panel

To navigate and control the ITM-SC application, the HP graphical user interface (GUI) displays a front panel. Depending on the user class, a number of different icons on the front panel give access to the different modules of the application. The procedure to open or close a module is explained and a short description of the modules is given.

The front panel window is different for administrator, supervisor and operator.

System Administrator Front Panel

The front panel of the system administrator is shown below.



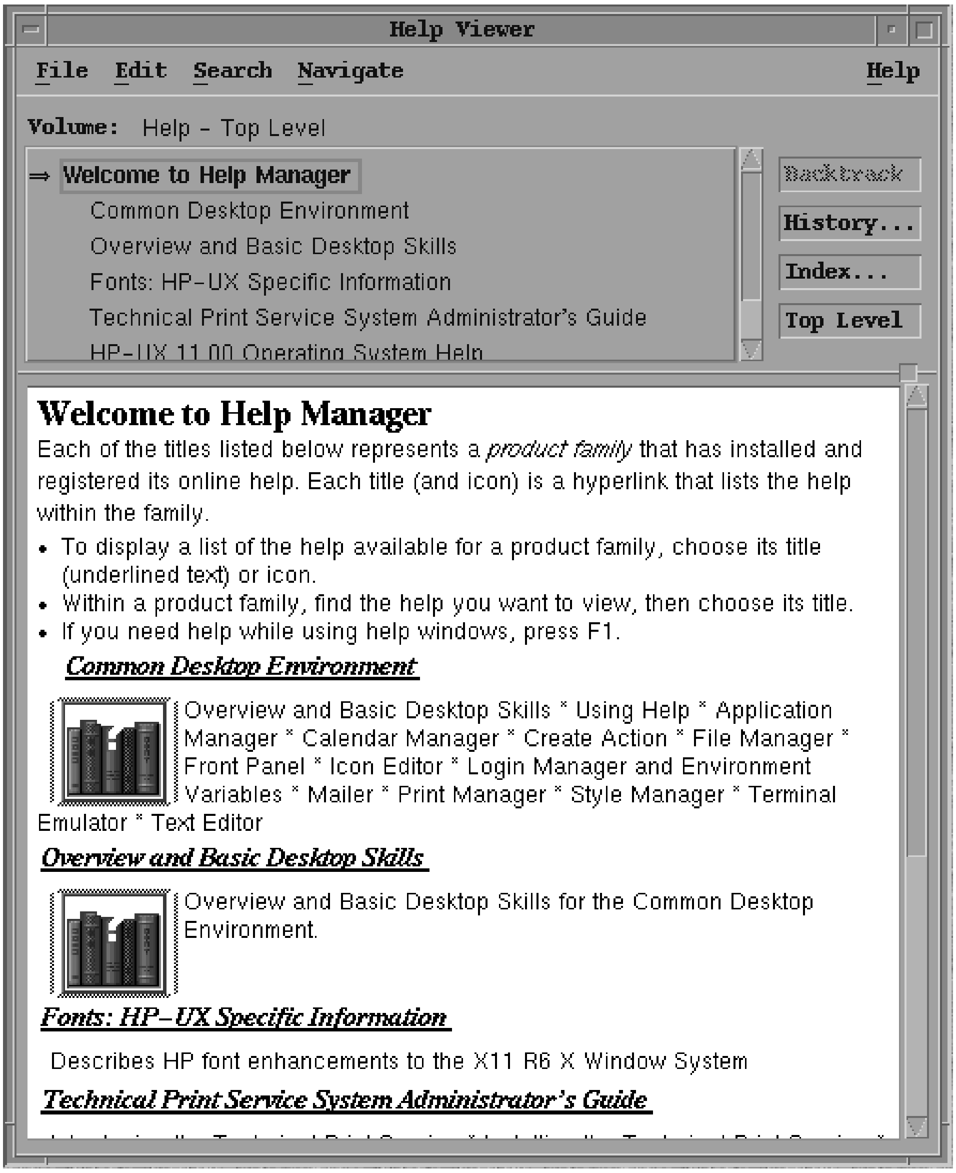
□

General Modules

Purpose General modules available to each user are described below. For more information about the general modules can be found in the on-line documentation via the Help button. Refer to System Administrator Front Panel to locate the buttons and modules.

Help Manager The Help Manager provides access to online help for HP-VUE. This information includes coverage of workstation controls and tool use.

The Help Manager menu is shown below.



Volume: Help – Top Level

⇒ **Welcome to Help Manager**
Common Desktop Environment
Overview and Basic Desktop Skills
Fonts: HP–UX Specific Information
Technical Print Service System Administrator's Guide
HP–UX 11.00 Operating System Help

Welcome to Help Manager

Each of the titles listed below represents a *product family* that has installed and registered its online help. Each title (and icon) is a hyperlink that lists the help within the family.

- To display a list of the help available for a product family, choose its title (underlined text) or icon.
- Within a product family, find the help you want to view, then choose its title.
- If you need help while using help windows, press F1.

Common Desktop Environment

Overview and Basic Desktop Skills * Using Help * Application Manager * Calendar Manager * Create Action * File Manager * Front Panel * Icon Editor * Login Manager and Environment Variables * Mailer * Print Manager * Style Manager * Terminal Emulator * Text Editor

Overview and Basic Desktop Skills

Overview and Basic Desktop Skills for the Common Desktop Environment.

Fonts: HP–UX Specific Information

Describes HP font enhancements to the X11 R6 X Window System

Technical Print Service System Administrator's Guide

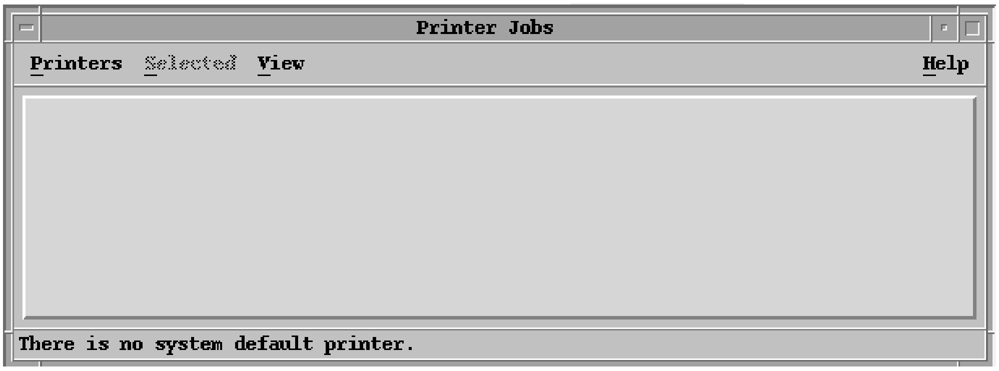
Print Manager

The Print Manager makes it possible to:

- Check the status of a print job.
- Cancel a print job.

The Print Manager Menu differs depending on the printers that are defined with the System Administration Manager (SAM). (Refer to the Subnetwork Installation Guide).

The Print Manager icon gives access to a menu of available printers.



There is no system default printer.

Workspace Switch

The Workspace Switch provides greater workspace flexibility by using a virtual window on which multiple windows can be created.

Several workspaces can be selected on the workstation, however only one of these is shown on the physical window at a time.

Style Manager

The Style Manager makes it possible to customize visual elements and the workstation behavior. Select the Style Manager icon to access the menu for customizing.

Icons on the Style Manager menu are described below:

Menu Option	Function
Color	Sets workspace colors and palettes.
Font	Sets HP-VUE font sizes.
Backdrop	Sets workspace backdrop pattern.
Keyboard	Sets keyboard click volume and character repeat settings.

Menu Option	Function
Mouse	Sets mouse left or right handed control, button click settings, double click speed, pointer acceleration and pointer movement threshold.
Audio	Sets beeper volume, tone and duration.
Screen	Sets number of minutes before the window times out to prevent burn out of the monitor, and set password protection at time out.
Window	Sets the way windows are opened and activated.
Startup	Sets the start up and ending of a session.

Screen Saver Options

A screen saver will protect the terminal window from burned-in images and enhances security by blanking the screen. Note that a screen saver does not password protect the screen. When requiring a password lock activate the screenlock as well.

The Screen Saver is invoked when no keyboard or mouse activity occurs after a predetermined time. Applications active when the Screen Saver is invoked remain open. However, those applications are subject to their time-out restrictions.

Screen Saver properties can be set only when the user is logged in as `root`. The ITM-SC Administrator as well as the other ITM-SC users do *not* have the rights to change these settings.

The Screen Saver time-out can be set from 1 minute to 120 minutes. Options for the screen saver are described below:

Option	What It Does
Time-out	Specifies the time interval (from 1 to 120 minutes) from the last mouse move or keystroke to when the window times out. The slider control decreases or increases the number of minutes.
Full Screen Cover	Determines whether or not to completely cover the window when Lock is used from the front panel.

Terminal Window

The Terminal icon provides access to a terminal window.

A terminal window is a screen that allows HP-UX commands to be executed.

□

Buttons and Mouse Movement

Button Names and Functions

The ITM-SC guides the user through the system by means of windows. These windows can contain the following buttons:

Button	Function
`Apply`	Executes the changes made. The window remains open to permit similar action.
`OK`	Accepts or executes changes and closes the window.
`Edit`	Provides the option to change data in shown data entry fields. A different window can be displayed.
`Close`	Closes the window and resumes normal operation of the application, without changes.
`Print`	Prints the information to the selected output.
`Help`	Provides additional information through the context-sensitive on-line help.
`Cancel`	Cancels the selected action or changes.

Using the Mouse

Mouse movements are described in the table below:

Movement	Function
`Select`	Select an object or menu item, click the left button (default) on the mouse with the pointer on the object.
`Drag`	To move an object to an other location, select the object by using the left button (default). Then click it with the middle mouse button and hold that button down, while moving the mouse.
	To move a group of objects to another location, use the left button to define a box over the group of objects and move the box. Moving of a group can also be done by pressing **Ctrl** + **left mouse button** to select each object of the group. Then click it with the middle mouse button and hold that button down, while moving the mouse.
`Menu`	To display a menu that is associated with the pointer location or the selected object, click the right button (default) of the mouse.

□

Section: ITM-SC Specific Modules and Windows

Overview

Purpose

This section describes subjects which are more ITM-SC specific. Subjects described in the section are:

- ITM-SC specific modules
- General ITM-SC windows
- Main EMS menu window

□

Accessing the ITM-SC Specific Modules

Module Icons

Some of the modules on the frontpanel have submenus for accessing one or more applications. The Management and Administration module both contain several applications.

Opening a Module

Select the triangle just above the modules to open the modules.

Closing a Module

Modules can be closed by selected closing the window (or **ALT-F4**) or by selecting the triangle at the bottom of the menu.

□

Management Module

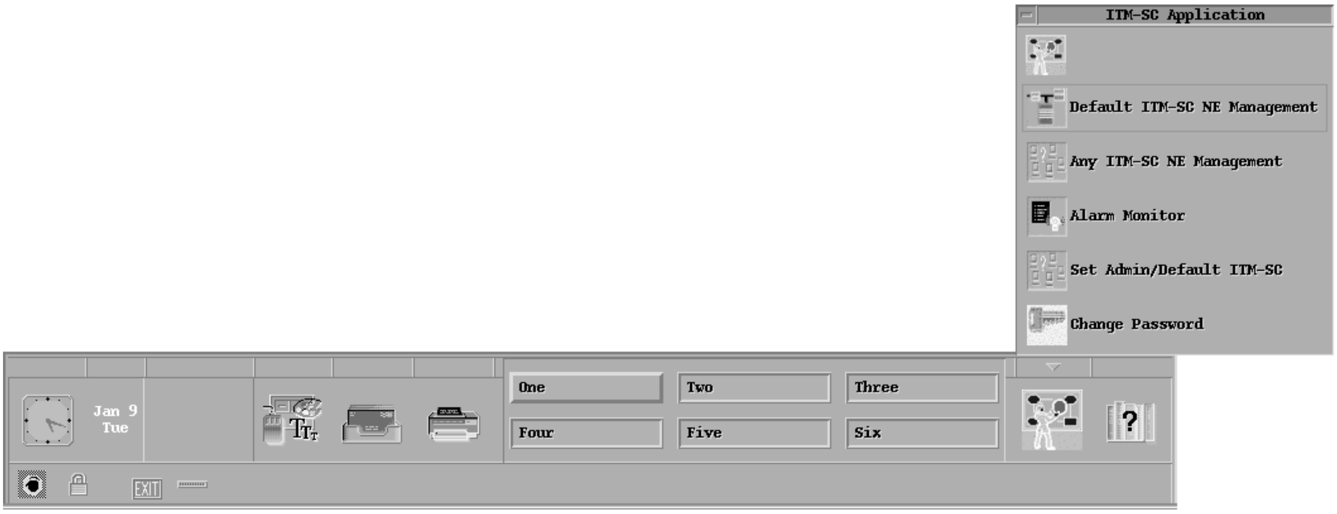
Purpose

Through the Management Module the operator has the choice to:

- Start the network element management.
- Monitor a number of ITM-SCs for raised alarms.

Management Menu

The Management menu provides options for managing network elements.



Menu Options

Selections on the Management menu are described below:

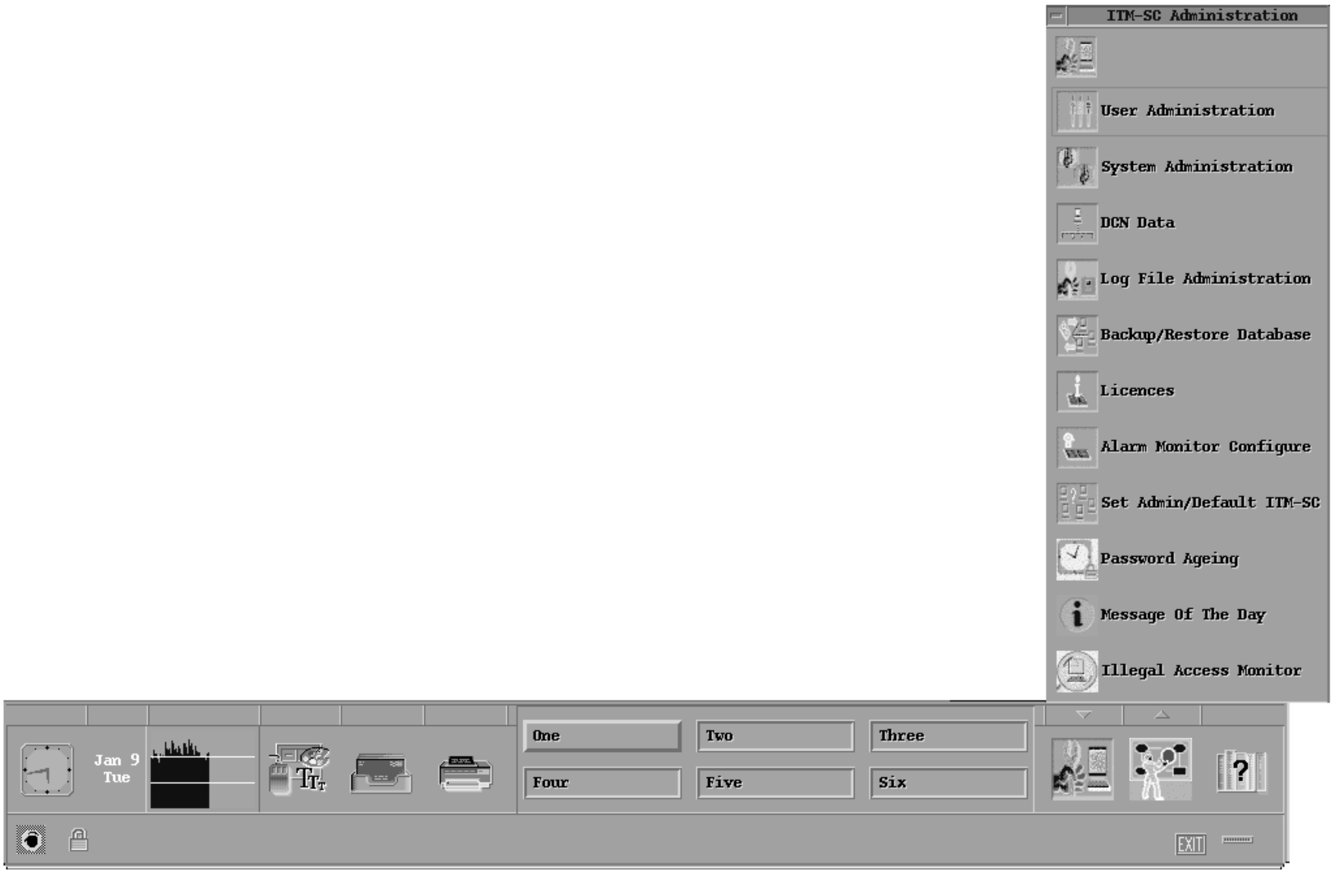
Menu Option	Function
Default ITM-SC NE Management	Default ITM-SC NE Management allows the user to access the default ITM-SC server.
Any ITM-SC NE Management	Any ITM-SC NE Management allows the user to access any ITM-SC server.
Alarm Monitor	Alarm Monitor to configure, start and stop the monitoring of listed ITM-SCs for raised alarms. This is only relevant for a multi-server configuration.
Set Admin/Default ITM-SC	Set Admin/Default ITM-SC allows the user to change the default ITM-SC server.
Change Password	Change password allows to change the ITM-SC password of the user currently logged in.

□

Administration Module

Purpose The Administration Module is only accessible when the administrator is logged in. This module gives access to the ITM-SC administration tasks.

Administration Menu The Administration menu is shown below:



Menu Options The Administration menu options are described below:

Menu Option	Function
User Administration	Add, delete or modify user logins.
System Administration	Start or stop the ITM-SC application.
DCN Data	Manage the Data Communications Network data.
Log File Administration	View or delete ITM-SC logins.
Backup/Restore Database	Backup or restore the application database.

Menu Option	**Function**
Licences	Enter or change licence information.
Alarm Monitor Configure	Configure a selected server to provide system alarm monitoring information.
Set Admin/Default ITM-SC	Select the server to which the subsequent administration commands are applied to.
Password Ageing	Enable/disable the password ageing parameters.
Message Of The Day	Enable/disable the message of the day parameters.
Illegal Access Monitor	Enable/disable the illegal access monitor parameters.

□

General ITM-SC Windows

Introduction

The Element Management System (ITM-SC) contains four types of windows:

- EMS-Menu.
- Selection Dialog window.
- Information window.
- Edit window.

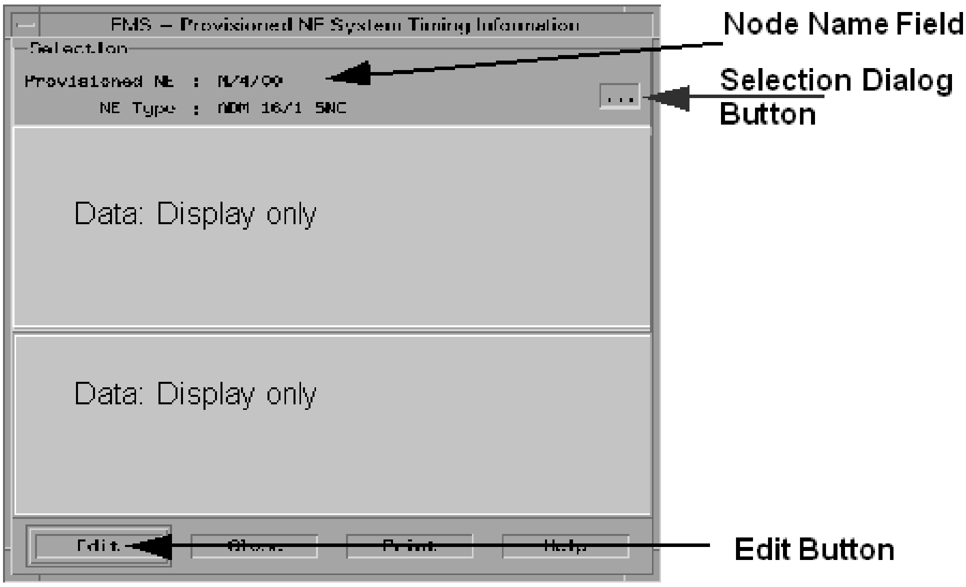
Button Names and Functions

The ITM-SC guides the user through the system by means of windows. These windows can contain the following buttons:

Button	Function
`Apply`	Executes the changes made. The window remains open to permit similar action.
`OK`	Accepts or executes changes and closes the window.
`Edit`	Provides the option to change data in shown data entry fields. A different window can be displayed.
`Close`	Closes the window and resumes normal operation of the application, without changes.
`Print`	Prints the information to the selected output.
`Help`	Provides additional information through the context-sensitive on-line help.
`Cancel`	Cancels the selected action or changes.

Information Window

An Information window makes it possible to change or view information of a component (for instance a node).



EMS – Provisioned NE System Timing Information

Selection

Provisioned NE : M/4/90
NE Type : ADM 16/1 SNC

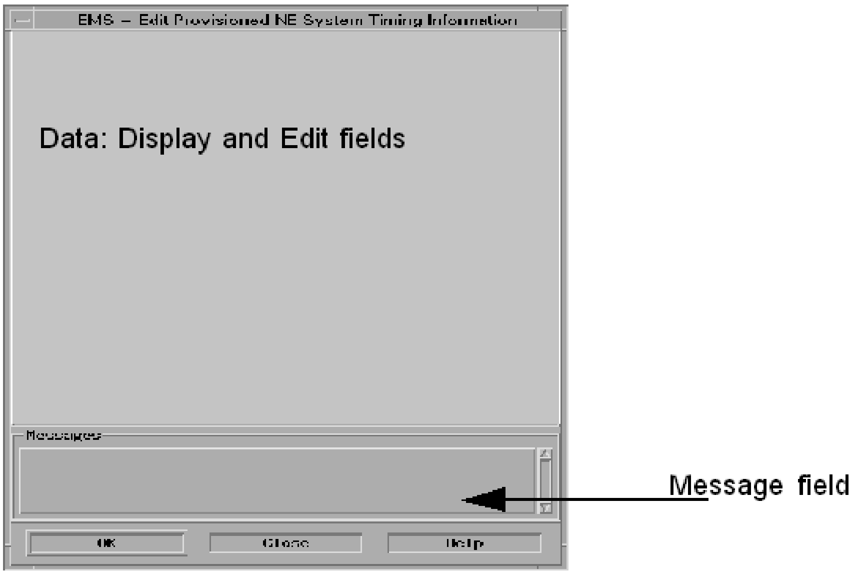
Data: Display only

Data: Display only

It is possible to click on the selection dialogue button to select a specific NE. When clicking the selection dialogue button a list with node names appears. From this list a node can be selected to edit or view the nodes information.

Edit Window

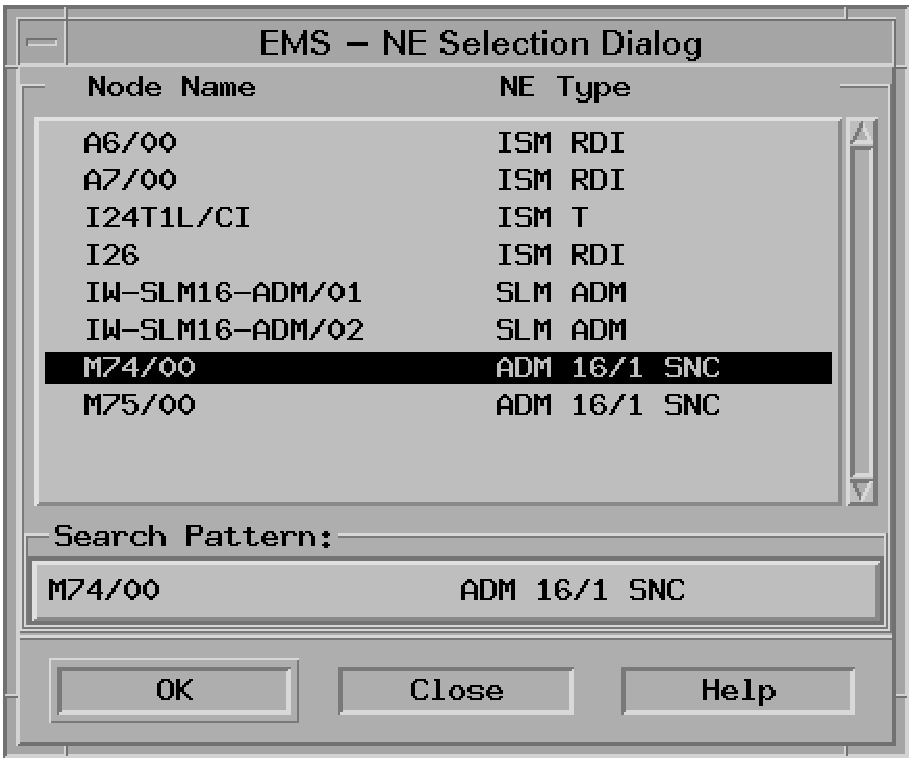
An Edit window makes it possible to edit the data of a network element. The message field will display information about the action performed by the ITM-SC.


EMS – Edit Provisioned NE System Timing Information
Data: Display and Edit fields
Messages
Message field
OK
Close
Help

Selection Dialog Window

The Selection Dialog window makes it possible to select a NE, slot, port, termination point, time, date etc. out of a list. The chosen items will be used to edit the characteristics of the item or filter lists by means of the item.

This example window below provides a list of network elements.



Node Name	NE Type
A6/00	ISM RDI
A7/00	ISM RDI
I24T1L/CI	ISM T
I26	ISM RDI
IW-SLM16-ADM/01	SLM ADM
IW-SLM16-ADM/02	SLM ADM
M74/00	ADM 16/1 SNC
M75/00	ADM 16/1 SNC

Search Pattern: M74/00 ADM 16/1 SNC

To speed up the search for an item the Search Pattern can be used. When using the Search pattern and when a match for the typed selection is found, the found item is highlighted in the list. When more than one match is found, the first match is marked with a diamond symbol.

□

Main EMS—Menu Window

Introduction

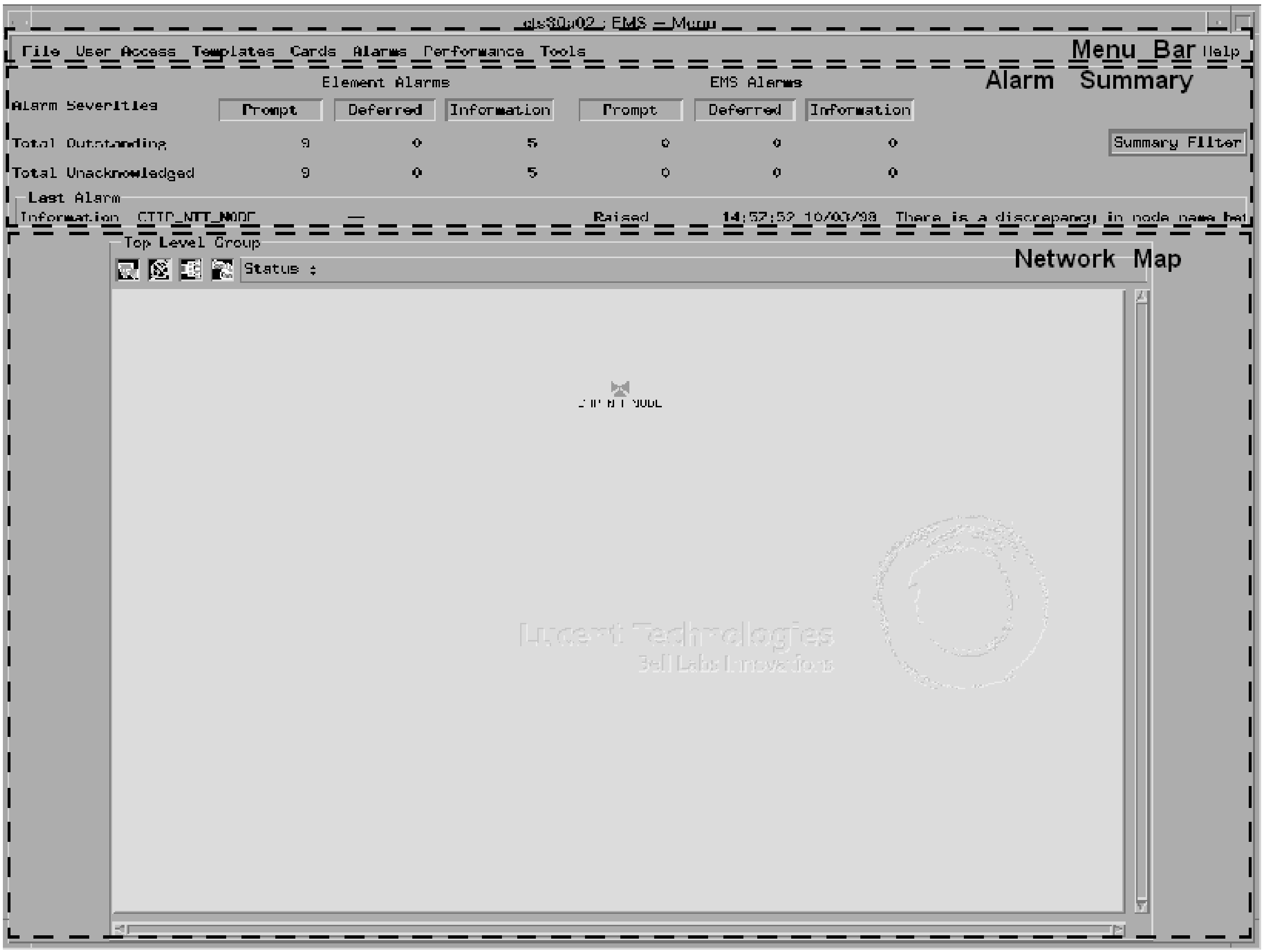
The EMS - Menu window is the main window of the ITM-SC application. The EMS - Menu contains several fields that either provide information about the current status of the network element, or that can be used to manage the network element.

Parts of the EMS - Menu

The EMS - Menu can be divided into three parts:

- Menu Bar.
- Alarm Summary.
- Network Map.

The picture below distinguishes the 3 parts.



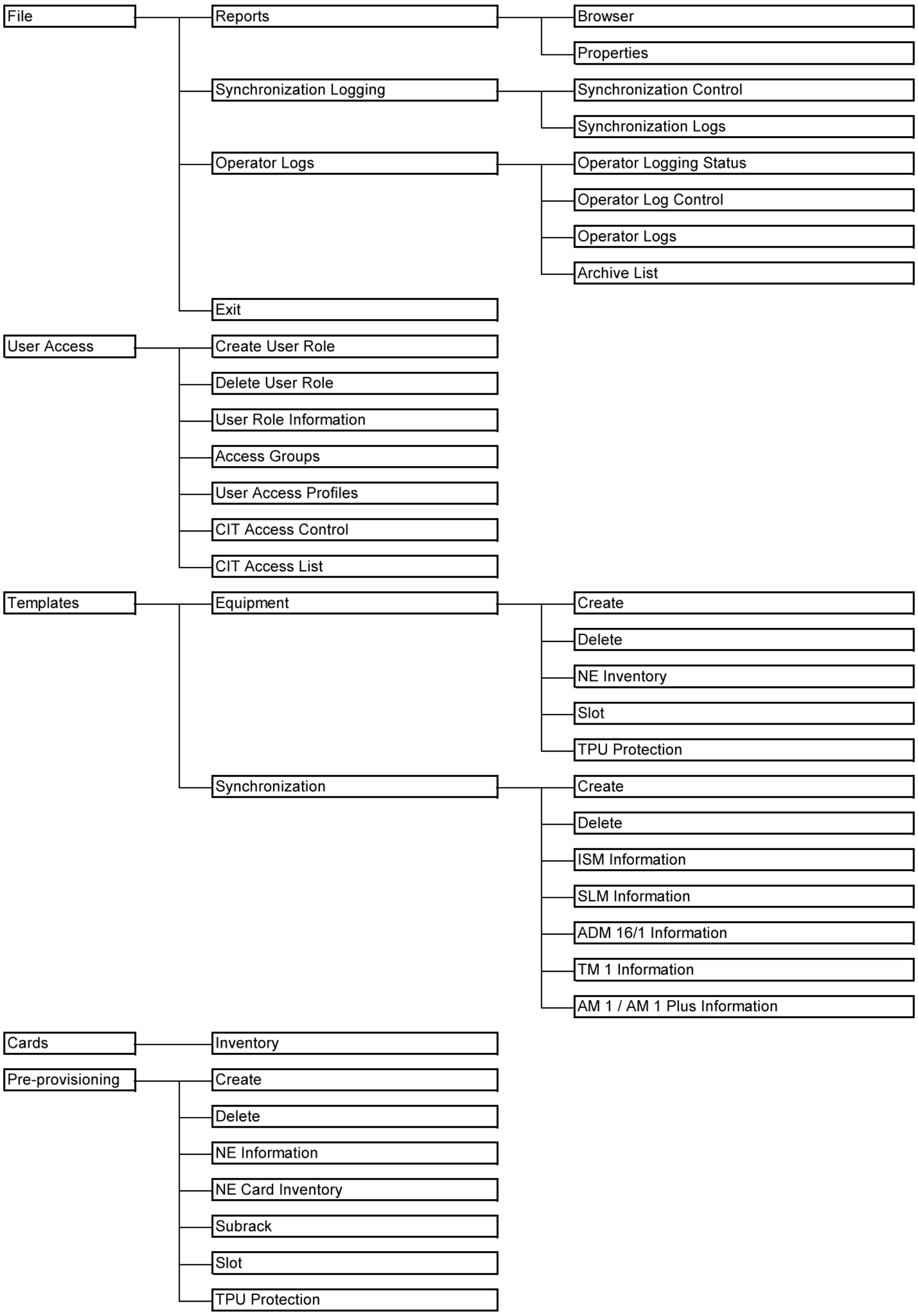
Alarm Severities	Element Alarms Prompt	Element Alarms Deferred	Element Alarms Information	EMS Alarms Prompt	EMS Alarms Deferred	EMS Alarms Information
Total Outstanding	9	0	5	0	0	0
Total Unacknowledged	9	0	5	0	0	0

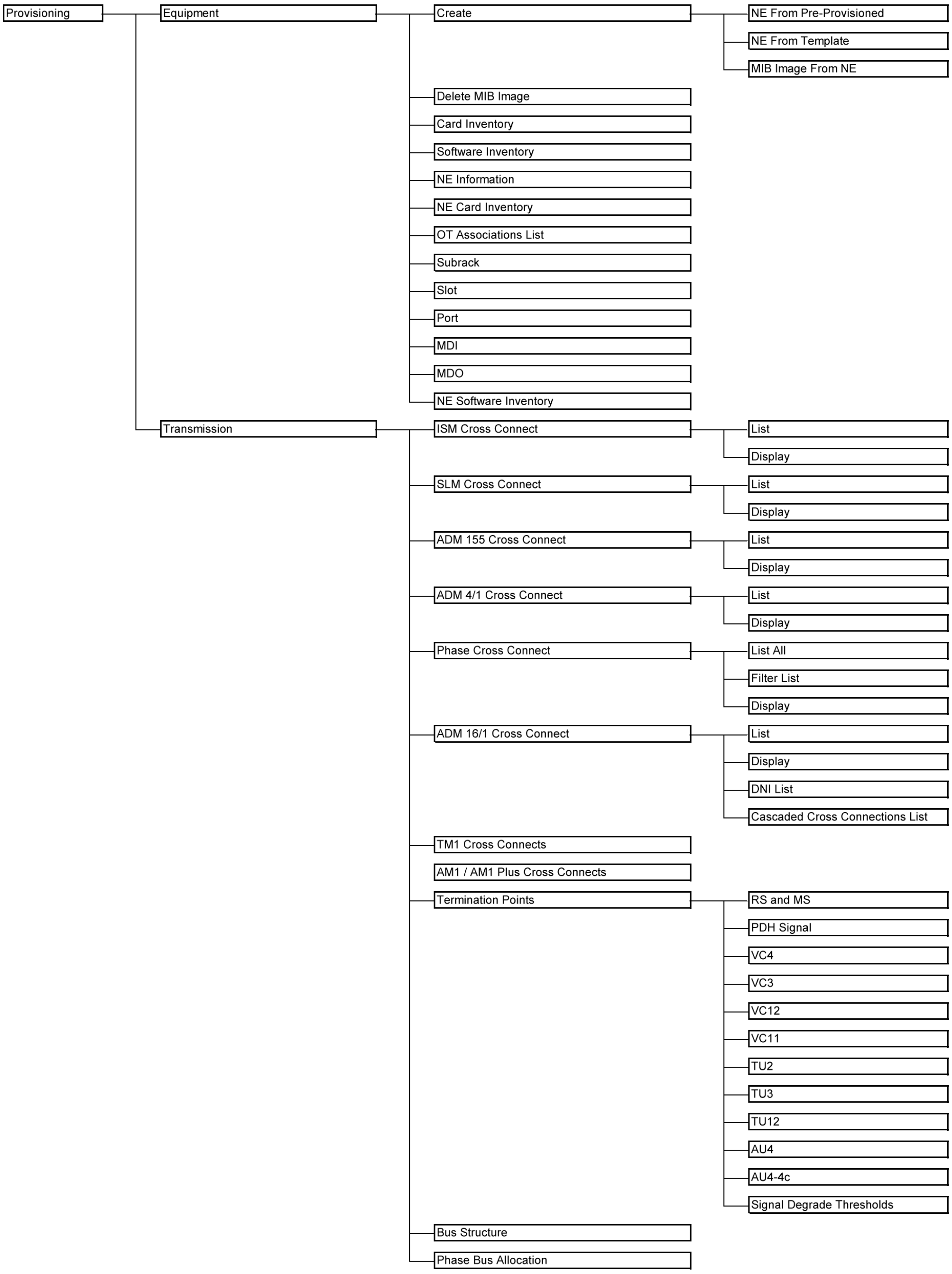
Last Alarm

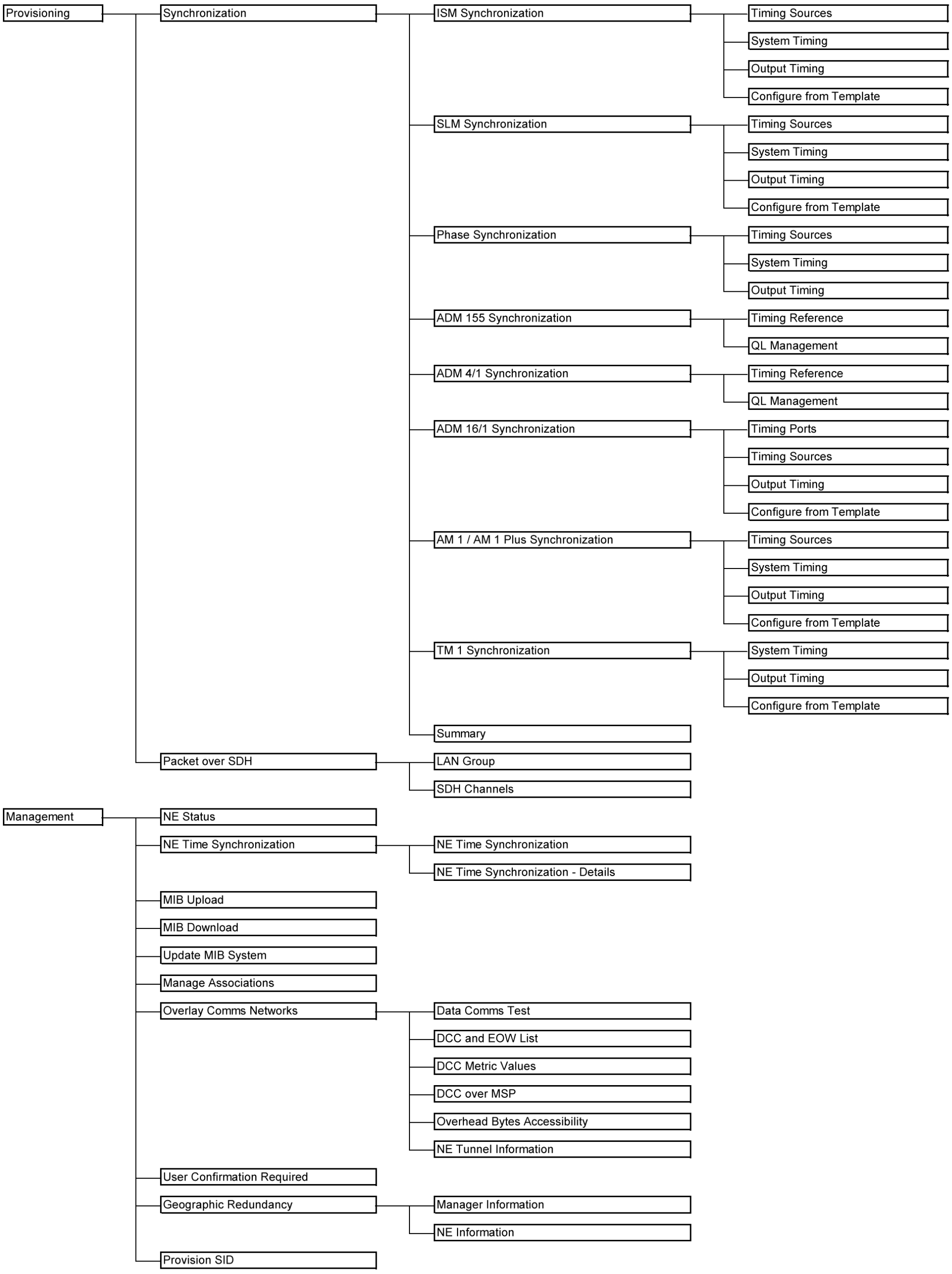
Information CTIP_NTT_NODE — Raised 14:57:52 10/03/98 There is a discrepancy in node name bet

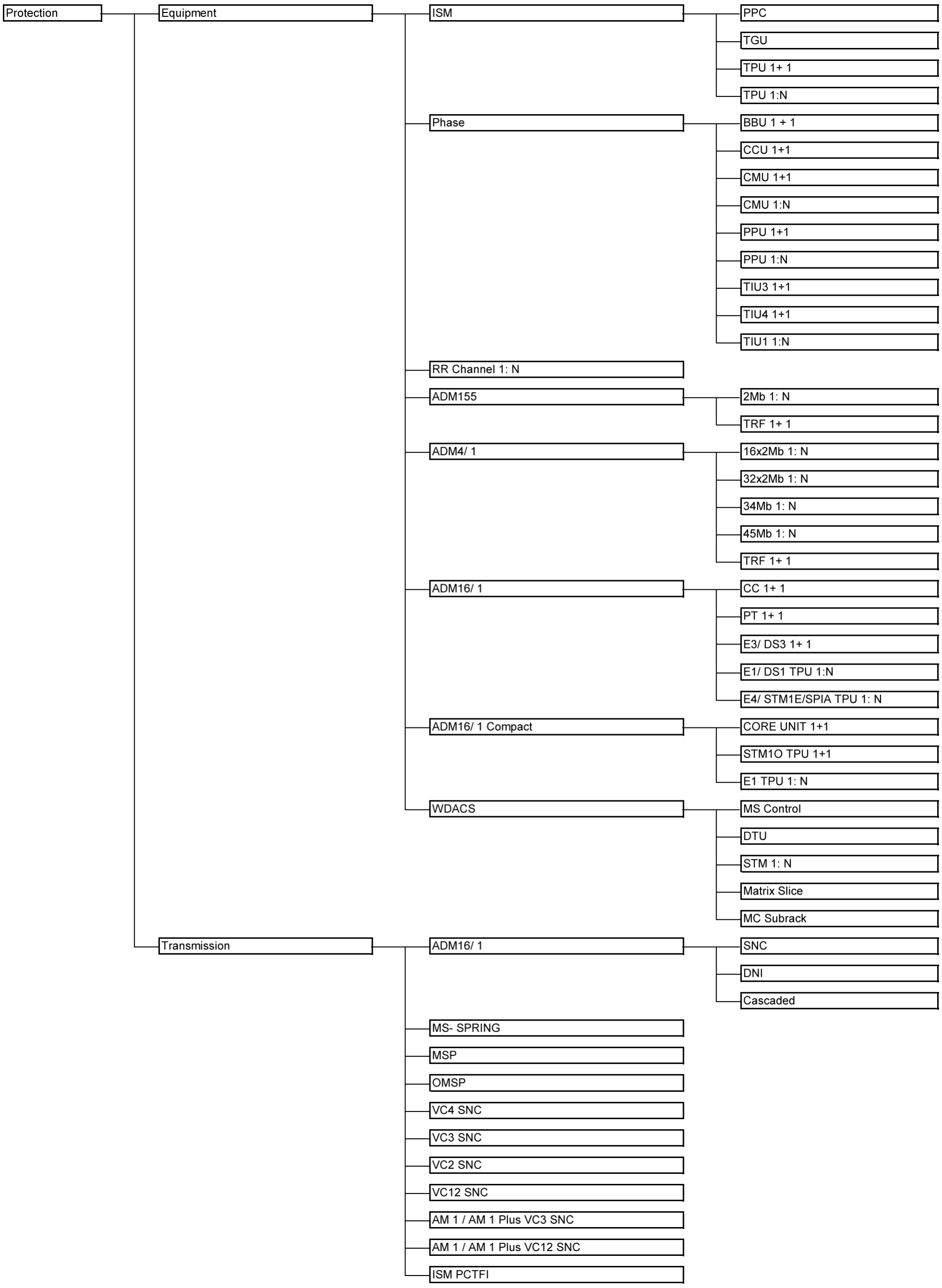
Menu Bar Via the Menu Bar it is possible to manage the network element. It consist of several buttons that have one or more submenus attached to it. By clicking a menu bar button, the submenus will scroll down and the submenu that is required can be selected. These submenus can, on their part, contain several sub-submenus as well.

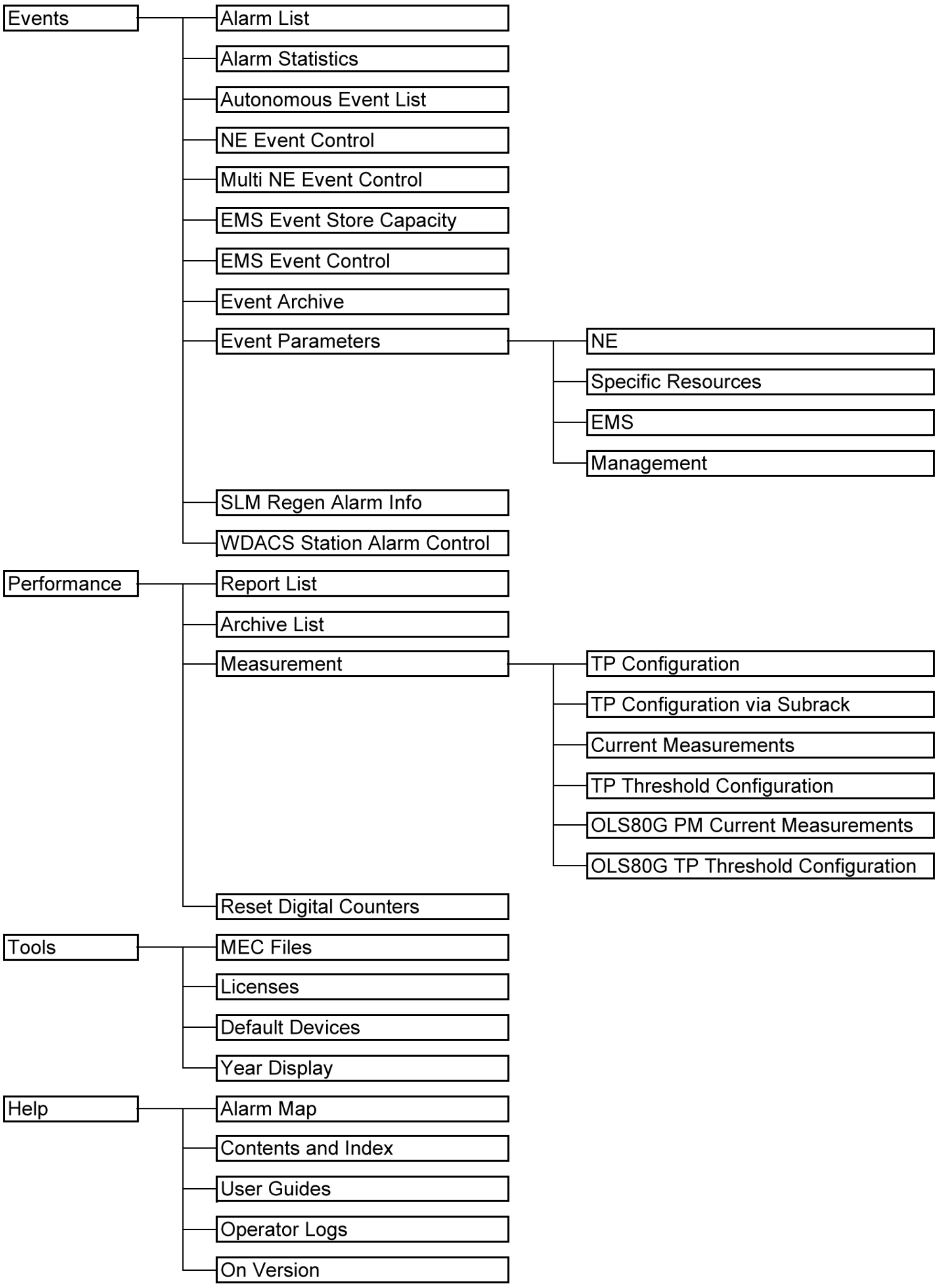
Menu bar structure The structure underlying the menu bar is as follows:




Provisioning
Equipment
Create
NE From Pre-Provisioned
NE From Template
MIB Image From NE
Delete MIB Image
Card Inventory
Software Inventory
NE Information
NE Card Inventory
OT Associations List
Subrack
Slot
Port
MDI
MDO
NE Software Inventory
Transmission
ISM Cross Connect
List
Display
SLM Cross Connect
List
Display
ADM 155 Cross Connect
List
Display
ADM 4/1 Cross Connect
List
Display
Phase Cross Connect
List All
Filter List
Display
ADM 16/1 Cross Connect
List
Display
DNI List
Cascaded Cross Connections List
TM1 Cross Connects
AM1 / AM1 Plus Cross Connects
Termination Points
RS and MS
PDH Signal
VC4
VC3
VC12
VC11
TU2
TU3
TU12
AU4
AU4-4c
Signal Degrade Thresholds
Bus Structure
Phase Bus Allocation


Provisioning
Synchronization
ISM Synchronization
Timing Sources
System Timing
Output Timing
Configure from Template
SLM Synchronization
Timing Sources
System Timing
Output Timing
Configure from Template
Phase Synchronization
Timing Sources
System Timing
Output Timing
ADM 155 Synchronization
Timing Reference
QL Management
ADM 4/1 Synchronization
Timing Reference
QL Management
ADM 16/1 Synchronization
Timing Ports
Timing Sources
Output Timing
Configure from Template
AM 1 / AM 1 Plus Synchronization
Timing Sources
System Timing
Output Timing
Configure from Template
TM 1 Synchronization
System Timing
Output Timing
Configure from Template
Summary
Packet over SDH
LAN Group
SDH Channels
Management
NE Status
NE Time Synchronization
NE Time Synchronization
NE Time Synchronization - Details
MIB Upload
MIB Download
Update MIB System
Manage Associations
Overlay Comms Networks
Data Comms Test
DCC and EOW List
DCC Metric Values
DCC over MSP
Overhead Bytes Accessibility
NE Tunnel Information
User Confirmation Required
Geographic Redundancy
Manager Information
NE Information
Provision SID


Protection
Equipment
ISM
PPC
TGU
TPU 1+ 1
TPU 1:N
Phase
BBU 1 + 1
CCU 1+1
CMU 1+1
CMU 1:N
PPU 1+1
PPU 1:N
TIU3 1+1
TIU4 1+1
TIU1 1:N
RR Channel 1: N
ADM155
2Mb 1: N
TRF 1+ 1
ADM4/ 1
16x2Mb 1: N
32x2Mb 1: N
34Mb 1: N
45Mb 1: N
TRF 1+ 1
ADM16/ 1
CC 1+ 1
PT 1+ 1
E3/ DS3 1+ 1
E1/ DS1 TPU 1:N
E4/ STM1E/SPIA TPU 1: N
ADM16/ 1 Compact
CORE UNIT 1+1
STM1O TPU 1+1
E1 TPU 1: N
WDACS
MS Control
DTU
STM 1: N
Matrix Slice
MC Subrack
Transmission
ADM16/ 1
SNC
DNI
Cascaded
MS- SPRING
MSP
OMSP
VC4 SNC
VC3 SNC
VC2 SNC
VC12 SNC
AM 1 / AM 1 Plus VC3 SNC
AM 1 / AM 1 Plus VC12 SNC
ISM PCTFI



Alarm Summary

The Alarm Summary provides an overview of the alarms risen on both the NEs and the NE management system. A more detailed description of the alarm summary can be found in the chapter “Event Management”.

Network map

The Network Map is the main window for managing all NEs within the subnetwork and gives direct information about NEs their status. A more detailed description of the Network Map can be found in the section “Network Map” of this chapter.

□

Section: ITM-SC General Tasks

Overview

Purpose

This section describes subjects which are ITM-SC related such as:

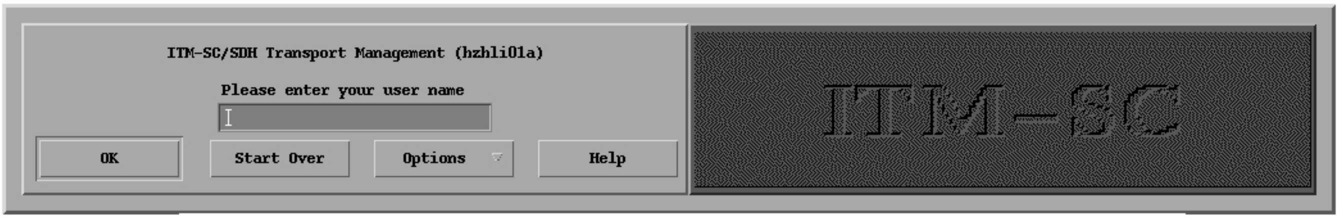
- Accessing the ITM-SC.
- Changing of ITM-SC passwords.
- ITM-SC Reports
- Log out of the ITM-SC.

□

Parameters for Accessing the ITM-SC

Login Before the ITM-SC application can be started the user needs to login.

Window to use The following window is used to login into the ITM-SC.



ITM-SC/SDH Transport Management (hzhli01a)

Please enter your user name

Login and Password The login or user name has up to 8 alphanumeric characters (a..z, A..Z, 0..9). The Password requires a minimum of 6 characters (a..z, A..Z, 0..9 and other printable characters e.g. - * +) with at least 2 alphabetic characters and at least 1 non alphabetic character.

Button Description Buttons on the window are described below:

Button	**Function**
OK	Confirms the start of the login after filling in the “Login” and “Password” fields.
Start Over	Removes data from the “Login” and “Password” fields. Lets the user begin the login procedure again, without registering a login attempt. Clear is quicker than backspacing, which can also be used.
Options	Displays a menu containing Restart Server, Copyright, Fail-safe Session, HP-VUE Lite Session, HP-VUE Session and Languages. These items are HP specific and control features of the workstation and what happens after login. For more information about the selectable items, refer to the HP system documentation.
Help	Provides information on how to login.

□

Accessing the ITM-SC

Purpose To login in to the ITM-SC.

Related information For more information on the parameters used refer to:

- Parameters for Accessing the ITM-SC

Procedure Perform the following procedure to Log in to the ITM-SC.

1 Enter Login (user name) and click OK or press **ENTER**.

2 Enter password. Click OK or press **ENTER**.

Result:

If the login is successful, an HP copyright message appears. After this the Front Panel appears.

An “Incorrect Login” message appears when the login or password entered is incorrect. Press **ENTER** or click OK when this message appears. After this the login process can be restarted.

END OF STEPS

□

Changing Password

Purpose

To increase the security of the ITM-SC and its network managed the user is able to change his/her own ITM-SC password.

Before you begin

In this procedure a shell window is provided to change the password. A script will guide the user through the change of password.

Related information

Related procedures are:

- Modifying ITM-SC User Information
- Configuring Password Ageing.

Procedure

Follow the script below to change the ITM-SC password.

1 Open the *ITM-SC Management* menu and select the *Changing Password* icon.

Result:

A shell window appears asking the user for the current password.

2 Enter the current password. Press **ENTER**.

Result:

The user is asked to enter a new password.

3 Enter a new password. Press **ENTER**.

Result:

The user is asked to re-enter the new password.

4 Re-enter the new password. Press **ENTER**.

Result:

If the new password is accepted the following message will appear: Password has been updated successfully. The shell window will disappear automatically.

END OF STEPS

□

Report Concepts

Background

When selecting anywhere in the ITM-SC the `Print` button, system information that is shown in that window, can be sent to two different outputs. It can be printed directly to a printer or to a file (a report). A report will be stored on the ITM-SC for later use.

File directory and format

If a report is created a file, representing the report, is stored on the ITM-SC.

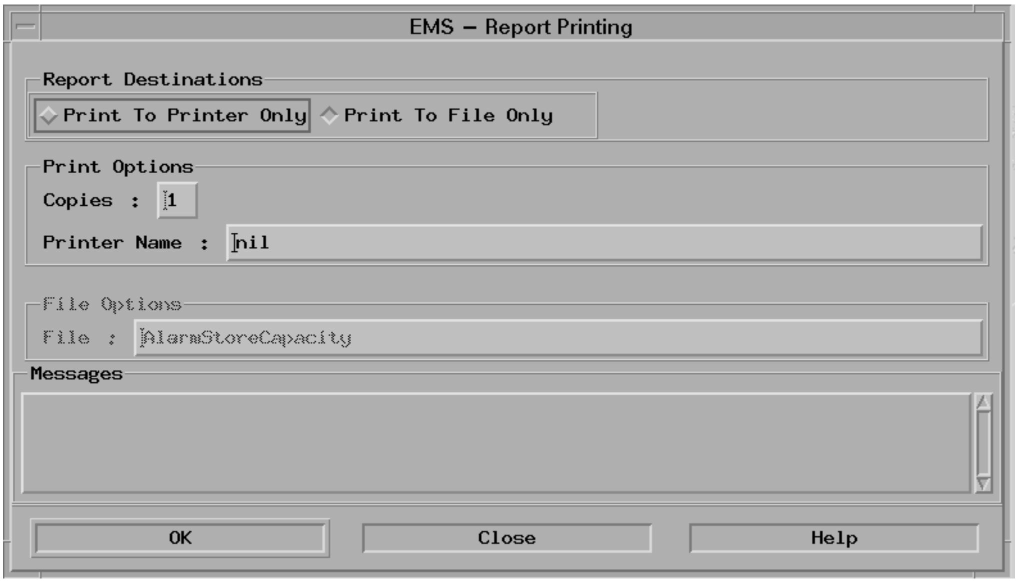
The location of these files is: */var/spool/itm/sc/reports/<ServerName>/* where <*ServerName*> is the name of the server. The format of these files are ASCII.

Limited printing capacity

When printing long reports, only the first 2000 lines will be printed. The user will be notified if the report is not printed entirely.

Report Printing window

The Report Printing window allows the user to decide which type of output is generated.


EMS – Report Printing

Report Destinations

◇ Print To Printer Only ◇ Print To File Only

Print Options

Copies : 1

Printer Name : nil

File Options

File : AlarmStoreCapacity

Fields to Use

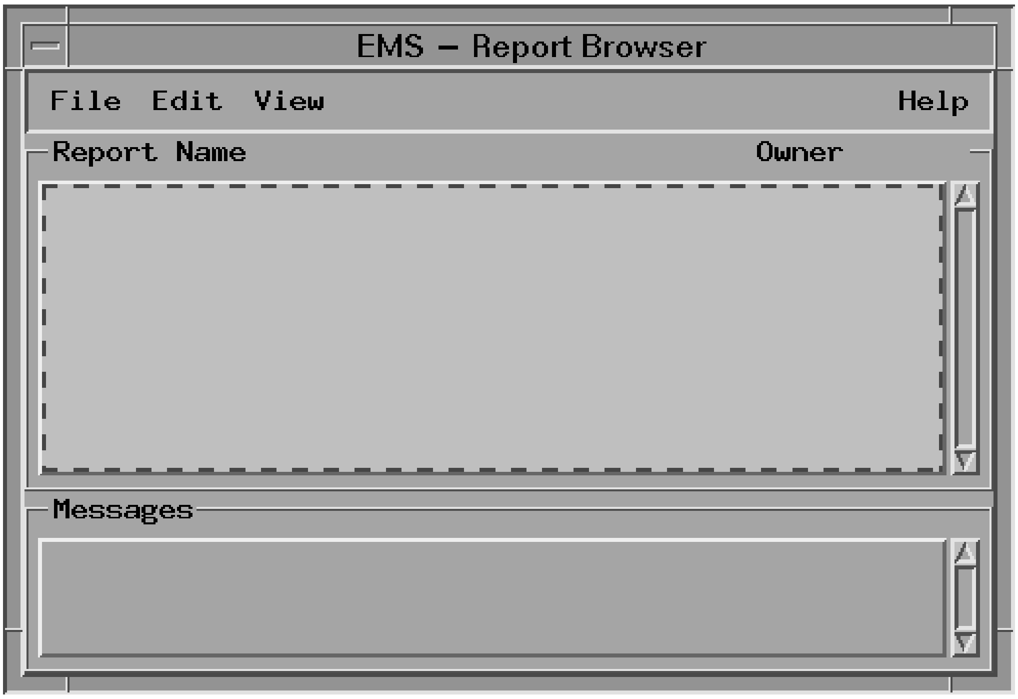
Use these fields to determine the print output:

Field	Description
Report Destinations	Shows the possible outputs: Printer or File. *Print to Printer Only* is the default setting.

Field	Description
Print Options	Is only highlighted if *Print to Printer Only* is selected. The Printer Name is the name of the default printer, but if an other printer is required, its name can be entered. The number of copies can also be entered.
File Options	Is only highlighted if *Print to File Only* is selected. The name of the file to print to can be entered. Note that if the entered file name already exists, the old file will be overwritten!

Report Browser window

The Report Browser window is used to view the reports stored on the ITM-SC system.



Report Options

Use the *File* menu of the Report Browser to:

- Browse online or hardcopy a report.
- Rename a report.
- Copy a report to another device, such as computer disk.
- Delete a report.
- View the report names of all the users.

□

Printing a Report

Purpose To store or print all kinds of system data for evaluation.

Related information The related concept is:

- Report Concepts

Procedure Perform the following procedure for printing data by a selected printer.

1 Click on the `Print` button in the information window from which the data is to be printed.

2 Select the desired output device.

If the output device is a printer, enter the number of copies and, if needed the name of the printer.

If the output device is a file, enter the file name.

3 Click `OK`.

Result:

The report will be printed. Note that the only the first 2000 lines will be printed of reports which exceed this limit.

END OF STEPS

□

View a Report

Purpose Use this procedure to view the information that has been printed to files.

Related information The related concept is:

- Report Concepts

Procedure Follow these steps to browse a report:

1 Select *File* -> *Reports* -> *Browser*.

Result:

The Report Browser window appears.

2 Select the Report Name from the list of report names. When no reports are shown select View and All or User successively.

3 Execute the desired operation.

4 After operating on the file select *File* -> *Close* to complete the procedure.

END OF STEPS

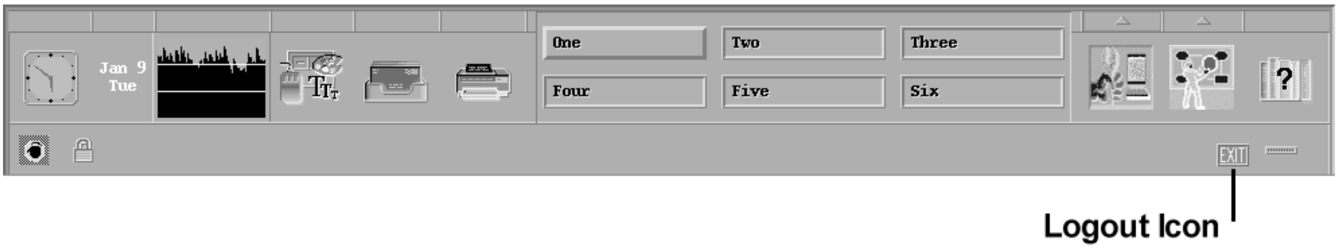
□

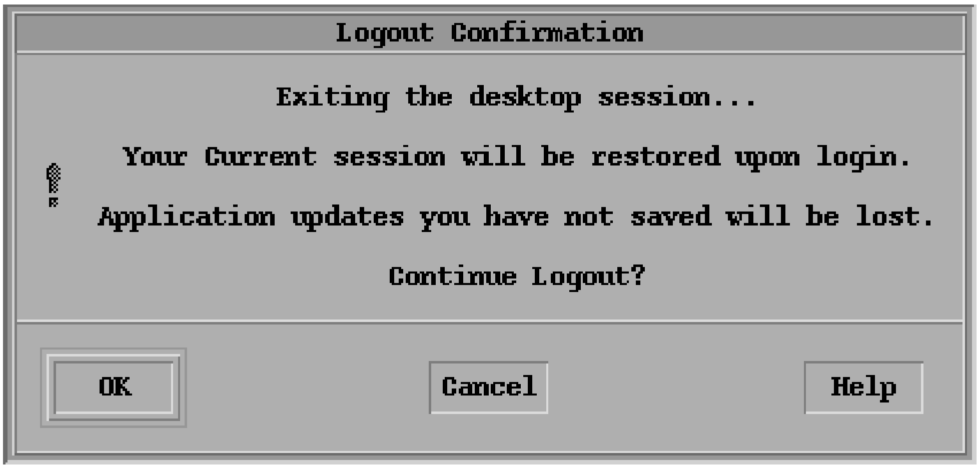
Logout of the ITM-SC

Background When the user has completed his work on the ITM-SC, he or she can log out of the Graphical User Interface. Then unauthorized users will not be able to access the ITM-SC.

Security In the style manager the administrator can enable logout confirmation, so an accidental logout can be prevented. Furthermore, an administrator is the only user that can make lasting changes in the style manager. Any changes to settings made by other users are lost at logout.

Windows to Use To log out of the system, the Logout icon and the Logout Confirmation window (optional) are used.




Logout Confirmation

Exiting the desktop session...

Your Current session will be restored upon login.

Application updates you have not saved will be lost.

Continue Logout?

□

Logout

Related information

The related concept is:

- Logout of the ITM-SC

Procedure

To logout perform the following procedure:

1 Click on the Logout icon.

Result:

If provisioned, the Logout confirmation window appears. A confirmation is then requested to make sure that the session has to be ended.

2 Click `OK`.

Result:

After confirming, the login window is displayed until the workstation time-out threshold is reached, then the screen saver appears and the log out procedure is completed.

END OF STEPS

□

Section: ITM-SC Network Map

Overview

Purpose This section will give an description of the features and use of the Network Map as well as provide some tasks to manage the Network Map.

□

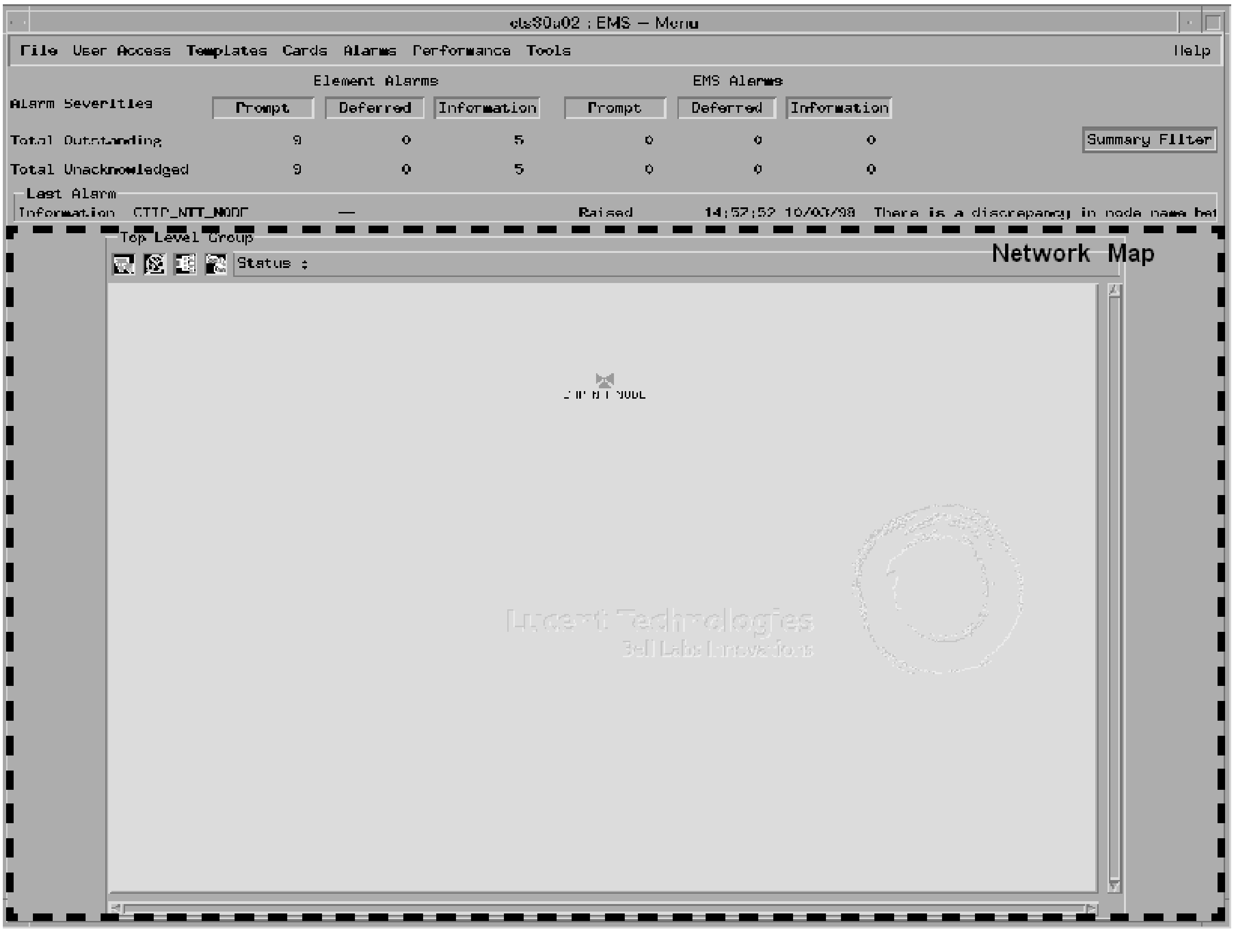
ITM-SC Network Map Concepts

Introduction

After activating Network Element Management from the Management Module, the Subnetwork Map window is displayed. This window is the main window for managing all network elements within the subnetwork and gives direct information about network elements, their status and Map groups.

Example of Network Map

An example of the Network Map is shown below.



	Element Alarms			EMS Alarms		
Alarm Severities	Prompt	Deferred	Information	Prompt	Deferred	Information
Total Outstanding	9	0	5	0	0	0
Total Unacknowledged	9	0	5	0	0	0

Last Alarm

Information CTIP_NTT_NODE — Raised 14:57:52 10/03/98 There is a discrepancy in node name bet

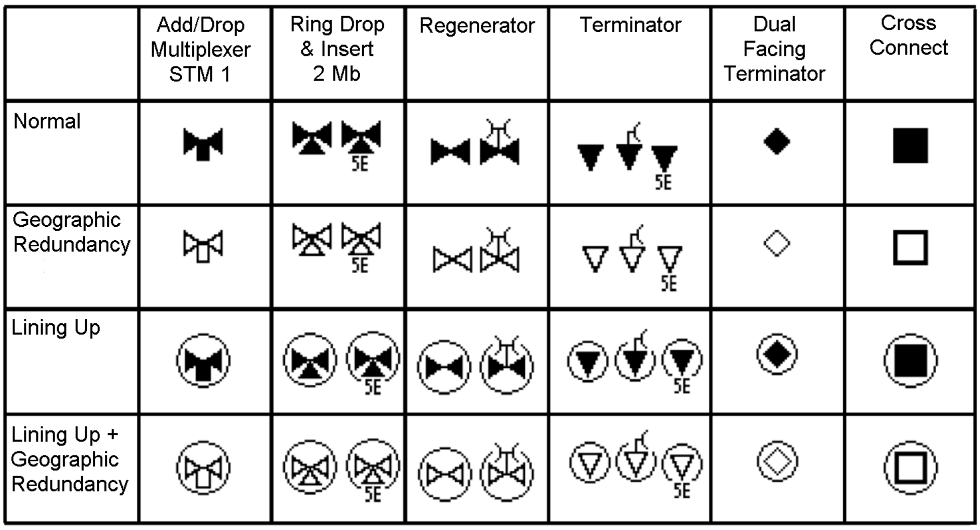
Network Map Icons

The Network Map icons are described in the table below:

Icon	Name	Description
	Up	To go up a group from the current group (unless at top-level already). Changes the display to show the group.

Icon	Name	Description
	Con-nections	This button will toggle the display of the RR connectivity lines. Note: only applicable for Radio Relay NEs.
	Display groups	Toggles the display between the contents of groups and the group icon. This also can be done by pressing control (CTRL) and selecting the Group or NE.
	Modify groups	Used to modify the grouping of network elements. This also can be done by selecting and NE or Group together with the right mouse button. Select from the pop up menu Modify Map Grouping of Nodes

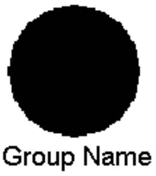
Network Element Icons The following icons represent the different types of network elements in different statuses.



	Add/Drop Multiplexer STM 1	Ring Drop & Insert 2 Mb	Regenerator	Terminator	Dual Facing Terminator	Cross Connect
Normal	⋈	⋈ ⋈ 5E	⋈ ⋈	▼ ▼ ▼ 5E	◆	■
Geographic Redundancy	⋈	⋈ ⋈ 5E	⋈ ⋈	▽ ▽ ▽ 5E	◇	□
Lining Up	⋈	⋈ ⋈ 5E	⋈ ⋈	▼ ▼ ▼ 5E	◆	■
Lining Up + Geographic Redundancy	⋈	⋈ ⋈ 5E	⋈ ⋈	▽ ▽ ▽ 5E	◇	□

Map Group A Map Group is a group of NEs which are put together because they are geographically or functionally related.

Group Icon The following icon represents a group of nodes:



NE Status

The color of each icon on the window represents the current status of the network element or connection. If two conditions exist for the same network element or connection, the network element icon or line is colored to indicate the condition with the highest severity. All alarms of the entire subnetwork are shown in one window; this is sometimes called the Alarm Map.

Colors of Alarms

The list below describes alarm colors and severity or status.

Color	Meaning
White	The NE or Connection is currently selected.
Grey	No current ‘associations’ exist with the NE or Connection. An association exist when there is communication between an ITM-SC and an NE.
Red	A ‘Prompt Alarm’ is currently on the NE or Connection.
Yellow	A ‘Deferred Alarm’ is currently on the NE or Connection.
Orange	An ‘Information Alarm’ is currently on the NE or Connection.
Green	No alarms currently on the NE or Connection.
Blue	The node has been pre-provisioned.

Additional Alarm Information

Additional information about an alarm can be given by the flashing square or “outlined” icon:

Action	**Description**
Flashing square	The alarm is not acknowledged yet. This is valid to each NE type but not for connections.
Outline	The network element is protected under Geographic Redundancy by this ITM-SC, but is not managed currently by this ITM-SC. This ITM-SC is not associated with this network element, so the outline is shown in grey. Valid for each NE type.
Short Beep	Indicates the arrival of a new alarm.

Specific Actions on the Network Map

Information about network elements or connections can easily be obtained using the Network Map. The alarms display can be filtered in such a way that only alarms of the selected network element or connection are shown.

To ..	Do this ..

Select an NE or group of NEs	Click once on the specific item.
Select multiple NEs	Press shift and draw using the cursor to make a rectangle over all NEs to select. This can also be done by pressing Ctrl and clicking with left mouse button on the desire NEs
Clear all selections	Click once on the Network Map outside any node or group.
Retrieve the alarm list of a NE or connection	Double click left-button on the specific NE or connection.
Drag selected nodes/groups	select nodes/groups and hold middle mouse button and drag to new position.

Pop-up Menus

The following pop-up menus can be accessed via selecting an item using the right mouse button.

Selecting item	provides shortcut to
NE	Alarm List Shelf Display
background	Change the Groupings

□

Customizing ITM-SC Network Map Concepts

Introduction

To prevent the Network Map from appearing cluttered when several network elements occupy a small space, those network elements can be grouped together into a map group which is represented by a single icon. For example network elements can be grouped in a geographical of functional way. It is possible that a map group contains another map group.

Customizing Features

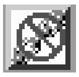
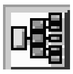
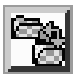
In order to customize the Network Map three procedures are provided:

- Creating of Map Groups.
- Modifying of Map Groups.
- Placing NEs in Map Groups.

These procedures can be found in this section under Managing Map Groups Procedures.

Icons for Customizing the Network Map

Four icons are provided to customize the Network Map. When network elements are mentioned, this is irrespective of network element type or whether the network element is associated or not. Non-associated network elements are called nodes. Within Map Groups nodes are treated in the same way as network elements.

Icon	Name	Description
	Up	To go up a group from the current group (unless at top-level already). Changes the display to show the group.
	Connections	This button will toggle the display of the RR connectivity lines. Note: only applicable for Radio Relay NEs.
	Display groups	Toggles the display between the contents of groups and the group icon. This also can be done by pressing control (CTRL) and selecting the Group or NE.
	Modify groups	Used to modify the grouping of network elements. This also can be done by selecting a NE or Group together with the right mouse button. Select from the pop up menu Modify Map Grouping of Nodes

Moving icons

To move a node or Map Group icon, select the node/group icon and drag the icon to the new position while holding the middle mouse button.

□

Parameters for Managing Map Groups

Old Group Name Displays the old name of a group. This field is grayed out when creating a map group.

New Group Name When creating a group: this is the name of the group to be created.

When modifying a group: this is the new group name.

Parent Group Name This is the name of the group's parent in the hierarchy.

When creating a group: specifies where in the hierarchy the group appears.

When modifying a group: provides a mechanism for moving the group to a different parent.

Background Image File This is the name of the background GIF filename used for the background image when the group is displayed. By default for a new group, it will be the Lucent logo file. The files available are the files in the directory: *../lib/map_data*. To display a new file, this file must be present in this directory.

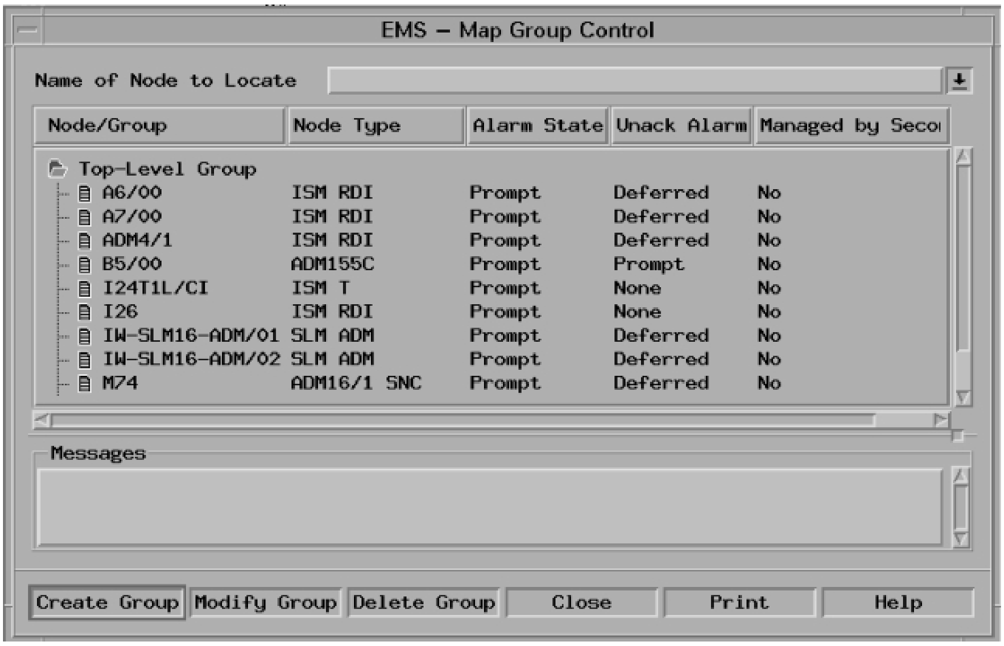
□

Windows for Managing Map Groups

Windows to use The windows to be used to managing the Map Groups and their contents are:

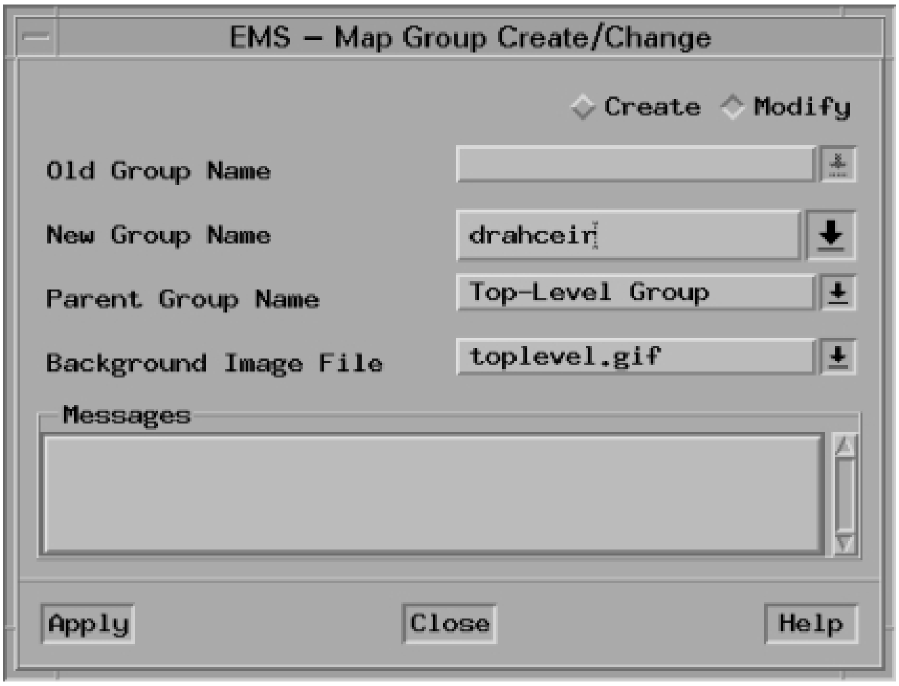
- *EMS - Map Group Control.*
- *EMS - Map Group Create/Change.*

EMS - Map Group Control



Node/Group	Node Type	Alarm State	Unack Alarm	Managed by Seco
Top-Level Group				
A6/00	ISM RDI	Prompt	Deferred	No
A7/00	ISM RDI	Prompt	Deferred	No
ADM4/1	ISM RDI	Prompt	Deferred	No
B5/00	ADM155C	Prompt	Prompt	No
I24T1L/CI	ISM T	Prompt	None	No
I26	ISM RDI	Prompt	None	No
IW-SLM16-ADM/01	SLM ADM	Prompt	Deferred	No
IW-SLM16-ADM/02	SLM ADM	Prompt	Deferred	No
M74	ADM16/1 SNC	Prompt	Deferred	No

EMS - Map Group Create/Change



Old Group Name

New Group Name: drahceir

Parent Group Name: Top-Level Group

Background Image File: toplevel.gif

□

Managing Map Groups Procedures

Purpose

Three procedures are provided to:

- create new map groups
- modify existing map groups
- Place/insert NEs into a map group

Before you begin

Before performing this procedure make sure:

- The background image file is present in the *..../lib/map_data* directory.

Before performing this procedure note the following:

- There is no correlation between Map Groups and Access Groups. Map groups only re-arrange the graphical presentation of NEs and Nodes on the Network Map. Access Groups are groups of NEs created for user security.

Related information

Related concepts are:

- ITM-SC Network Map Concepts
- Customizing ITM-SC Network Map Concepts

Create Map Groups

Follow these steps to create a network element group and apply a background image file:

1 Click with the `right mouse button` on Network Map (NOT on a node!) or click on the Modify groups icon.

Result:

When using the first option the Network Map Background pop-up menu appears.

When using the Modify groups icon the *EMS - Map Group Create/Change* window appears. Proceed with step 3!

2 Select `Change the Groupings`.

Result:

The *EMS - Map Group Control* window appears, showing a hierarchical view of the Network map's Map Groups.

3 Select `Create Group`.

Result:

The *EMS - Map Group Create/Change* window appears.

4 Fill in New Group Name.

5 Select the Parent Group Name when the created group has to be placed in a other Map Group.

6 Select the appropriate filename in Background Image File and click `Apply`.

Result:

A new Map Group is created and is displayed in the *EMS - Map Group Control* window. Double click on the Map Group to display the content of the Map Group with the selected background image file as background.

7 Click on the `Close` button.

Result:

The *EMS - Map Group Control* window appears. It is possible to continue to modify Map Groups.

8 Click the `Close` button in the *EMS - Map Group Control* window when the Map Groups modifications is completed.

Result:

The *EMS - Map Group Control* window disappears.

END OF STEPS

Modify Map Groups

Follow these steps to modify network element groups:

1 Click with the `right mouse button` on Network Map (NOT on a node!) or click on the Modify groups icon.

Result:

When using the first option the Network Map Background pop-up menu appears.

When using the Modify groups icon the *EMS - Map Group Create/Change* window appears. Proceed with step 3!

2 Select `Change the Groupings`.

Result:

The *EMS - Map Group Control* window appears. This window provides a hierarchical presentation of the Network map's Map Groups.

3 Select a Map Group.

4 Click the `Modify Group` button.

Result:

The *EMS - Map Group Create/Change* window appears.

5 Select the Map Group to modify, enter the modifications and click `Apply` to activate the changes.

6 Click `Close`.

Result:

The *EMS - Map Group Control* window appears.

7 Click `Close` in the *EMS - Map Group Control* window.

Result:

The changes made are activated and accessible and the Map Groups are updated with the changes to complete the procedure.

END OF STEPS

Place NEs in Map Groups

Follow these steps to rearrange network elements in network element groups:

1 Click with the `right mouse button` on Network Map (NOT on a node!) or click on the Modify groups icon.

Result:

When using the first option the Network Map Background pop-up menu appears.

When using the Modify groups icon the *EMS - Map Group Create/Change* window appears. Proceed with step 3!

2 Select `Change the Groupings`.

Result:

The *EMS - Map Group Control* window appears. This window provides a hierarchical view of the network map's Map Groups. All NEs, whether or not a member of a Map group, are shown.

3 To add an NE to a group, use the mouse to drag the node to the hierarchy display. Select an NE with the left mouse button, and drag it with the middle mouse button to the group. Release the button.

4 When an NE is difficult to find, select the NE number or name in the *Name of Node to Locate* field.

Result:

The requested node is highlighted.

5 Continue to move the nodes until they are arranged within the Map Groups as wanted.

6 Click `Close`.

Result:

Modifications are activated for the Map groups and the procedure is completed.

END OF STEPS

□

Lucent Technologies
Bell Labs Innovations

Glossary

# **5ESS**

Number 5 Electronic Switching System

5TAD

Five Tributary Add Drop subrack (WaveStar® ADM 16/1)

9TAD

Nine Tributary Add Drop subrack (WaveStar® ADM 16/1)

12 digit Numerical Code (12NC)

Used to uniquely identify an item or product. The first ten digits uniquely identify an item. The eleventh digit is used to specify the particular variant of an item. The twelfth digit is used for the revision issue. Items with the first eleven digits the same, are functionally equal and may be exchanged.

A **AAU**

Alarm Adapter Unit (RR)

AC

Alternating Current

ACU

Alarm Collection Unit (RR)

ADM

Add-Drop Multiplexer

Add-Drop Multiplexer 155 Mbit/s Compact Subrack (ADM-155C)

A network multiplexer that is designed to flexibly multiplex plesiochronous and STM-1 tributary port signals into STM-1 line port signals.

Administrative Unit (AU)

Carrier for TUs.

Administrative Unit Pointer (AU PTR)
Indicates the phase alignment of the VC-n with respect to the STM-N frame. The pointer position is fixed with respect to the STM-N frame.

Administrator
See ITM-SC System Administrator.

Agent
Performs operations on managed objects and issues events on behalf of these managed objects. All SDH managed objects will support at least an agent. Control of distant agents is possible via local ″Managers″.

Alarm
The notification (audible or visual) of a significant event. See also Event.

Alarm Adapter Unit (AAU)
Radio Relay circuit pack that is used for collection of external alarms and remote control of external equipment.

Alarm Collection Unit (ACU)
Radio Relay circuit pack that performs collection of equipment alarms, analogue measurement from internal monitoring points and calculating data.

Alarm Indication Signal (AIS)
Code transmitted downstream in a digital Network that shows that an upstream failure has been detected and alarmed if the upstream alarm has not been suppressed. Also referred to as All OneS.

ALS
Automatic Laser Shutdown

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

Aligning
Indicating the head of a virtual container by means of a pointer, i.e. creating an Administrative Unit (AU) or a Tributary Unit (TU).

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 8-bit code used for exchanging information among data processing systems and associated equipment.

Anomaly

A difference between the actual and desired operation of a function.

ANSI

American National Standards Institute

Assembly

Gathering together of payload data with overhead and pointer information (an indication of the direction of the signal).

APS

Automatic Protection Switching

AS

Alarm Suppression assembly

Association

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

Asynchronous

See Non-synchronous.

ATC

Auxiliary Transmission Channel

ATM

Asynchronous Transfer Mode

ATPC

Automatic Transmit Power Control

AU

Administrative Unit

AU4AD

Administrative Unit 4 Assembler/Disassembler

AUG

Administrative Unit Group

AUTO

Automatic

Automatic Transmit Power Control (ATPC)

Reduces the transmitter power output level during normal propagation conditions, and increase the power output to maximum level during fading periods trying to maintain nominal receiver input level.

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

B3ZS
Bipolar 3-Zero Substitution

B8ZS
Bipolar 8-Zero Substitution

BBTR
Backplane Bus TRansceiver

BC
Board Controller

BCC
Board Controller Complex

BIN
BINary

BIP
Bit Interleaved Parity

BISDN
Broadband Integrated Services Digital Network

Bit Error Ratio (BER)
The ratio of bits received in error to bits sent.

Bit Interleaved Parity (BIP)
A method of error monitoring using a specified number of bits (BIP-8)

BLD OUT LG
Build-Out Lightguide

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

Branching
Interconnection of independent line systems.

Broadband Communication
Voice, data, and/or video communication at greater than 2 Mbit/s rates.

Broadband Service Transport
STM-1 concatenation transport over the SLM for ATM applications.

BUSTR
BUS Transmitter and Receiver

C

CAS
Channel Associated Signalling

CAT
CATastrophic

CC
Cross-Connection Cross-Connect (WaveStar® ADM 16/1)

CCIR
See ITU-R.

CCITT
See ITU-T.

CCS
Common Channel Signaling

CEPT
Conférence Européenne des Administrations des Postes et des Télécommunications

Channel
A sub-unit of transmission capacity within a defined higher level of transmission capacity, e.g. a CEPT-4 (140 Mbit/s) within a 565 Mbit fiber system.

Circuit
A combination of two transmission channels permitting bi-directional transmission of signals between two points, to support a single communication.

CIT
Craft Interface Terminal

Clear Channel (Cl. Ch.)
A provisionable mode for the 34 and 140 Mbit/s tributary outputs that causes parity violations to not be monitored or corrected before the 34 and 140 Mbit/s are encoded.

Client
Computer in a computer network that generally offers a user interface to a server. See also Server.

CMI
Coded Mark Inversion

CO
Central Office

Concatenation
A procedure whereby a multiplicity of Virtual Containers is associated one with another with the result that their combined capacity can be used as a single container across which bit sequence integrity is maintained.

Configuration Management (CM)
Subsystem of the ITM-SC that, among other things, configures the network and processes messages from the network.

CONN PCB
Connector Printed Circuit Board

Container (C)
Carries plesiochronous signal, the ″payload″.

Co-resident
A hardware configuration where the ITM-SC and ITM-NM applications can be active at the same time independently on the same hardware and software platform without interfering each others functioning.

Common Object Request Broker Architecture (CORBA)
CORBA allows applications to communicate with one another no matter where they are located or who has designed them.

CP
Circuit Pack

Craft Interface Terminal (CIT)
Local manager for SDH Network Elements.

CRC
Cyclic Redundancy Check

Cross-Connect Map
Connection map for an SDH Network Element; contains information about how signals are connected between high speed timeslots and low speed tributaries. See also Squelch Map.

Cross Polarization Interference Cancellation
This feature permits both orthogonal polarizations of one Radio Frequency carrier to be used simultaneously, thus achieving greater spectral efficiency.

CV
Code Violation

D

DACS
Digital Access & Cross-connect System

DACScan-T
See Integrated Transport Management Network Manager.

Database Administrator
A user who administers the database of the ITM-SC application. See also User Privilege.

Data Communication Channel (DCC)
The embedded overhead communication channel in the SDH line. This is used for end-to-end communication and maintenance. It carries alarm, control, and status information between Network Elements in an SDH network.

Data Communication Equipment (DCE)
Provides the signal conversion and coding between the data terminating equipment and the line. The DCE may be separate equipment or a part of the data terminating equipment.

Data Terminating Equipment (DTE)
Originates data for transmission and accepts transmitted data.

DC
Direct Current

DCF
Data Communications Function

DCN
Data Communications Network

DCS
Digital Cross-connect System

DDF
Digital Distribution Frame

Dedicated Protection Ring (DP-Ring)
A protection method used in ISM Network Elements.

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.

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

Digital Link
A transmission span such as a point-to-point 2 Mbit/s, 34 Mbit/s, 140 Mbit/s, VC12, VC3 or VC4 link between controlled Network Elements. The channels within a digital link are insignificant.

Digital Section
A transmission span such as an STM-N or 565 Mbit/s signal. A digital section may contain multiple digital channels.

DIL
Dual In Line

Directory Service Network Element (DSNE)
A designated Network Element that is responsible for administering a database that maps Network Elements names (node names) to addresses (node Id). There can be one DSNE per (sub)network.

Disassembly
Splitting up a signal into its constituents as payload data and overhead (an indication of the direction of a signal).

Domain
The domain of an ITM-SC is the set of all SDH Network Elements that are controlled by that particular ITM-SC.

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

DPLL
Digital Phase Locked Loop

DPS
Data communication Packet Switch (ISM)

DR
Digital Radio

DRI
Dual Ring Interworking

DS-n
Digital Signal, Level n

DTMF
Dual Tone Multi-Frequency

DUS
Do not Use for Synchronization

DWDM
Dense Wavelength Division Multiplexing

E

EC-n
Electrical Carrier, Level n

ECC
Embedded Control Channel

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

Element Management System (EMS)
See Integrated Transport Management Subnetwork Controller.

EMC
ElectroMagnetic Compatibility

EMI
ElectroMagnetic Interference

EOW
See Orderwire.

Equivalent Bit Error Ratio (EBER)
The calculated average bit error rate over a data stream.

Errored Second (ES)
A performance monitoring parameter.

ES
End System

ESD
ElectroStatic Discharge

ESPG
Elastic Store & Pointer Generator

ETSI
European Telecommunication Standardisation Institute

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 ITM-SC.

Event Management (EM)
Subsystem of ITM-SC that processes and logs event reports of the network.

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 the approximate agreement with the synchronization reference frequency.

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

F

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.

FAS
Frame Alignment Signal

FAW
Frame Alignment Word

FC
Full contact Connector

FCC
Federal Communications Commission

FDDI
Fiber Distributed Data Interface

FEP
Front End Processor

Free Running
An operating condition of a Network Element in which its local oscillator is not locked to any synchronization reference and is using no storage techniques to sustain its accuracy.

G

Geographic Location
Location of the ITM-SC server. This is entered as part of the installation procedure of an ITM-SC.

Gateway Network Element (GNE)
Passes information between other Network Elements and management systems via a Data Communications Network.

Geographic Redundancy (GR)
Allows protection of management for a Network Element by assigning it to two ITM-SCs. The first primary ITM-SC, usually manages the Network Element and is now in the protected domain. If the primary ITM-SC or the link between the Network Element and the primary fails, the secondary ITM-SC will automatically take over management of the Network Element and is now in the protecting domain. The two ITM-SCs are connected by a peer to peer link, which they use to pass Geographic Redundancy management information over. This link must be established before any Network Element can be protected by Geographic Redundancy.

Global Wait to Restore Time
Corresponds to the time to wait before switching back to the timing reference occurs after a timing link failure has cleared. This time applies for all timing sources in a system hence the name global. This can be between 0 and 60 minutes, in increments of one minute.

GUI
Graphical User Interface

H

HE
Host Exchange

High Density Bipolar 3 code (HDB3)
Line code for e.g. 2 Mbit/s transmission systems.

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

Higher order Path Adaptation (HPA)
Function that adapts a lower order Virtual Container to a higher order Virtual Container by processing the Tributary Unit pointer which indicates the phase of the lower order Virtual Container Path Overhead relative to the higher order Virtual Container Path Overhead and assembling/disassembling the complete higher order Virtual Container.

Higher order Path Connection (HPC)
Function that provides for flexible assignment of higher order Virtual Containers within an STM-N signal.

Higher order Path Termination (HPT)
Function that terminates a higher order path by generating and adding the appropriate Virtual Container Path Overhead to the relevant container at the path source and removing the Virtual Container Path Overhead and reading it at the path sink.

HMI
Human Machine Interface

HO
High Order

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 synchronized reference.

Host Name
Name of the server on which the ITM-SC is running.

HP-UX
Unix Operating System for Hewlett Packard platform.

HS
High Speed

I

ICB
Interconnection Box

ICP
InterConnection Panel

IEC
International Electrotechnical Committee

IEEE
Institute of Electrical and Electronic Engineers

IF
Intermediate Frequency

IFT
InterFace Terminal

Intelligent Synchronous Multiplexer (ISM)
A network multiplexer that is designed to flexibly multiplex plesiochronous and STM-1 tributary port signals into STM-1 or STM-4 line port signals.

Intergrated Transport Management Craft Interface Terminal (ITM-CIT)
Local manager for SDH Network Elements in a subnetwork. Also referred to as Craft Interface Terminal.

Intermediate System (IS)
A system which routes/relays management information. An SDH Network Element may be a combined Intermediate and end system.

IPS

Inter Processor Status

IS

In-Service

ISDN

Integrated Services Digital Network

IS-IS Routing

The Network Elements in a management network, route packets (data) between each other using a IS-IS level protocol. The size of a network running IS-IS Level 1 is limited, and therefore certain mechanisms are employed to facilitate the management of larger networks. For STATIC ROUTING, the capability exists for disabling the protocol over the LAN connections, effectively causing the management network to be partitioned into separate IS-IS Level 1 areas. In order for the ITM-SC to communicate with a specific Network Element in one of these areas, the ITM-SC must identify through which socalled Gateway Network Element this specific Network Element is connected to the LAN. All packets to this specific Network Element are routed directly to the Gateway Network Element by ITM-SC, before being re-routed (if necessary) within the Level 1 area. For DYNAMIC ROUTING an IS-IS Level 2 routing protocol is used allowing a number of Level 1 areas to interwork. The Network Elements which connect an IS-IS area to another area are set to run the IS-IS Level 2 protocol within the Network Element and on the connection between other Network Elements. Packets can now be routed between IS-IS areas and the ITM-SC does not have to identify the Gateway Network Elements.

ISO

International Standards Organisation

ITM-SC Administrator

See ITM-SC System Administrator.

ITM-SC System Administrator

A user of the ITM-SC application with System Administrator privileges. See also User Privilege.

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.

J **Jitter**

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

L **LAN**

Local Area Network

LBA

Lightwave Booster Amplifier.

LCN

Local Communications Network

LDI

Linear Drop/Insert (Add-Drop)

LED

Light Emitting Diode

LEN

Local Exchange Node

LF

Low Frequency

LH

Long Haul

License key

An encrypted code that is required to enable the use of specific modules in the ITM-SC. Valid license keys can be obtained from your provider.

Line

Transmission line; refers to a transmission medium, together with the associated high speed equipment, required to provide the means of transporting information between two consecutive Network Elements, one of which originates the line signal and the other terminates the line signal.

Line Build Out (LBO)

An optical attenuator that guarantees the proper signal level and shape at the receiver input.

Line Overhead Controller (LOC)

SLM circuit pack that accesses the overhead bytes from the high speed line.

LNC

LiNe Controller (SLM)

LO
Low Order

LOF
Loss Of Frame

LOM
Loss Of Multiframe

LOP
Loss Of Pointer

LOS
Loss Of Signal

Lower order Path Adaptation (LPA)
Function that adapts a PDH signal to a synchronous network by mapping the signal into or de-mapping the signal out of a synchronous container.

Lower order Path Connection (LPC)
Function that provides for flexible assignment of lower order VCs in a higher order VC.

Lower order Path Termination (LPT)
Function that terminates a lower order path by generating and adding the appropriate VC POH to the relevant container at the path source and removing the VC POH and reading it at the path sink.

LPU
Line Port Unit (ISM)

LPU155
Line Port Unit 155 Mbit/s (WaveStar® ADM 4/1)

LRX
Line Receiver (SLM)

LS
Low Speed

LTA
Line Terminal Application (SLM)

LTX
Line Transmitter (SLM)

LTX/EML
Line Transmitter with Electro-absorption Modulated Laser (SLM)

M **MAF**

Management Application Function

Management Connection

Identifies the type of routing used (STATIC or DYNAMIC), and if STATIC is selected allows the Gateway Network Element to be identified. See also IS-IS Routing.

Management Information Base (MIB)

The database in the Network Element and contains the configuration data of the Network Element. A copy of each MIB is available in the ITM-SC and is called the MIB image. Under normal circumstances the MIB and MIB image of one Network Eelement are synchronized.

Manager

Capable of issuing network management operations and receiving events. The manager communicates with the Agent in the controlled Network Element.

Manufacturer Executable Code (MEC)

Network Element system software in binary format that after being downloaded to one of the stores can be executed by the system controller of the Network Element.

Mapping

Gathering together of payload data with overhead, i.e. packing the PDH signal into a Virtual Container.

MDI

Miscellaneous Discrete Input

MDO

Miscellaneous Discrete Output

Mediation Device (MD)

Allows for exchange of management information between Operations System and Network Elements.

MEF

Maintenance Entity Function (in NE)

MEM

System MEMory unit (for SLM ADM NEs)

Message Communications Function (MCF)

Function that provides facilities for the transport and routing of Telecommunications Management Network messages to and from the Network Manager.

MF

Mediation Function

MFS
Multi Frame Synchronization signal

MIB image
See Management Information Base.

Midspan Meet
The capability to interface between two lightwave Network Elements of different vendors. This applies to high speed optical interfaces.

MMI
Man-Machine Interface Also referred to as Human Machine Interface (HMI)

MO
Managed Object

Motif
X-Windows System supplied by Open Software Foundation.

MS
Multiplexer Section

MTBF
Mean Time Between Failures

MTBMA
Mean Time Between Maintenance Activities

MTIE
Maximum Time Interval Error

MTPI
Multiplexer Timing Physical Interface

MTTR
Mean Time To Repair

Multiplexer Section OverHead (MSOH)
Part of the Section Overhead. Is accessible only at line terminals and multiplexers.

Multiplexer Section Protection (MSP)
Provides capability for switching a signal from a working to a protection section.

Multiplexer Section Shared Protection Ring (MS-SPRING)
A protection method used in SLM Add-Drop Multiplexer Network Elements.

Multiplexer Section Termination (MST)
Function that generates the Multiplexer Section OverHead in the transmit direction and terminates the Multiplexer Section OverHead in the receive direction.

Multiplexer Timing Source (MTS)
Function that provides timing reference to the relevant component parts of the multiplex equipment and represents the SDH Network Element clock.

Multiplexing
A procedure by which multiple lower order path layer signals are adapted into a higher order path, or the multiple higher order path layer signals are adapted into a multiplex section.

N **NEF**
Network Element Function

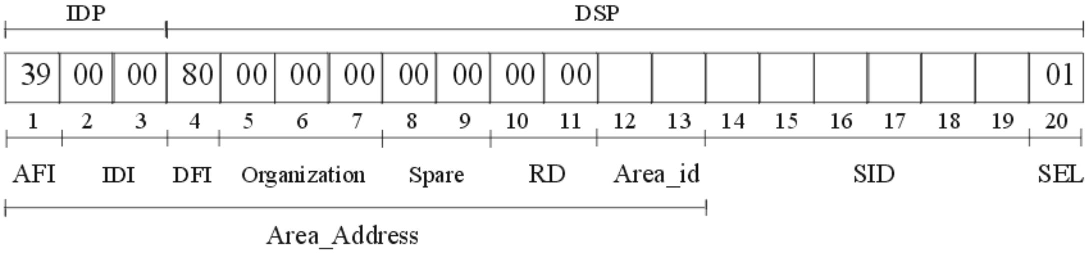
NEM
Network Element Manager

Network Element (NE)
A Network Element is comprised of telecommunication equipment (or groups/parts of telecommunication equipment) and support equipment that performs network element functions and has one or more standard Q-type interfaces. A Network Element is direct manageable by a management system. See also Node.

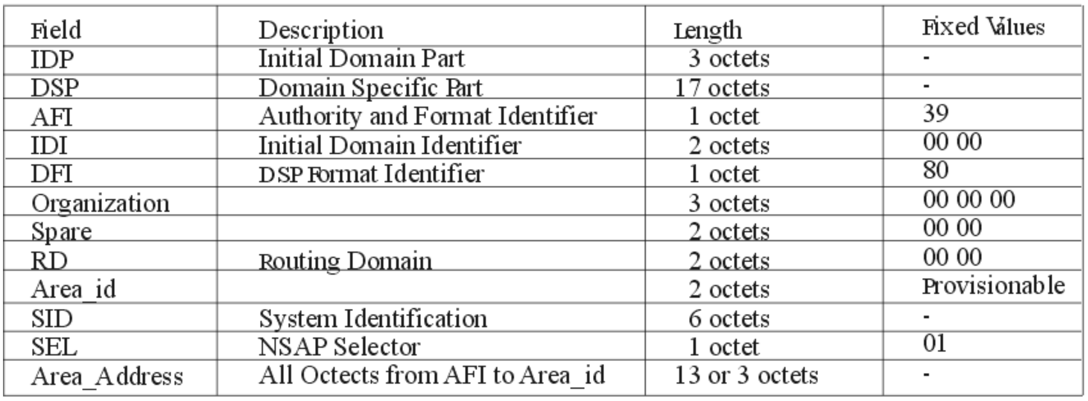
Network Element Equivalent (NEE)
The functionality, database size and processing power required from the ITM-SC is different for each Network Element type supported. Therefore each type represents an amount of Network Element Equivalent.

Network Mediation Unit (NMU)
Used to collect fault and alarm events from transmission equipment. The ITM-SC can forward alarms to the NMU. The NMU can forward alarms to an Operations System.

Network Service Access Point (NSAP)
An end system address of the System Controller according to ISO 8348 AD2. The format used is ISO_DCC_LUCENT, which has the following structure:



Where



Field	Description	Length	Fixed Values
IDP	Initial Domain Part	3 octets	-
DSP	Domain Specific Part	17 octets	-
AFI	Authority and Format Identifier	1 octet	39
IDI	Initial Domain Identifier	2 octets	00 00
DFI	DSP Format Identifier	1 octet	80
Organization		3 octets	00 00 00
Spare		2 octets	00 00
RD	Routing Domain	2 octets	00 00
Area_id		2 octets	Provisionable
SID	System Identification	6 octets	-
SEL	NSAP Selector	1 octet	01
Area_Address	All Octects from AFI to Area_id	13 or 3 octets	-

NMC

Network Maintenance Center

NMS

Network Management System

NNE

Non-SDH Network Element

NNI

Network Node Interface

Node

Defined as all equipment that is controlled by one system controller. A node is not always direct manageable by a management system. See also Network Element.

NOMC

Network Operation Maintenance Channel

Non-revertive switching

In non-revertive switching there is an active and standby high speed line, circuit pack, etc. When a protection switch occurs, the standby line, circuit pack, etc., is selected causing the old standby line, circuit pack, etc., to be used for the new active line, circuit pack, etc. The original active line, circuit pack, etc., becomes the standby line, circuit pack, etc. This status remains in effect when the faults clears. Therefore, this protection scheme is non-revertive in that there is no switch back to the original status in effect before the fault occurred.

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

Not Protected Domain
The not protected domain for the ITM-SC contains all the Network Elements which are managed by one ITM-SC and are not currently protected by another ITM-SC. If the ITM-SC fails, the Network Elements in this domain are not managed by any ITM-SC. See also Geographic Redundancy.

NPI
Null Pointer Indication

NRZ
Non-Return to Zero

NSA
Non-Service Affecting

NVM
Non-Volatile Memory

O **OA**
Optical Amplifier (OLS)

OAA case tools
A software package/tool to aid the process of requirements, analysis, design and implementation of object orientated systems.

OAM&P
Operations, Administration, Maintenance and Provisioning

OC-n
Optical Carrier, Level n

ODF
Optical Distribution Frame

ODU
Optical Demultiplexer Unit (OLS)

OFS
Out of Frame Second

OI
Optical Interface (WaveStar® ADM 16/1)

OMU
Optical Multiplexer Unit (OLS)

Operations System (OS)
Operations System is the system which provides operations, administration and maintenance functions.

Operator
A user of the ITM-SC application with Operator privileges. See also User Privilege.

Optical Line System (OLS)
A high-capacity lightwave system that is designed to multiplex eight optical signals with different wavelengths into one combined signal through an optical fiber. There is a difference of 1.5 micrometer in wavelength between two multiplexed signals.

OOF
Out Of Frame

OOS
Out Of Service

OSB
Optical Splice Box

OSF
Open Software Foundation Operations System Function

OSF/Motif
The WaveStar® ITM-SC application has an X-windows graphical representation and the components used in the “Graphical User Interface” are OSF/Motif compliant, these components comprise of items such as: scrollbars, menus, radio buttons, etc.

OSI
Open Systems Interconnection

OW
(Engineering) Order Wire

P

PABX
Private Automatic Branch eXchange

Paddle Board - Peripheral Control and Timing link (PB-PCT)
Is a small circuit board used in a 5ESS exchange for protection switching and optical to electrical conversion of the PCT-link.

Path
A logical connection between a termination point at which a standard format for a signal at the given rate is assembled, and transmitted and another termination point at which the received

standard frame format for the signal is disassembled.

Path Overhead (POH)
Virtual Container Path Overhead provides for integrity of communication between the point of assembly of a Virtual Container and its point of disassembly.

PC
Personal Computer

PCB
Printed Circuit Board

PCM
Pulse Code Modulation

PCT-link
Peripheral Control and Timing-link

PDH
Plesiochronous Digital Hierarchy

Peer ITM-SC
ITM-SC at the other end of the Peer to Peer link.

Peer to Peer link
Connection between two ITM-SCs with Geographic Redundancy. The link is used to co-ordinate the management of a Network Element. See also Geographic Redundancy.

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

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

PI
Physical Interface Plesiochronous Interface (WaveStar® ADM 16/1)

Platform
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.

PMA
Performance Monitoring Application

Pointer
An indicator whose value defines the frame offset of a virtual container with respect to the frame reference of the transport entity on which it is supported.

POTS
Plain Old Telephone Service

PP
Pointer Processing

PPC
Pointer Processor and Cross-connect (ISM)

Primary ITM-SC
ITM-SC that is usually managing a Network Element. If the primary ITM-SC fails, management of the Network Element is passed over to the secondary ITM-SC. A Network Element should be provisioned normally on the primary ITM-SC and then be configured for use on the secondary. See also Geographic Redundancy.

Primary Reference Clock (PRC)
The main timing clock reference in SDH equipment.

Protected Domain
The protected domain for an ITM-SC contains all the Network Elements this manager is the primary ITM-SC for and are protected by another secondary ITM-SC. See also Geographic Redundancy.

Protecting Domain
The protecting domain for an ITM-SC contains all the Network Elements this manager is the secondary ITM-SC for. See also Geographic Redundancy.

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.

PSA
Partially Service Affecting

PSDN
Public Switched Data Network

PSF
Power Supply Filter

PSF-SIP
Power Supply Filter; originally designed for Italian customer.

PSN
Packet-Switched Network

PSTN
Public Switched Telephone Network

PT
Protected Terminal Power supply filter and Timing circuit pack (WaveStar® ADM 16/1)

Q **QAF**
Q Adapter Function (in NE)

Q-LAN
Thin Ethernet LAN which connects the manager to Gateway Network Elements so that management information between Network Elements and management systems can be exchanged.

QOS
Quality Of Service

Quality Level (QL)
The quality of the timing signal(s) provided to clock a Network Element. The level is provided by the Synchronization Status Marker which can accompany the timing signal. If the System and Output Timing Quality Level mode is “Enabled”, and if the signal selected for the Station Clock Output has a quality level below the Acceptance Quality Level, the Network Element “squelches” the Station Clock Output Signal, which means that no signal is forwarded at all. Possible levels are: - PRC (Primary Reference Clock) - SSU_T (Synchronization Supply Unit - Transit) - SSU_L (Synchronization Supply Unit - Local) - SEC (SDH Equipment Clock) - DUS (Do not Use for Synchronization)

R **RA**
Regenerator Application (SLM)

Radio Protection Switching system (RPS)
Its main function is to handle the automatic and manual switching from a main channel to a common protection channel in an N+1 system.

Radio Relay (RR)
A point-to-point Digital Radio system to transport STM-1 signals via microwaves.

RCU
Rigid Connect Unit (SLM)

RCVR Data Distribution Unit (RCVR)
Radio Relay circuit pack that performs distribution of the protection channel and the low priority traffic in the receiver side.

RDDU
RCVR Data Distribution Unit (RR)

RDI
Remote Defect Indicator. Previously known as Far End Receive Failure (FERF).

RDI
Ring Drop/Insert (Add-Drop)

RDSV
Running Digital Sum Violations

Receive-direction
The direction towards the cross-connect.

REGEN
Regenerator (SLM)

Regenerator Loop
Loop in a Network Element between the Station Clock Output(s) and one or both Station Clock Inputs, which can be used to dejitterize the selected timing reference in network applications.

Regenerator Overhead Controller (ROC)
SLM circuit pack that provides user access to the SDH overhead channels at repeater sites.

Regenerator Section Termination (RST)
Function that generates the Regenerator Section Overhead (RSOH) in the transmit direction and terminates the RSOH in the receive direction.

REI
Remote Error Indication. Previously known as Far End Block Error (FEBE).

Relay Unit (RU)
Radio Relay circuit pack whose main function is to perform protection switching when the Alignment Switch in the demodulator unit is unable to perform protection switching.

Restore Timer
Counts down the time (in minutes) during which the switch waits to let the worker line recover before switching back to it. This option can be set to prevent the protection switch continually switching if a line has a continual transient fault. This field is greyed out if the mode is non-revertive.

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 back to the original working line.

RF
Radio Frequency

RFI
Remote Failure Indicator

RGU
ReGenerator Unit (SLM)

Route
A series of contiguous digital sections.

RPS
Ring Protection Switching

RSM
Remote Switching Module

RSOH
Regenerator Section OverHead; part of SOH.

RZ
Return to Zero

S **SA**
Service Affecting Synchronous Adapter (WaveStar® ADM 16/1)

SAI
Station Alarm Interface

SC
Square coupled Connector

SD
Signal Degrade

SDH-TE
SDH - Terminal Equipment

Specification and Design Language (SDL)
This is a standard formal language for specifying (essentially) finite state machines.

SEC
SDH Equipment Clock

Secondary ITM-SC
Backup ITM-SC for a Network Element should the primary ITM-SC fail. A Network Element should be provisioned normally on the primary ITM-SC and then be configured for use on the secondary. See also Geographic Redundancy.

Section
A transport entity in the transmission media layer network which provides integrity of information transfer across a section layer network connection by means of a termination function at the section layer.

Section Adaptation (SA)

Function that processes the AU-pointer to indicate the phase of the VC-3/4 POH relative to the STM-N SOH and assembles/disassembles the complete STM-N frame.

Section Overhead (SOH)

Capacity added to either an AU-4 or assembly of AU-3s to create an STM-1. Contains always STM-1 framing and optionally maintenance and operational functions. SOH can be subdivided in MSOH (multiplex section overhead) and RSOH (regenerator section overhead).

SEF

Support Entity Function (in NE)

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 require generally sufficient performance. See also Client.

Severely Errored Frame Seconds (SEFS)

A performance monitoring parameter.

Severely Errored Second (SES)

A second with a binary error ratio and used as a performance monitoring parameter.

Severity

See Alarm Severity

Service

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

SH

Short Haul

SI

Synchronous Interface (WaveStar® ADM 16/1)

SIB

Subrack Interface Box

SLC

Subscriber Loop Carrier

SLM

Signal Label Mismatch

Smart Communication Channel (SCC)
A HDLC messaging channel between the SDH-TE and the 5ESS host node. Similar to the DCC messaging channels located in the STM-N section overhead.

SML
Service Management Level

SMN
SDH Management Network

SMS
SDH Management Subnetwork

SNC/I
SubNetwork Connection (protection) / Inherent monitoring

SNC/NI
SubNetwork Connection / Non Intrusive monitoring

SNR
Signal to Noise Ratio

Soft Windows
PC emulator package for HP platforms.

SONET
Synchronous Optical Network

Space Diversity (SD)
Reception of the Radio signal via mirror effects on earth.

SPB2M
Subrack Protection for 2 Mbit/s Board (WaveStar® ADM 4/1)

SPI
SDH Physical Interface Synchronous-Plesiochronous Interface (WaveStar® ADM 16/1)

Squelch Map
Traffic map for SLM Add-Drop Multiplexer Network Elements that contains information for each cross-connection in the ring and indicates the source and destination Network Elements for the low speed circuit that the cross-connection is part of. This information is used to prevent traffic misconnection in rings with isolated Network Elements or segments. See also Cross Connection Map.

SSM
Synchronization Status Marker

Standby
The operational mode of a physical entity that indicates that the entity is not providing service, but standby. This designation will change with each switch action.

Station Clock Input (SCI)
An external clock may be connected to a Station Clock Input.

Station Clock Output (SCO)
A clock signal that can be used for other systems.

Streched Ring (STRING)
An open ring in which each node is an Add-Drop Multiplexer. The end nodes operate with one high speed line equipped.

STS
Synchronous Transport Signal; used in SONET.

Subnetwork
A group of interconnected/interrelated Network Elements. The most common connotation is an SDH network in which the Network Elements have data communications channels (DCC) connectivity.

Supervisor
A user of the ITM-SC application with Supervisor privileges. See also User Privilege.

Supervisory Unit (SU)
Radio Relay circuit pack that gives comprehensive supervision and control facilities to the user by collecting information from the Alarm Collection Units and Alarm Adapter Units.

SUPV
Supervision unit (WaveStar® ADM 4/1)

SUPV_SVC
Supervision with Service Channel unit (WaveStar® ADM 4/1)

SVCE
Service

Switch Receive Unit (SWR)
SLM circuit pack that provides the cross-connect in the receive direction between high speed line timeslots and low speed tributaries.

Switch Transmit Unit (SWT)
SLM circuit pack that provides the cross-connect in the transmit direction between high speed line timeslots and low speed tributaries.

Switching Module (SM)
An access module from the 5ESS switch.

Synchronization Supply Unit (SSU)

A circuit pack that recovers and reshapes the clock signal in order to filter out jitter. The Local (SSU_L) and Transit (SSU_T) types are available.

Synchronous

The essential characteristic of time-scales or signals such that their corresponding significant instants occur at precisely the same average rate.

Synchronous Digital Hierarchy (SDH)

A hierarchical set of digital transport structures, standardized for the transport of suitable adapted payloads over transmission networks.

Synchronous Equipment Management Function (SEMF)

Function that converts performance data and implementation specific hardware alarms into object-oriented messages for transmission over the DCC and/or Q-interface. It also converts object-oriented messages related to other management functions for passing across the S reference points.

Synchronous Line Multiplexer (SLM)

A line multiplexer that is designed to multiplex VC-4 and STM-1 tributary port signals into STM-16 line port signals.

Synchronous Network

The synchronization of synchronous transmission systems with synchronous payloads to a master Network clock that can be traced to a single reference clock.

Synchronous Transport Module (STM)

The information structure used to support (section layer) connections in SDH.

System Administrator

A user of the computer system on which the ITM-SC application can be installed. See also User Privilege.

System Controller (CTL)

ISM circuit pack that controls the configuration of an Intelligent Synchronous Multiplexer system.

System Controller (SC)

WaveStar® ADM 16/1 circuit pack that controls and provisions all units. It also contains the data communication packet switch functionallity which is necessary for routing of management information between Network Elements and their management system.

System Controller (SCT)

SLM Line Terminal and Regenerator Network Element circuit pack that provides the highest level of system control for the Synchronous Line Multiplexer system. The SCT circuit pack provides overall administrative control of the system. Its memory is included in the same one circuit pack.

System Controller (STC)
SLM Add-Drop Multiplexer Network Element circuit pack that provides the highest level of system control for the Synchronous Line Multiplexer system. The STC circuit pack provides overall administrative control of the system. Its memory is provided by the MEM circuit pack.

System Controller (SYSCTL)
OLS circuit pack that provides the highest level of system control for the Optical Line System. The SYSCTL circuit pack provides overall administrative control of the system. Its memory is provided by the SYSMEM circuit pack.

System Memory Unit (MEM)
SLM Add-Drop Multiplexer Network Element circuit pack that provides the highest level of system control for the Synchronous Line Multiplexer system. The MEM circuit pack provides memory support for the System Controller (STC) circuit pack.

System Memory Unit (SYSMEM)
OLS circuit pack that provides the highest level of system control for the Optical Line System. The SYSMEM circuit pack provides memory support for the SYSCTL circuit pack.

T

TCA
Threshold Crossing Alarm

TCP/IP
Transmission Control Protocol/Internet Protocol

TDEV
Timing DEViation

TDM
Timing Division Multiplexing

Template
A collection of parameters that define a specific Network Element configuration. A Template gives the user the opportunity to configure parameters in a Network Element with a single operation. They are re-usable, and allow the user to configure the parameters in many Networks Elements in the same way. A set of Default templates is provided, and the user can create new templates and edit or delete user-created ones. Note that a template is always associated with one specific Network Element type and can not be used for other Network Element types.

TERM
Terminal Multiplexer

TGU
Timing Generator Unit

TI
Timing Interface (WaveStar® ADM 16/1)

TLM
TeLeMetry Unit (OLS)

TLP
Terminal with Line Protection

TMN
Telecommunications Management Network

TPU
Tributary Port Unit

TPU-PCT
Tributary Port Unit - Peripheral Control and Timing link

TPU2
Tributary port Unit 2 Mbit/s (WaveStar® ADM 4/1)

TPU34/45
Tributary port Unit 34 / 45 Mbit/s (WaveStar® ADM 4/1)

TPU155
Tributary port Unit 155 Mbit/s (WaveStar® ADM 4/1)

Transmit-direction
The direction outwards from the cross-connect.

Trellis Code Modulation
A combined coding and modulation scheme for improving the reliability of a digital transmission system without increasing the transmitted power or the required bandwidth.

TRF
TRansFer unit (WaveStar® ADM 4/1)

Tributary
A signal of a specific rate (2 Mbit/s, 34 Mbit/s, 140 Mbit/s, VC12, VC3, VC4, STM-1 or STM-4) that may be added to or dropped from a line signal.

Tributary Overhead Controller (TOC)
SLM circuit pack that allows access to the overhead bytes of the incoming tributary signal.

Tributary Overhead Controller (TOHCTL)
OLS circuit pack that allows access to the overhead bytes of the Supervisory channel.

Tributary Unit (TU)
An information structure which provides adaptation between the lower order path layer and the higher path layer. Consists of a VC-n plus a tributary unit pointer TU PTR.

Tributary Unit Pointer (TU PTR)
Indicates the phase alignment of the VC with respect to the TU in which it resides. The pointer position is fixed with respect to the TU frame.

TSA
Time Slot Assignment

TSI
Time Slot Interchange

TTP
Trail Termination Point

TUG
Tributary Unit Group

U **UAS**
UnAvailable Seconds

ULDT
Ultra Long Distance Transmission

UIM/X
A package used for developing the WaveStar® ITM-SC GUI for X-windows.

Unavailable Seconds
A performance monitoring parameter.

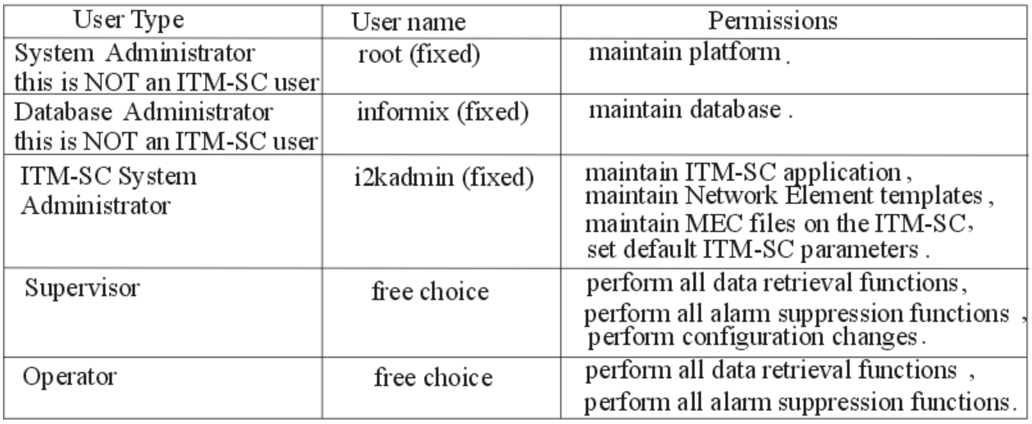
Uninterruptable Power Supply (UPS)
Allows connected computer equipment to gracefully shutdown, therefore preventing damage in case of a power fail and absorb dips in the supplied power.

Universal Co-ordinated Time (UTC)
A time-zone independent indication of an event. The local time can be calculated from the Universal Co-ordinated Time.

UPL
User PaneL

Upstream
At or towards the source of the considered transmission stream, i.e. looking in the opposite direction of transmission.

User Privilege
Permissions a user has to perform actions on the computer system on which the ITM-SC application runs. The following users can be distinguished:



User Type	User name	Permissions
System Administrator this is NOT an ITM-SC user	root (fixed)	maintain platform .
Database Administrator this is NOT an ITM-SC user	informix (fixed)	maintain database .
ITM-SC System Administrator	i2kadmin (fixed)	maintain ITM-SC application , maintain Network Element templates , maintain MEC files on the ITM-SC, set default ITM-SC parameters .
Supervisor	free choice	perform all data retrieval functions, perform all alarm suppression functions , perform configuration changes.
Operator	free choice	perform all data retrieval functions , perform all alarm suppression functions.

V **VF**

Voice Frequency

Virtual Container (VC)

Container with path overhead.

W **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.

WAN

Wide Area Network

Wander

Long term variations of amplitude frequency components (below 10 Hz) of a digital signal from their ideal position in time possibly resulting in buffer problems at a receiver.

WaveStar® ADM 16/1

A network multiplexer that is designed to flexibly multiplex plesiochronous and STM-1 tributary port signals into STM-4 or STM-16 line port signals.

WaveStar® Integrated Transport Management Subnetwork Controller (ITM-SC)

Manager for SDH Network Elements in a subnetwork. Also referred to as Element Management System.

WaveStar® Network Management System (NMS)

Manager for SDH Network Elements in a network. Formerly known as DACScan-T.

WDM

Wavelength Division Multiplexing

What You See Is What You Get (WYSIWYG)

Information as displayed on the screen will appear in the same way on printed output.

Wideband Communications
Voice, data, and/or video communication at digital rates from 64 kbit/s to 2 Mbit/s.

Windows
Graphical User Interface on PC systems.

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.

WS
Work Station

WSF
Work Station Facility

X

XMTR
Transmitter (RR)

XMTR Switch Unit
Radio Relay circuit pack that performs connections for protection switching and transmission of low priority traffic on the protection channel.

XPIC
Cross Polarization Interference Cancellation

XSU
XMTR Switch Unit (RR)

X-Terminal
Workstation that can support an X-Windows interface

X-Windows
Graphical User Interface on Unix Systems.

Lucent Technologies
Bell Labs Innovations

Index