Lucent Technologies
Bell Labs Innovations

DEFINITY® Fault Management Release 2.0

User Guide

J58890UC L107
PG-5E677
585-229-808, Issue 1
November 1998

Contents

About This Book

Chapter Contents

Introduction

This chapter contains helpful information about the documentation and the Lucent resources available to customers for the **DEFINITY Network Management Release 2.0** products, which include:

- DEFINITY Proxy Agent
- DEFINITY Fault Management
- DEFINITY Performance Management (new product)

The ***User Document Set*** section contains the complete list of installation guides and user guides that are delivered on CD-ROM. This section also includes an overview of this book, the target audience for this book, and the format conventions used in the procedures.

The ***Lucent Resources*** section includes essential information about the Project Provisioning Package which contains:

- System requirements for hardware and software
- Ordering information
- Installation options
- Custom services
- Lucent and customer responsibilities

The account executives can provide customers with a copy of the Project Provisioning Package upon request.

User Document Set

The ***User Document Set*** for Release 2.0 is delivered on a separate CD-ROM. The CD-ROM contains all the installation and user guides for the **DEFINITY Network Management Release 2.0** products, including:

- DEFINITY Proxy Agent Installation Guide
- DEFINITY Proxy Agent User Guide
- DEFINITY Fault Management Installation Guide
- DEFINITY Fault Management User Guide
- DEFINITY Performance Management and Common Software Installation Guide
- DEFINITY Performance Management User Guide

The ***installation guides*** for the products specifically cover the procedures to install and set up the software so that the product is ready to use. Generally, only an experienced network manager should install and set up the software.

The ***user guides*** for the products describe the functions, screens, and procedures to operate and manage the software. Once the software is set up, then users should refer to the user guides to operate and administer the product.

Installation Procedures

The insert on the CD-ROM contains the procedures to install the guides on Windows. The ***Readme*** file on the CD-ROM also contains the complete procedures to install the guides on UNIX and networks.

Main Menu

After you install the guides, you can access the books from the **Main Menu.**

The **Introduction** section on the Main Menu contains procedures for navigating between the books and searching for specific information.

The **Comments** section contains an evaluation form. You are encouraged to submit the form with your suggestions for improvements ***and*** comments on the useful elements of the documentation.

DEFINITY Fault Management User Guide

The ***DEFINITY Fault Management User Guide Release 2.0*** contains the explanation and procedures to manage the day-to-day operations of the software and related external devices.

The user guide is divided into two sections:

- Section 1 Network Management Systems (NMS) includes chapters 1 through 4. For an overview of the chapters, refer to *Chapter 1, "NMS Overview"*.
- Section 2 DEFINITY Fault Management includes chapters 5 through 12. For an overview of the chapters, refer to *Chapter 5, "Fault Management Overview"*.

The chapters in the NMS overview are laid out by functions and are organized by the primary tasks to operate the software, including:

- Login and access procedures
- System help and navigation features
- Administration procedures to add, change, and delete data
- Operational procedures to manage the software features and functions

The user guide is an essential resource for users who are unfamiliar with the purpose and operation of the product.

Audience

The target audiences for the ***DEFINITY Fault Management User Guide Release 2.0*** are general users at all levels.

The **customer** users include the following:

- Network managers
- System administrators
- Technicians

The **Lucent** users include the following:

- Service providers and technicians
- Sales teams
- Training and Education
- Translation Services

The user guide is particularly helpful to ***new*** users who administer the software as part of their routine duties.

Format Conventions

The format conventions used in this book are visual cues to help users identify the type of action they should take to execute the steps in the procedures.

The use of the format conventions are consistent throughout all the books in the ***User Document Set*** for this release.

Table 1. Format Conventions

Convention	Description
Bold text	Indicates that you should type the **bold text** exactly as shown. Example: Type **display status**
	1 of 3

Table 1. Format Conventions

Convention	Description
[**Bold text in brackets**]	Indicates that you should type **discrete** data that is specific to your system, ***without*** the brackets. Discrete data can be any of the following: • Managed node name • Name of a directory or file • Drive name • Any data that is ***not*** a default option Examples: • Type [**d**] **install** • Type your [**password**] • Select the [**managed node name**] from the Help list.
Function keys	Appear in bold capital letters and indicate that you should press that key on the keyboard to execute a specific action. Examples: • Press **ENTER** (also refers to the **RETURN** key) • Press **TAB** • Press **ESC**
	2 of 3

Table 1. Format Conventions

Convention	Description
Series of Menu Options **File > Save**	The greater than (**>**) symbol indicates that your should select an option from a series of menus. For example, Click **File > Save** means that you should: • Click on the first menu (File). • Then click on the second option (Save) from the second menu.
Result paragraph	Describes the result of an action taken in a step, as described in the following example: ***Result:*** The system displays the MAIN MENU. A results paragraph may also contain a message or a prompt in `constant width` font. A prompt sets up the action to be taken in the next step. ***Result:*** The system displays the command window that contains the prompt: `Do you wish to continue? y/n`
	3 of 3

Lucent Resources

Lucent Technologies provides customers with a variety of planning, consulting, and technical services.

The ***account executives*** are the customers' primary source to obtain information and explore custom options to meet their specific business needs.

The sections below briefly describe the services that are available to customers.

Project Provisioning Package

The ***Project Provisioning Package*** for this release contains the specific recommendations and specifications to plan and install the ***DEFINITY Network Management*** products.

A copy of the Project Provisioning Package is posted on the DEFINITY Solutions website. You can access the website at:

www.bcs.lucent.com/sales_market/definity/sysmgmt/dfm.htm

Customers can also request a copy of the package from their account executive.

The package is intended to clarify the responsibilities of the customer and Lucent during the installation project. The package contains the following information:

- Installation options (see below)
- Connectivity diagrams
- Ordering information
- Pre-installation hardware and software requirements

- Installation schedule and responsibilities
- Platform acceptance test
- Post installation verification and acceptance

The Provisioning Package also contains detailed explanations of the three (3) implementation options that are available to customers:

1. Customer installation of the NMS platform and DEFINITY Network Management products.
2. Lucent Technologies Technical Support Center (TSC) installation of the DEFINITY Network Management products.
3. Lucent Technologies NetCare® Network Consulting Group installation of a complete ***turn-key*** system for the Network Management System (NMS).

Options two and three are further explained in the sections below.

Technical Support Center (TSC)

The Technical Support Center (TSC) is part of the Technical Support Organization (TSO).

You can call the Technical Support Organization (TSO) at the toll-free number below and follow the prompts to reach the TSC:

TSO 1-800-242-2121

The Technical Support Center (TSC) works with account executives and customers to install and support the DEFINITY Network Management products.

Both the customer and TSC perform the Post Installation Verification and Acceptance Test of Fault Management.

Time and Materials Charges

If customers choose to install the DEFINITY Network Management products themselves, then the TSC is ***not*** responsible for the installation of the product software.

If the customers do ***not*** install and set up the system according to the guidelines in the Project Provisioning Package, then the TSC will bill the customers for support on a time and materials basis.

NetCare Network Consulting Group

The NetCare® Network Consulting Group is part of the Professional Services Organization. NetCare is available to work with customers to design and build a ***turn-key*** Network Management System.

Customers can select all or any combination of the NetCare services summarized below:

- Plan and design a custom network system
- Purchase and configure the Network Management System (NMS)
- Install and integrate the DEFINITY Network Management software products on the NMS platform
- Train users on the operation and management of the software tools

Account executives can provide customers with additional information about NetCare and other custom services.

Year 2000 Compliance

The Business Communication System (BSC) part of Lucent Technologies makes the following statement with respect to any product manufactured and sold by Lucent BCS in connection with a product's operation in the year 2000.

Any product or version/release of a product that is introduced as generally available on or after September 30, 1996, will be year 2000 compliant or Lucent BSC will make it year 2000 compliant at our cost.

Any other product, depending on the specific product and its release or version, will fit into one of the following categories:

- The product is year 2000 compliant.
- If the product is not year 2000 compliant, Lucent BCS will provide an upgrade path to a generally available release that is year 2000 compliant at a reasonable cost to the customer; or
- If the product is not year 2000 compliant, and no upgrade path to a generally available release that is year 2000 compliant is available, Lucent BCS will evaluate whether there are potential modifications to the product that will make it year 2000 compliant, and if Lucent BCS determines that such modifications are economically practical, Lucent BCS will offer such modifications to the customer at a reasonable cost; or
- If the product is not year 2000 compliant, and if Lucent BCS determines that it is not economically practical to make the product year 2000 compliant, Lucent BCS will inform the customer of this fact and offer migration options at a reasonable cost.

1 NMS Overview

Chapter Contents

Introduction

The Network Management System (NMS), and the DEFINITY Proxy Agent, along with DEFINITY Fault Management facilitate centralized management of DEFINITY systems. To maintain this centralized management, Fault Management complies with Simple Network Management Protocol (SNMP). While the DEFINITY Proxy Agent is SNMP compliant, it operates remotely and connects to multiple managed nodes concurrently.

SNMP Information Exchange

SNMP specifications define how Performance Management and DEFINITY systems exchange information. The information exchange works like this:

- Proxy Agents receive data from managed nodes.
- Proxy Agents manage the information with a Management Information Base (MIB).
- Proxy Agents use SNMP protocol to translate the information into data that the NMS can read.
- Proxy Agents forward alert and threshold data to the NMS.
- Finally, the NMS translates and displays the information on submaps that depict DEFINITY systems.

NMS Submaps

On these maps, the NMS creates icons that represent managed nodes and Proxy Agents and also creates lines to represent connections between each Proxy Agent and its associated managed nodes. The NMS has the capability to produce three different submap options to depict a DEFINITY system. This allows you to organize managed nodes by geographic location or in a customized fashion as well as with one all-encompassing, generic map.

The icons on these submaps change colors to identify alarm states for Proxy Agents and alerts for managed nodes. The lines change colors to indicate changes in the connection states between Proxy Agents and their associated managed nodes.

ThIs chapter contains the following information:

- Descriptions of new features
- Descriptions of NMS capabilities
- Commands used to access information in the NMS
- Steps to access the NMS
- Steps to exit from the NMS

New Features

The list below contains a brief description of the updates to Fault Management, Release 2.0:

Supported systems

Fault Management supports the following systems:

- DEFINITY PBX G3, Release 4 and DEFINITY ECS, Release 5 through 6
- Multipoint Conferencing Unit (MCU) Version 5.0
- Supports DEFINITY Legacy equipment at the Network Management System (NMS) level

Network Management products

Fault Management is compatible with the following network management products:

- DEFINITY Proxy Agent, Release 2.0
- DEFINITY Performance Management, Release 2.0

Connection types

The Proxy Agent now supports both ***static*** and ***dynamic*** connections to managed nodes.

You can assign up to **150** dynamic connections on the MANAGED NODES screen. The Proxy Agent only supports **30** active connections at a given time. The 30 active connections can be a combination of static and dynamic connections.

Static connections

A ***static*** connection maintains a ***continuous*** communication link between the Proxy Agent and the managed node.

We recommend that you select the static connection to monitor ***critical*** managed nodes for 24 hours per day, 7 days per week.

Dynamic connections

A ***dynamic*** connection maintains a ***temporary*** communication link between the Proxy Agent and the managed node.

We recommend that you select the dynamic connection to monitor ***less critical*** managed nodes on an as-needed basis.

Any Simple Network Management Network Protocol (SNMP) request or alarm on a managed node will initiate a dynamic connection. The dynamic connection will stay up as long as the Proxy Agent is actively processing SNMP requests and then ***time-out*** after a specified period.

The NMS does ***not*** poll for health data if a dynamic connection is assigned to a managed node.

System Requirements

The ***Project Provisioning Package*** for this release contains the ***specific*** recommendations and specifications to plan and install the Fault Management software.

The package also defines the terms and conditions for the three installation options:

- Customer installation
- Technical Support Center (TSC) installation services
- NetCare® Network Consulting Group installation of a complete ***turn-key*** system

Refer to *"Lucent Resources" on page 17* for more information.

Hardware Requirements

You should work with your Lucent account executive to determine the hardware requirements that your organization needs to meet its business and performance specifications.

Supported Systems

Release 2.0 of Fault Management ***only*** supports the switches listed below:

- DEFINITY G3 PBX release G3V4 through DEFINITY ECS release R6
- Multipoint Conferencing Unit (MCU) version 5.0 and later
- Legacy equipment at the NMS level

Software Requirements

The DEFINITY Fault Management application operates with the software listed below:

- DEFINITY Proxy Agent, Release 2.0
- DEFINITY Performance Management, Release 2.0 (new product)
- DEFINITY Network Management Common Software (required if Fault and Performance Management are both installed)
- Network Management System (NMS) platform (see below)

NMS Platforms

The DEFINITY Fault Management 2.0 product supports the following Network Management System (NMS) platforms:

- HP OpenView Releases 4.11, 5.0, and 5.01 installed on hardware below:
  - Solaris Release 2.5.1
  - HP/UX Release 10.20
- Tivoli TME 10 NetView Release 4.1.2 installed on AIX Releases 4.1.5

NMS Capabilities

The Network Management System (NMS) provides an overall view of DEFINITY systems. The two NMS platforms used with Fault Management are: NetView and OpenView. Both platforms provide identical functionality for monitoring DEFINITY equipment. The differences between the two programs is evident only in command procedures.

This section contains brief descriptions of the chapters that discuss NMS capabilities.

NMS Submaps

Chapter 2, "NMS Submap Administration" describes the 4 submap options available on the NMS. This chapter also contains procedures that are necessary to set up maps in the NMS.

NMS Alarm Notification

Chapter 3, "NMS Alarm Notification" describes alarm states and alarm notification methods available at the NMS level. This chapter also contains procedures that are necessary to access information regarding alarm states.

Legacy Equipment

Chapter 4, "Legacy Equipment" identifies Legacy equipment. This chapter also contains procedures necessary to set up Legacy equipment and to access detailed information regarding alarms and errors that occur on Legacy equipment.

NMS Command Procedures

Each icon or connection line on an NMS submap provides access to command procedures or to screens that contain information about managed nodes or connections.

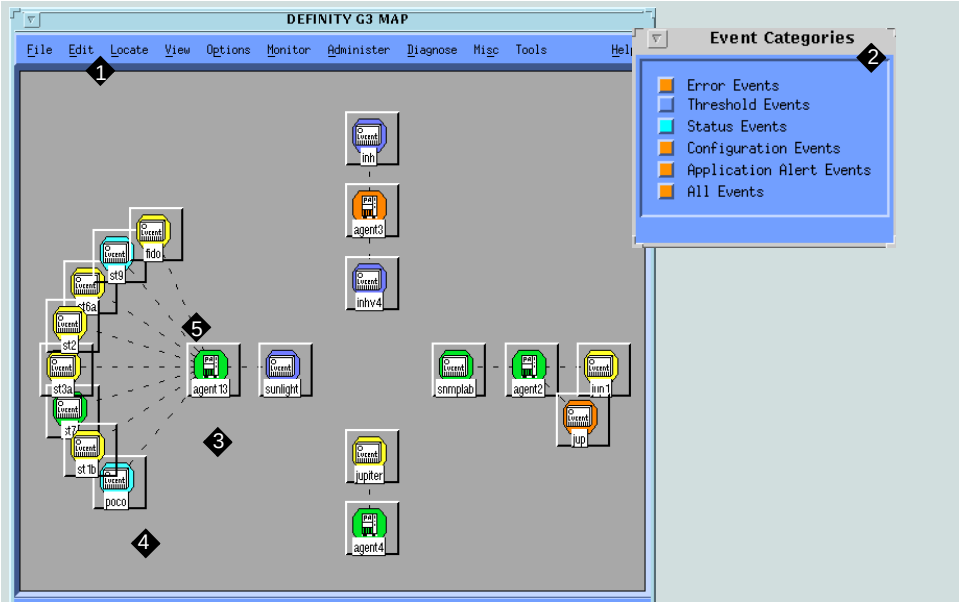
In addition, each icon provides access to one of the following applications:

- Proxy Agent
- Trouble Tracker
- Fault Management

Both NetView and OpenView provide multiple methods for accessing this information. This section identifies screen components that allow you to initiate commands and contains descriptions of commands available on the NMS.

Screen Components

The following example is a generic submap with screen components that display on any submap.



1 Menu Bar
2 Application Alert Event Log
3 Proxy Agent Icon
4 Managed Node Icon
5 Connection Line

Figure 1. DEFINITY Generic Submap

Menu Bar

To access submenus for DEFINITY equipment, click an icon or a connection line. Then, select one of the following:

- For OpenView, select **Fault > DEFINITY**
- For NetView, select **Monitor > DEFINITY**

Result: The system displays the DEFINITY submenu

The selections that are available on this submenu vary based upon the graphical element you selected. Items that are ***not*** available display in grey.

Application Alert Event Log

The Application Alert Event Log contains a running record of actions that occur on the NMS.

The following example shows activity that occurred in the All Events category.

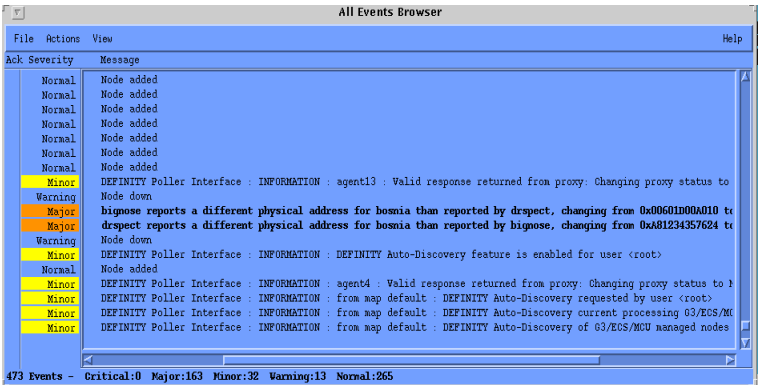


Figure 2. Application Event Alert Log — All Events

Proxy Agent Icon

When you select a Proxy Agent Icon, DEFINITY submenu options reflect commands that are available for that Proxy Agent. You may also double-click the Proxy Agent icon to initiate a telnet session to the Proxy Agent application.

If you have OpenView, you can select the Proxy Agent Icon. Then, press the third mouse button to display a menu that contains the same information as the DEFINITY submenu located on the main menu bar.

Legacy Icon

Legacy Icons have a single capability. When you double-click any Legacy Icon, you initiate a telnet session to the Trouble Tracker.

Managed Node Icon

When you select a managed node icon, DEFINITY submenu options reflect commands that are available for that managed node. You may also double-click a managed node icon to start the Fault Management application.

If you have OpenView, you can select a managed node icon. Then, press the third mouse button to display a menu that contains the same information as the DEFINITY submenu located on the main menu bar.

Connection Line

When you select a connection line, the DEFINITY submenu options reflect commands that are available for that connection. You may also double-click the connection line to display the Connection Status screen.

If you have OpenView, you can select a connection line. Then, press the third mouse button to display a menu that contains the same information as the DEFINITY submenu located on the main menu bar.

NMS Access Procedure

To access the NMS, complete the following steps:

Procedure 1. Access the NMS

Step	Action
1	Log in to UNIX.
2	At a UNIX prompt, type one of the following: • NetView: **$OV_BIN/nv6000** • OpenView: **$OV_BIN/ovw&** ***Result:*** The system opens the NMS application

NMS Exit Procedure

To exit from the NMS, complete the following steps:

Procedure 2. Exit from the NMS

Step	Action
1	Close all programs associated with the NMS.
2	At the main window, select one of the following: • NetView: Click **File > Exit** • OpenView: Click **Map > Exit** ***Result:*** The system closes the NMS application.

2 NMS Submap Administration

Chapter Contents

Introduction

The Network Management System (NMS) provides graphical user interface (GUI) capabilities that allow you to view alarm states for Proxy Agents and managed nodes. You can also view the connection status between Proxy Agents and their associated managed nodes.

The NMS creates four network submaps to display this information. These submaps include:

- Generic
- USA
- Custom
- Legacy

This chapter contains the following NMS submap procedures:

- Select a network submap
- Modify submap information on the Proxy Agent
- Modify submap information in the *Location Override* file

Description: Auto-Discovery

Using the Auto-Discovery feature, the NMS performs the following functions to translate data from the Proxy Agent into these submaps:

- Searches for Proxy Agent and managed node data
- Adds Proxy Agent icons and managed node icons to designated DEFINITY submaps
- Shows connections between Proxy Agents and managed nodes
- Shows connections between Trouble Trackers and Legacy managed nodes

To utilize Auto-Discovery you must assign Auto-Discovery passwords and set up the Auto-Discovery feature.

Set Auto-Discovery Passwords

The default installation setting for Fault Management grants access to Auto-Discovery for all users. Users who have access to Auto-Discovery can modify NMS submaps.

If you wish to restrict Auto-Discovery access, you must assign Auto-Discovery passwords. Anyone who has root level access can restrict individual or group access to Auto-Discovery.

Procedure: Set Auto-Discovery Passwords

Procedure 3. Set Auto-Discovery passwords

Step	Action
1	To administer Auto-Discovery passwords, edit one of the following files from a UNIX editor: • NetView: **/usr/OV/OneVision/DG3Poll/AD_Passwds** • OpenView: **/opt/OV/OneVision/DG3Poll/AD_Passwds** ***Result:*** The system displays the Auto-Discovery passwords administration file.

Procedure 3. Set Auto-Discovery passwords

Step	Action
2	In the first field, type one of the following options in upper case: • **L** for an individual user • **G** for groups of users Press the **SPACEBAR**
3	In the second field, type one of the following in lower case: • individual [**unix login id**] • group [**unix group id**] Then, press **ENTER** ***Result:*** The system designates user access to Auto-Discovery.
	2 of 2

SECURITY ALERT:

Unauthorized users who attempt to access Auto-Discovery receive a message in the Application Alert Event Log that provides authorization status for each user. The NMS displays the Application Alert Event Log appears on all NMS screens.

Set Up Auto-Discovery

To set up NMS submaps, you must activate Auto-Discovery. Activating Auto-Discovery allows the NMS to create submaps from information that was transmitted from Proxy Agents.

Setting up Auto-Discovery on a public network differs from the process of setting up Auto-Discovery on a private network. This section contains procedures for both network types.

Set up Public Networks

If you have a public network, follow the procedure below to set up Auto-Discovery. This procedure activates Auto-Discovery for the first time and during any active network session.

Procedure 4. Set up public networks

Step	Action
1	Access the Network Management System.
2	From the menu bar, select one of the options below: • In NetView, click: **Monitor > DEFINITY > Execute Auto-Discovery** • In OpenView click: **Fault > DEFINITY > Execute Auto-Discovery** ***Result:*** The system activates Auto-Discovery.

Set up Private Networks

If you have a private network, you must complete the following steps to ensure that the Proxy Agent and NMS can communicate effectively.

The entries you type in the NMS must ***exactly*** match the entries that you typed in the Proxy Agent. Refer to the PA001 form that was used during the installation for the DEFINITY Proxy Agent.

Procedure 5. Set up private networks

Step	Action
1	From the menu bar in the Network Management System, click **Options > SNMP Configuration**. ***Result:*** The system opens the SNMP Configuration window and displays existing managed nodes at the top portion of the screen.
2	Turn off the **USE PROXY TO ACCESS TARGET** button, if it is selected.

1 of 2

Procedure 5. Set up private networks

Step	Action
3	Type information in the fields below. Do ***not*** change any other fields. • *Target* — Proxy Agent [**host name or IP address**] The name that resides in the host file. • *Get Community String* — [**community name**] The name you administered for the private network on the Proxy Agent *Network Managers* screen. • *Set Community String* — [**g3pa**] Identical to the Set Community data administered on the Proxy Agent *Network Managers* screen.
4	Click **ADD**. Then, click **OK**.
5	To activate Auto-Discovery, select one of the following commands: • In NetView, click: **Monitor > DEFINITY > Execute Auto-Discovery** • In OpenView, click **Fault > DEFINITY > Execute Auto-Discovery** ***Result:*** The system activates Auto-Discovery.
	2 of 2

Select Network Submap

The NMS provides four submap options that allow you to organize your DEFINITY system in four different ways. You can organize your DEFINITY system using the following submaps:

Description: NMS Submap Options

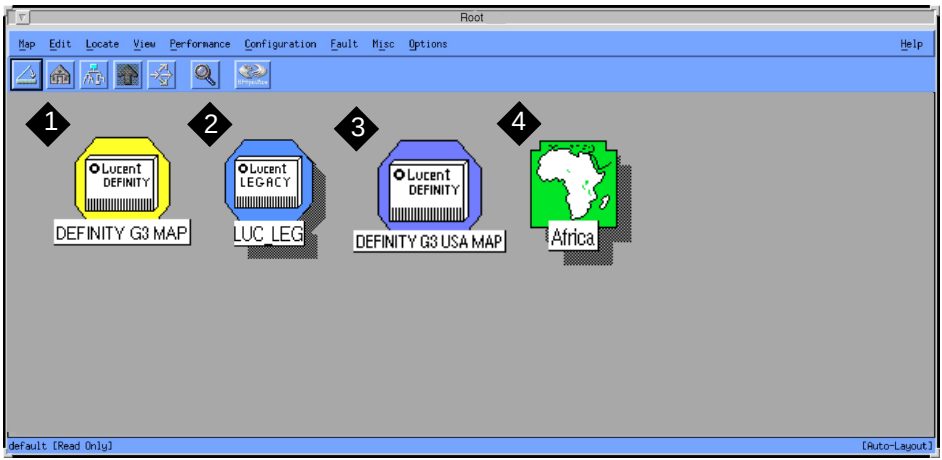
- Generic submap. The Generic submap is the system default. This submap provides point-to-point connections and displays an overview of your DEFINITY system.
- USA submap. The USA submap allows you to organize your DEFINITY system by geographic location in the United States. The USA submap allows you to drill down to state submaps.
- Custom submap. The custom submap allows you to organize your DEFINITY system according to your specific business needs. The custom submap allows you to place icons on a user-specified submap.
- Legacy submap. The Legacy submap provides point-to-point connections that allow you to monitor Legacy equipment and Trouble Trackers.

This section provides the following information about submaps:

- Advantages for using each submap
- Graphical views of each submap
- Procedures to access submaps

Example: Icons to Access Submaps

The system displays the Root map when you log in to the NMS. Icons representing NMS submaps display on this screen. The example below shows DEFINITY submap icons that appear on the Root map.



1 DEFINITY Generic submap icon
2 DEFINITY Legacy submap icon
3 DEFINITY USA submap icon
4 DEFINITY Custom submap icon

Figure 3. NMS Root map

Generic Submap

The generic submap uses a point-to-point layout to display an overview of all Proxy Agents and their associated managed nodes. The generic submap resides on the open map and at the root level of the NMS.

Example: Generic Submap

You double-click the DEFINITY Generic submap icon on the Root map to open the DEFINITY submap shown below.

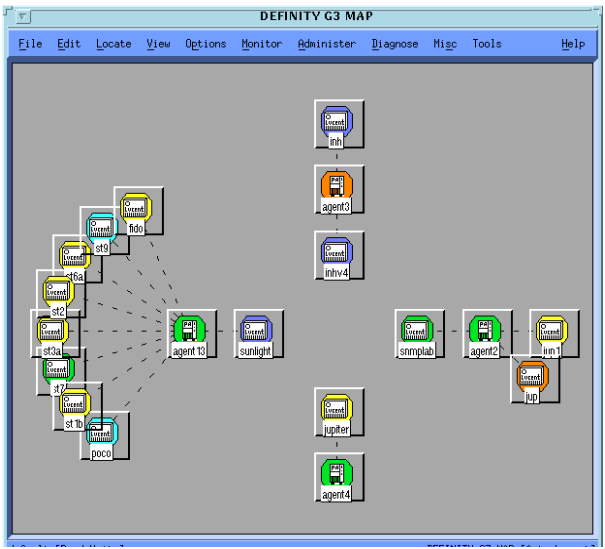


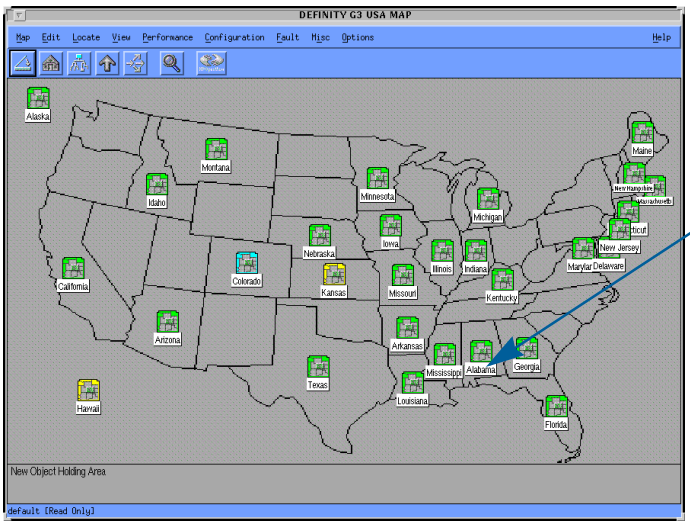
Figure 4. Example of a DEFINITY submap

USA Submap

The USA submap allows you to view your DEFINITY system by geographic location. Managed nodes and Proxy Agent icons appear on the state that you administered in the Proxy Agent.

Example: USA Submap

You double-click the DEFINITY USA submap icon on the Root map to open the DEFINITY USA submap shown below:



Double-click a managed node icon in a state to open a submap that displays all DEFINITY managed nodes in that state.

Figure 5. Example of a DEFINITY USA submap

Example: State Submap

You double-click a managed node icon on a USA submap to display a state submap similar to the map shown below. The state submap shows the status of a connection between the managed node and the Proxy Agent.

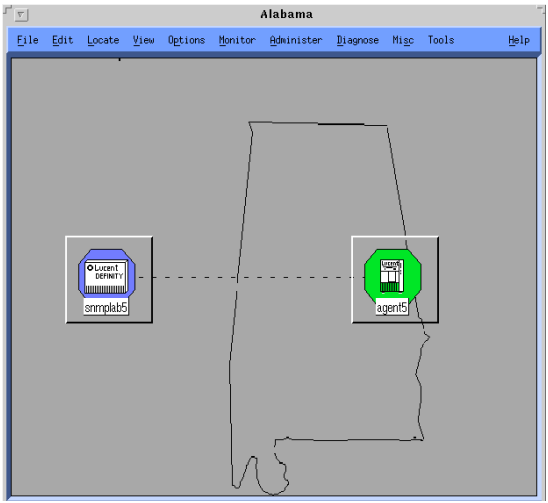


Figure 6. Example of a state submap

Custom Submap

Custom submaps allow you to manage the DEFINITY system at a more specific level than the other submaps. For example, you can organize information according to business territories or according to the type of DEFINITY systems that you manage.

Example: Custom Submap

To create a custom submap similar to the example below, you must administer a custom map on the Proxy Agent *Managed Nodes* screen or the Auto-Discovery configuration file.

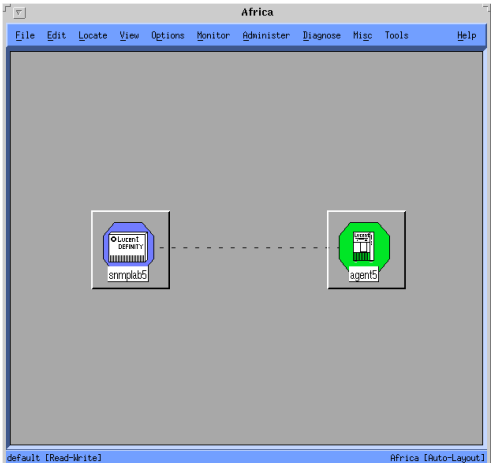


Figure 7. Example of a custom submap

Legacy Submap

The Legacy submap is designed to monitor early releases of DEFINITY equipment and AUDIX equipment. However, you can also monitor more current releases of DEFINITY equipment from the Legacy submap.

Example: Legacy Submap

You double-click the DEFINITY Legacy submap icon on the Root map to open the DEFINITY Legacy submap shown below:

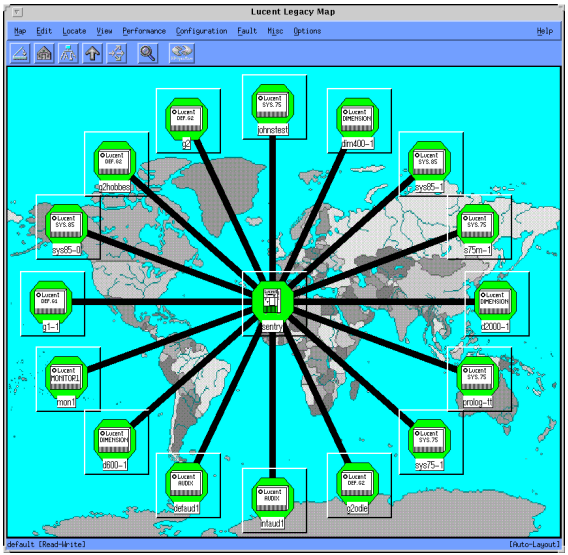


Figure 8. Example of a DEFINITY Legacy submap

Manage Submap Connections

The NMS allows you to view two types of connections and to view the status of each connection. The two types of connections that you can administer are: static or dynamic. The status of each of these connections reflects the activity of that connection.

From the NMS, you can connect managed nodes to Proxy Agents, disconnect managed nodes from Proxy Agents, and verify the status of a connection.

This section contains:

- Graphical depictions of connections as they appear on network submaps
- Descriptions that contrast the differences between static and dynamic connections
- Descriptions of the six connection status
- Procedures to establish connections
- Procedures to drop connections
- Methods to verify connection status

View Types of Connections

To view connection types, you must go to a DEFINITY submap. At the submap, you will see one of the following types of connections:

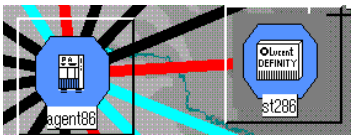


Figure 9. Sample OpenView 5.0 static connection

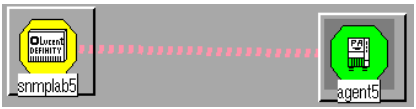


Figure 10. Sample OpenView 5.0 dynamic connection

Figure 11. Sample NetView or OpenView 4.11 static connection

Figure 12. Sample NetView or OpenView 4.11 dynamic connection

Static and Dynamic connections

The Proxy Agent release 2.0 supports both ***static*** and ***dynamic*** connections. A Proxy Agent only supports 30 ***active*** connections at a given time. The 30 active connections can be any combination of both static and dynamic connections.

However, if users administer 30 ***static*** connections, then the Proxy Agent will not allow the user to add any more managed devices, regardless of the connection type.

The following are examples of scenarios for assigning static and dynamic connections if either the DEFINITY Fault Management or the DEFINITY Performance Management products are installed on the Network Management Station (NMS):

- If users assign 25 static connections, the system allows them to add 125 managed devices with dynamic connections. This frees 5 ports to connect to the 125 managed nodes.
- If users assign 10 static connections, then the system allows them to add 140 managed devices with dynamic connections. This frees 20 ports to connect to 140 managed devices.

The examples above work similarly for DEFINITY Performance Management. However, we ***recommend*** that if users collect hourly data on certain DEFINITY systems, then they should only administer **30** static connections to each Proxy Agent. This will ensure continuous and accurate data collection for those systems.

Customers can resolve these limitations by adding additional Proxy Agents and then spread the static connections across the Proxy Agents.

Identify Connection Status

Each connection line appears in one of six colors that represent the six status options for connections. If you do not wish to use the system default colors, you may assign a custom color by modifying values in the **$APP_DEF/OVw** file. The table below describes connection status.

Table 2. NMS connection status

NMS	Status on the NMS	Default Color	Connection Status
NetView	OVw*unknownStatusLineColor	Cyan	Off
OpenView	OVw*warningStatusLineColor	Cyan	Off
NetView	OVw*marginalStatusLineColor	Yellow	Init
OpenView	OVw*marginalStatusLineColor	Yellow	Init
NetView	OVw*downStatusLineColor	Red	Down
OpenView	OVw*downStatusLineColor	Red	Down
			1 of 2

Table 2. NMS connection status

NMS	Status on the NMS	Default Color	Connection Status
NetView	OVw*downStatusLineColor	Red	Other
OpenView	OVw*downStatusLineColor	Red	Other
NetView	OVw*upStatusLineColor	Black	Up
OpenView	OVw*upStatusLineColor	Black	Up
NetView	OVw*user1StatusLineColor	Green	Idle
OpenView	OVw*testingStatusLineColor	Pink	Idle
			2 of 2

Connect a Managed Node

The NMS allows you to establish connections between a Proxy Agent and a managed node with the following steps:

Procedure: Connect a Managed Node

Procedure 6. Connect a Managed Node

Step	Action
1	Click on the line that represents a connection between a Proxy Agent and a managed node.
2	Select one of the following: • OpenView: Click **Fault > DEFINITY > Start Connection** • NetView: Click **Monitor > DEFINITY > Start Connection** ***Result:*** The system changes the connection line to black when the managed node connects successfully. If the connection does not achieve a successful connection, the line turns yellow indicating a status of **init**.

Disconnect a Managed Node

The NMS also allows you to disconnect a managed node from a Proxy Agent.

CAUTION:
If you disconnect a managed node, you place it in a status of **off**. To use this connection in the future, you must readminister the connection on the Proxy Agent.

Procedure: Disconnect a Managed Node

To disconnect a managed node from a Proxy Agent, complete the following steps:

Procedure 7. Disconnect a Managed Node

Step	Action
1	Click the line that represents a connection between a Proxy Agent and a managed node.
2	Select one of the following options from the menu bar: • OpenView: Click **Fault > DEFINITY > Stop Connection** • NetView: Click **Monitor > DEFINITY > Stop Connection** ***Result:*** They system changes the connection to cyan when the managed node disconnects from the Proxy Agent.

View Connection Status

During any active NMS session, you can access details about a selected connection. The information you can view is similar to the example shown below.

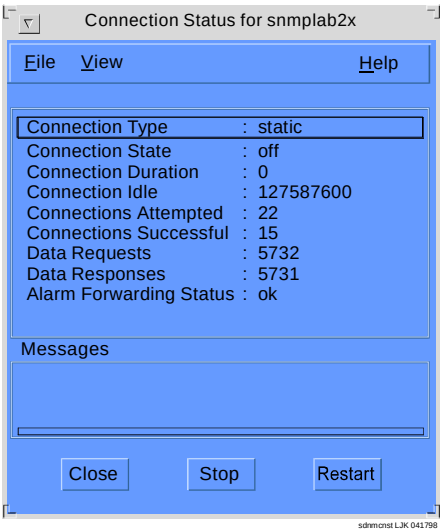


Figure 13. Sample Connection Status

Field Description

The following table provides descriptions for the connection details available on the Connection Status screen.

Table 3. Field descriptions for the Connection Status screen

Field	Description
Connection Status	The selected status for the connection. The connection status can be: **init**, **up**, **down**, **off**, **idle**, or **other**.
Connection Type	The type of connection: **static** or **dynamic**.
Connection Duration	The length of time that a connection is in the **up** status.
Connection Idle	The length of time that a connection is in the **idle** status.
Connections Attempted	The number of times the Proxy Agent attempted to connect to the managed node.
Connections Successful	The number of successful connections from the Proxy Agent to the managed node.
Data Requests	The number of data requests from a Proxy Agent to a managed node.
Data Responses	The number of times a managed node responds to a data request from a Proxy Agent.

Table 3. Field descriptions for the Connection Status screen

Field	Description
Alarm Forwarding Status	The system displays **ok** if the alarm status transmitted successfully. The system displays **failed** if the alarm status did not transmit successfully.
	2 of 2

View the Connection Status screen

To view details about a connection available on the Connection Status screen, complete the following steps:

Procedure 8. View the Connection Status screen

Step	Action
1	Click the line that represents a connection between a Proxy Agent and a managed node.
2	Select one of the following options from the menu bar: • OpenView: Click **Fault > DEFINITY > Connection Status** • NetView: Click **Monitor > DEFINITY > Connection Status** ***Result:*** The system displays the Connection Status screen for the selected connection.

Verify Connection Status

Proxy Agents maintain continuous contact with their associated managed nodes to transfer current data to the Network Management System (NMS). Lack of data or incorrect data can indicate that a connection problem exists.

The NMS provides several methods to verify connection status. The section describes the following methods you can use to verify connection status:

- Icon states
- Managed Node Lists
- Fault Management Startup Lists
- Warning Messages
- Data Refreshes

Icon States

In addition to providing alarm status, icon states also provide the current connection status for a managed node. You can determine the connection status of a managed node by viewing managed node icons on one of the four network submaps. See *Table 2 on page 54* for details.

Managed Node List screen

The Managed Node List screen contains all of the managed nodes that are connected to a Proxy Agent. This list shows the connection status for each managed node and other data as shown in the example below.

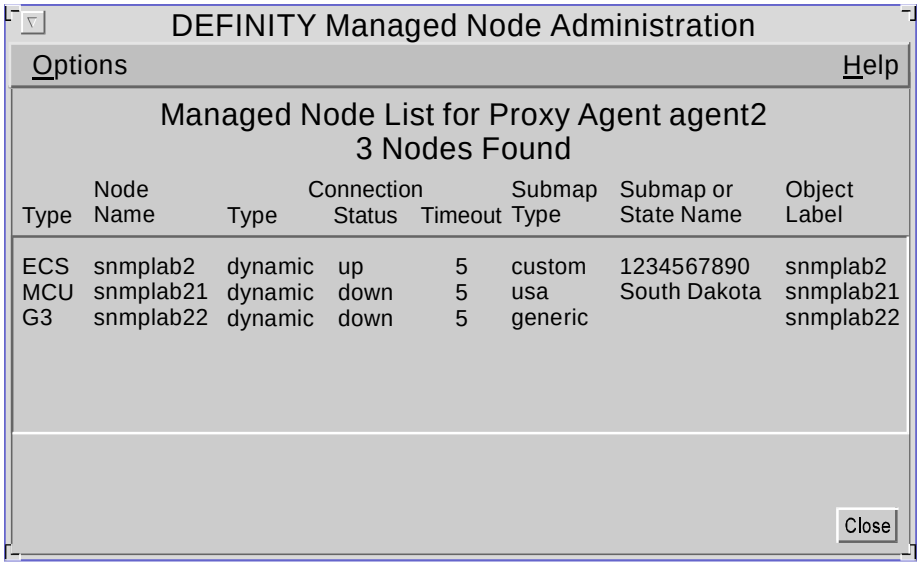


Figure 14. Managed Node List

Field Descriptions

The table below contains field descriptions for the Managed Node List for Proxy Agent screen shown above.

Table 4. Field descriptions for Managed Node List for Proxy Agent screen

Field	Description	Example
Type	The type of switch.	ECS
Node Name	The managed node name as administered in the Proxy Agent.	snmplab2
Connection Type	The type of connection: **static** or **dynamic**	dynamic
Connection	The status of the connection: **up**, **down**, **off**, **idle**, **other**, or **init**.	up
Timeout	Timeout refers to the time administered on the Managed Node screen on the Proxy Agent. This value indicates that the Proxy Agent must transfer data to the NMS before the allotted time expires.	60
Submap	The type of submap: Generic, USA, Custom, or Legacy	usa
Submap Location	The type of submap associated with either the USA or Custom submap	South Dakota

Table 4. Field descriptions for Managed Node List for Proxy Agent screen

Field	Description	Example
Object Label	The name you assign to an icon in the NMS. The object label does not need to match the name administered in the Proxy Agent.	Weiche
		2 of 2

Procedure: Open a Managed Node List

To open a managed node list, complete the following steps.

Procedure 9. Open a Managed Node List

Step	Action
1	Select a Proxy Agent icon from the network submap.
2	Select one of the following menu items: • NetView: Click **Monitor > DEFINITY > Show Managed Nodes** • OpenView: Click **Fault > DEFINITY > Show Managed Nodes** ***Result:*** The system displays the *Managed Node List for Proxy Agent* screen.

CAUTION:

The *Managed Node List for Proxy Agent* screen may not display the data or may display the data improperly.

Troubleshoot Managed Node List

Two problems can prevent the Managed Node List for Proxy Agent screen from opening or cause it to display improperly.

Problem 1. You opened the managed node list for Proxy Agent window, but no data displays.

Cause: The managed node list feature does not recognize the Proxy Agent.

Solution: Check the following:

- The network connection to the Proxy Agent must be up. If the connection is down, reconnect.
- The Proxy Agent running status. If the Proxy Agent is not running, start it.
- The Proxy Agent must be release 2.0. The managed node list feature does not recognize earlier versions.

Problem 2. The managed node list for Proxy Agent window displays data, but the data does not match the DEFINITY submap.

Cause: A managed node is administered with more than one Proxy Agent. Auto-Discovery can manage only one instance of a managed node.

Solution: Delete the managed node from all but one Proxy Agent.

Startup Messages

The Startup and Switch View screens in Fault Management display startup messages that tell you if the Proxy Agent is connected to a managed node:

The startup screen displays briefly. So, if you cannot read the messages, you can verify connectivity by refreshing data while Fault Management is running.

The table below contains messages that appear in the startup screen.

Table 5. Messages on the startup screen

Screen display	Connection status
`Refresh in progress, estimated delay nnn seconds, nnn seconds elapsed.` Tip: nnn = a number	Up
`Refresh on Startup Failed! Continuing with Cache Data.`	Down

Exception

Startup messages do not display if the *Refresh Proxy Agent On Startup* field on the Setup screen is set to **FALSE**.

You can access and modify this field by selecting ***Options > Setup*** on the Switch View in Fault Management.

Messages on the Switch View

If the Proxy Agent has not established a connection to a managed node during startup, the following items display:

- The Startup Refresh window appears in the center of the Switch View. The message in this window informs you that the refresh failed.
- A message also appears near the bottom of the Switch View. This message is described in *"Warning Messages" on page 69*.

Startup Refresh Window Does Not Display

The Startup Refresh window appears only if the *Refresh Proxy Agent On Startup* field on the Setup screen is set to **TRUE**.

You can access and modify this field by selecting ***Options > Setup*** on the Switch View.

Warning Messages

The following disconnect message appears in the message area of the Switch and Cabinet views:

```
WARNING: The data displayed is based on non-refreshed
cached data and may be out of date.
```

When warning messages appear

The system displays this message when either of the following conditions are true:

- The connection between the Proxy Agent and the managed node was not up when you started Fault Management
- The last refresh failed

The system displays this message regardless of the setting for the *Refresh Proxy Agent On Startup* field on the Setup screen.

Clearing the warning from the screen

Fault Management automatically clears this message from your screen after a successful alarms and errors refresh. This type of refresh indicates that the connection is **up** and that Fault Management has received new data.

Data Refreshes

You can verify that the Proxy Agent is connected to a managed node by refreshing the managed node data during a Fault Management session.

Fault Management can refresh managed node data only if the Proxy Agent is connected to the managed node. Therefore, if a refresh fails, the Proxy Agent may have lost contact with the managed node.

Manually Refresh Data

Complete the following steps to manually refresh data.

Table 6. Refresh data manually

Step	Action
1	Open the Switch View.
2	Select *one* of the following options from the menu bar: • ***Fault > Refresh Bulletin Board*** • ***Fault > Refresh Alarms and Errors*** • ***Configuration > Refresh Configuration Data*** ***Result:*** One of the following occurs: • A pop-up window states that the refresh failed, indicating that the connection is **down**. • No message appears, indicating that the connection is **up**.

Modify NMS Submaps

If you wish to change information for managed nodes, you can modify the Managed Node screen on the Proxy Agent or the data contained in the *Location Override* file on the Network Management System (NMS).

If you modify managed node information on the Proxy Agent all users have access to the updated information. If, however, you modify information in the *Location Override* file, only users who work at that terminal have access to the changes.

Modify the Location Override File

Modifying information in the *Location Override* file is particularly advantageous for users who:

- Wish to view DEFINITY systems in a different submap than was set up on the Proxy Agent
- Wish to hide managed nodes that they do not wish to view

Directions for modifying the *Location Override* file are contained within that file.

To modify the *Location Override* file, complete the following steps:

Procedure 10. Modify the Location Override file

Step	Action
1	At a UNIX prompt, edit one of the following files: • NetView: **/usr/OV/OneVision/DG3Poll/Location** • OpenView: **/opt/OV/OneVision/DG3Poll/Location** ***Result:*** The system displays the directions contained in the *Location Override* file.
2	Follow the directions contained in the *Location Override* file.
3	Write and quit the file.

Administer Changes on the Proxy Agent

The Proxy Agent allows you to complete the following actions for all DEFINITY systems except Legacy equipment:

- Add a managed node
- Modify a managed node location
- Delete a managed node
- Change a connection type

To make these changes, you must telnet to the Proxy Agent and modify the Managed Node screen. To telnet to the Proxy Agent, complete the procedure below.

Procedure 11. Telnet to the Proxy Agent

Step	Action
1	Double-click a Proxy Agent icon.
2	To log in to the Proxy Agent, type: **g3maadm** Then, press **ENTER** At the password prompt, type: [**password**] Then, press **ENTER** ***Result:*** The system displays the following command at the prompt: `Display Desktop y/n?`
3	Type **n** Then, press **ENTER**
4	To access the main Proxy Agent screen type: **proxy** Then, press **ENTER** ***Result:*** The system displays the main Proxy Agent screen.
5	Refer to *Chapter 4, Change Managed Nodes* in your *DEFINITY Proxy Agent User Guide* for procedures to make these changes.

3 NMS Alarm Notification

Chapter Contents

Introduction

When the Proxy Agent forwards traps to the Network Management System (NMS), the NMS color-codes icons to identify alarm states that occur on managed nodes.

When the NMS polls Proxy Agents and discovers an alarm, the NMS color-codes the associated Proxy Agent icons to reflect alarm states.

Fault Management comes with the facility to notify you by pager or by email when alarms occur. You may also install the add-on software, Tel-Alert or Remedy for additional notification capabilities.

This chapter describes the:

- Icon states for Proxy Agent alarms
- Icon states for managed nodes alarms
- Alarm notification methods

Identify Icons with Alarms

This section contains information that identifies icon states for Proxy Agents and managed nodes and describes the events that change an icon state.

When a Proxy Agent or a managed node has an alarm, the NMS colors the corresponding icon to indicate the severity of the alarm.

When a Proxy Agent or a managed node has multiple alarms with more than one level of severity, the icon color represents the most severe alarm

.

Proxy Agent Icon States

Proxy Agent alarms occur when alarm forwarding fails or when an authentication failure occurs. Because alarms manifest as colored icons, the following section refers to alarm states as icon states.

Each state of a Proxy Agent icon represents a condition that exists between a Proxy Agent and a managed node. The NMS platform assigns the names of these states.

The table below describes Proxy Agent icon states that occur in NetView and in OpenView.

Table 7. Proxy Agent icon states

NetView State Name	OpenView State Name	Description
Normal	Normal	The Proxy Agent is communicating with the NMS.
User1	Warning	The Proxy Agent is communicating with the NMS; however, the NMS received an Authentication Failure trap from the Proxy Agent.
User2	Major	The Proxy Agent failed to forward alarms to the administered destination.

Events that Change Proxy Agent Icon States

The color of a Proxy Agent icon changes when polling events or trap events indicate a change in the Proxy Agent alarm status.

Polling Events

The Proxy Agent icon state changes when the NMS polls one of the Proxy Agents and receives one of the unacceptable results identified in the table below.

Table 8. Polling changes for Proxy Agent icon alarm states

Result of poll	NMS	Default polling interval (min)	New State
AlarmForward = Failed	NetView OpenView	5	Major
Proxy Agent does not exist or does not respond	NetView	5	Unknown
	OpenView	5	Unknown

If the icon is in the **New State** and a subsequent poll finds an acceptable response, the icon returns to the **Normal State**.

Trap Events

Traps identify incorrect community string settings. You can configure the Proxy Agent to identify incorrect community strings settings. For more details, refer to *Chapter 5, Network Managers Administration* in your *Proxy Agent User Guide*.

If you configure the Proxy Agent to recognize incorrect community strings, the Proxy Agent sends an Authentication Failure trap to the NMS when an incorrect community string appears.

When the NMS receives an Authentication Failure trap, the NMS changes the icon state of the Proxy Agent icon to User1 in NetView and to Warning in OpenView:

Procedure: Clear a Trap

To clear a trap, complete the following steps:

Procedure 12. Clear a trap

Step	Action
1	Select the Proxy Agent icon.
2	At the menu bar, select one of the following: • NetView: Click **Monitor > DEFINITY > Clear Warning** • OpenView: Click **Fault > DEFINITY > Clear Warning** ***Result:*** The system clears the trap.

Managed Node Icon States

Managed node alarms occur when unacceptable conditions occur on a managed node. Because alarms manifest as color-coded icons, the following section refers to alarm states as icon states.

The state of a managed node icon represents the current alarm state for that managed node. The NMS platform assigns the names of these states.

The table below describes managed node icon states that occur in NetView and in OpenView

Table 9. Managed node icon alarm states

NetView State Name	OpenView State Name	Definition
Normal	Normal	The managed node has no alarms.
User1	Warning	The managed node has at least one warning alarm.
Marginal	Minor	The managed node has at least one minor alarm.

Table 9. Managed node icon alarm states

NetView State Name	OpenView State Name	Definition
User2	Major	The managed node has at least one major alarm.
Unknown	Unknown	One of the following conditions is true: • Communication between a Proxy Agent and a managed node is unstable; therefore, the Proxy Agent cannot indicate the status or health of the managed node. • The NMS cannot communicate with the Proxy Agent and, therefore, cannot determine the status of the managed node. • A dynamic connection that has not received a fault status update or a major or minor alarm.

Events that Change Managed Node Icon States

The color of a managed node icon changes when polling events or trap events send alarm information that indicates a change in the managed node alarm states. Below is a description of those polling and trap events.

Polling Events

The NMS polls Proxy Agents on a regular basis. When an unacceptable health condition arises for a managed node with static connections that are in the **up** state, that managed node icon accepts the corresponding icon state.

The table below describes polling events that change managed node icon states.

Table 10. Polling events that change managed node icon states

Result of poll	NMS	New icon state
g3healthMajor > 0	NetView	User2
	OpenView	Major
• g3healthMinor > 0, and • g3healthMajor = 0	NetView	Marginal
	OpenView	Minor
• g3healthWarning > 0, and • g3healthMajor = 0, and • g3healthMinor = 0	NetView	User1
	OpenView	Warning
		1 of 2

Table 10. Polling events that change managed node icon states

Result of poll	NMS	New icon state
• g3healthMajor = 0, and • g3healthMinor = 0, and • g3Warning = 0	NetView OpenView	Normal
Proxy Agent does not exist or does not respond	NetView OpenView	Unknown
Connection status is not **up**	NetView OpenView	Unknown
		2 of 2

Trap Events

When the NMS receives a trap with an alarm state that is more severe than the current alarm state on a managed node, the NMS updates the managed node state.

For example, when the NMS receives a minor alarm trap for a managed node with a warning that managed node icon state changes.

The table below shows the changes that occur when the NMS receives a minor alarm trap.

Table 11. Altered icon states from minor alarm traps

NMS	Current icon state	Changed icon state
NetView	User1	Changes to Marginal
	User2	Remains User1
OpenView	Warning	Changes to Minor
	Major	Remains Major

Set Up Alarm Notification

The Fault Management installation process allows you to install a script that forwards alarm information to a pager or to email. You can also install add-on software such as TelAlert or Remedy that provide additional methods for notifying you when alarms occur.

The following methods for receiving alarm notification are available to you through the NMS:

Table 12. NMS Alarm Notification Methods

Software	Notification Type	Description
Fault Management	CU Pager	Pages the system administrator and sends a code that identifies the alarm or error type.
Fault Management	email	Sends an email message to the system administrator that contains pertinent alarm or error information.
TelAlert	Alpha Page	Pages the system administrator and sends a code that identifies the alarm or error type. The alpha page also confirms when the system administrator received the page. The page repeats until the system administrator responds to the page.
		1 of 2

Table 12. NMS Alarm Notification Methods

Software	Notification Type	Description
TelAlert	Voice Page	Provides a voice page to the system administrator and sends a code that identifies the alarm or error type. The voice page also confirms that the system administrator received the page. The page repeats until the system administrator responds to the page.
TelAlert	Audix	Calls the system administrator's audix and leaves a voice message containing alarm or error information.
Remedy	Ticket	Provides alarm or error historical information for the system administrator.
		2 of 2

Set up Alert Notification

To set up alert notification, identify the notification method that meets your business needs, then complete the following procedure.

The files contained in the following procedure are samples and, therefore, requires that you to edit them before they will function properly.

Procedure 13. Set up Alert Notification

Step	Action
1	At a UNIX prompt, type: **cd /opt/OV/OneVision/bin/Samples** ***Result:*** The system changes to this directory and displays a list of files contained in that directory.
2	Copy one of the following script files to: **/opt/OV/OneVision/bin/DEFINITY_ARS**: • TA_AlphaPage • TA_VoicePage • TA_Audix • CU_Pager • Notify_Email • ARS_Ticket ***Result:*** The system displays procedures for the selected script.
	1 of 2

Procedure 13. Set up Alert Notification

Step	Action
3	Edit the DEFINITY_ARS script.
4	Write and quit the file.
	2 of 2

4 Legacy Equipment

Chapter Contents

Introduction

You can monitor alarms and errors for legacy equipment at the Network Management System (NMS) level. Since legacy equipment does not connect to Proxy Agents, you must install the **auto-disc** patch to Trouble Trackers. This patch provides Auto-Discovery capabilities for legacy equipment.

You ***cannot*** access the Fault Management application for legacy equipment.

To access alarm and error information for legacy equipment you can telnet to a Trouble Tracker associated to a managed node. From the Trouble Tracker, you can access detailed alarm and error information.

This chapter contains the following:

- List of supported legacy equipment
- NMS capabilities for legacy equipment
- Procedures to set up legacy equipment
- Procedures to telnet to Trouble Trackers

Prerequisite

To complete the procedures in this chapter, you must have access to Trouble Tracker documentation.

Supported legacy equipment

The legacy equipment that you can monitor includes early releases of DEFINITY systems as well as AUDIX systems. Supported legacy equipment includes:

- AUDIX
- DEFINITY G1
- DEFINITY G2
- DIMENSION
- System 75
- System 85
- Monitor 1
- Trouble Tracker

When you install Fault Management, you have the option to connect to Trouble Trackers; however, you can connect to a trouble tracker at any time.

Legacy NMS Capabilities

The trouble tracker integrates with the NMS to allow you to view legacy equipment in a similar manner as you would monitor more current DEFINITY equipment.

The sections below describe the NMS capabilities for legacy equipment

Alarm states for legacy icons

When a legacy managed node generates an alarm, the NMS color-codes the corresponding icon to indicate the severity of the alarm. When a legacy managed node has multiple alarms with more than one level of severity, the icon color represents the most severe alarm.

For more information, see *"Identify Icons with Alarms" on page 76*.

Alarm notification

If you set up the alarm notification feature for Fault Management the when you installed the application, you will receive pages or emails when alarms occur. You can also install two types of add-on software: TelAlert or Remedy. These add-on software packages provide alternate methods for notifying you when alarms occur.

For more information, see *"Set Up Alarm Notification" on page 85*.

Legacy submaps

The legacy submap provides point-to-point connections that allow you to monitor legacy equipment as well as G4 and more recent DEFINITY systems. You may populate legacy submaps with more current releases of DEFINITY equipment that connects to Proxy Agents.

For more information, see *"Select Network Submap" on page 44*.

Legacy connections

The NMS does not provide connection status information for legacy equipment.

You can administer up to 150 legacy managed nodes with dynamic connections; however, you may only view 30 connections at one time.

Set Up Legacy Equipment

To set up Auto-Discovery capabilities for Legacy equipment i, complete the following procedure.

Auto-Discovery File Location

The Auto-Discovery patch file resides in one of the following locations:

- OpenView: **/opt/OV/OneVision/bin/TTautodisc**
- NetView: **/usr/OV/OneVision/bin/TTautodisc**

Procedure 14. Set Up Legacy Equipment

Step	Action
1	Use **ftp** or **rcp** to copy the **TTautodisc** file to the **$TTASDIR** on the Trouble Tracker
2	Log in to the Trouble Tracker as the **ttas** user. (Refer to Trouble Tracker documentation.) ***Result:*** The system displays the Trouble Tracker Main Menu.
3	To access a UNIX shell, type**: !sh** ***Result:*** The system displays a UNIX shell prompt. At the prompt, type **./TTautodisc -i** Then, press **ENTER** ***Result:*** The system displays a password prompt.

Procedure 14. Set Up Legacy Equipment

Step	Action
4	Type: [**root password**] Press **ENTER** ***Result:*** The system displays the following message: `Execute the tool one time to initialize all NMS maps, and to ensure that the Trouble Tracker Auto-Discovery tool is set up properly.` Then, the system displays a prompt.
5	Type **./TTautodisc** Then, press **ENTER** ***Result:*** The system displays a prompt. If an error displays, resolve the error before continuing.
6	At the prompt, type: **exit** ***Result:*** The system displays the main Trouble Tracker menu. Legacy equipment is setup. **CAUTION:** If the system maintenance time or backup time for the Trouble Tracker is scheduled for midnight, we recommend that you modify the maintenance or backup time in the crontab file. To change this time, proceed to step 7.

Procedure 14. Set Up Legacy Equipment

Step	Action
7	From the *ttas login trouble tracker menu*, escape to the unix shell using the **! sh** command. (Refer to your Trouble Tracker documentation.) ***Result:*** The system displays a prompt.
8	At the prompt, type **crontab -l > /tmp/ct** Then, press **ENTER** ***Result:*** The system displays a prompt.
9	At the next prompt, type **vi /tmp/ct** Then, press **ENTER** ***Result:*** The system displays the time for system maintenance or backup on the TTautodisc line. The first two numbers indicate the time in military form. For example, 30 19 indicates 7:30 p.m.
10	Type a new maintenance of backup time on the **TTautodisc** line. Then, press **ENTER** ***Result:*** The system displays a prompt.

Procedure 14. Set Up Legacy Equipment

Step	Action
11	To re-register the new crontab file with cron: • Type: **crontab < /tmp/ct** • Then, press **ENTER** ***Result:*** The system displays a prompt. • Type: **crontab -l** • Then, press **ENTER** ***Result:*** The system updates the contents of the cron file.
	4 of 4

Modify Legacy Submaps

You can modify Legacy submaps in the Location Override file. In the *Location Override* file, you can complete the following actions for Legacy equipment:

- Change locations
- Hide a managed node

To make these changes, use a UNIX editor to access the *Location Override* file, then follow the directions contained in the file.

To access the *Location Override* file go to one of the following locations.

- NetView: **/usr/OV/OneVision/DG3Poll/Location**
- OpenView: **/opt/OV/OneVision/DG3Poll/Location**

Access the Trouble Tracker

The trouble tracker allows you to view detailed information about alarms and errors. If you want detailed information about an alarm, you can telnet to the trouble tracker using the following procedure:

Procedure 15. Telnet to the Trouble Tracker

Step	Action
1	Go to a Legacy submap.
2	Double-click any Legacy icon. ***Result:*** The system displays a telnet screen.
3	At the login prompt, type your Trouble Tracker [**login ID**] Then, press **ENTER** ***Result:*** The system displays a password prompt.
4	At the prompt, type your Trouble Tracker [**password**] Then, press **ENTER** ***Result:*** The Trouble Tracker displays the main menu.
5	Refer to your Trouble Tracker documentation for procedures to view alarm and error information.

5 Fault Management Overview

Chapter Contents

Introduction

Fault Management is a graphical tool that allows you to monitor DEFINITY equipment at a specific, component level. With Fault Management, you can view the configuration of managed nodes and any external device associated with a managed node.

You can also view related alarm and error information, or generate reports related to this equipment.

Fault Management refreshes data for managed nodes using Simple Network Management Protocol (SNMP) to provide up-to-date information about DEFINITY equipment.

This chapter contains more details about the following:

- Fault Management capabilities
- Fault Management command procedures
- Procedure to access Fault Management.
- Procedure to exit from Fault Management

Fault Management Capabilities

Fault Management allows you to monitor managed nodes for configuration and fault information. This section contains an overview of each Fault Management capability.

Customize Fault Management

Fault Management allows you to assign custom settings for colors used to designate alarm severity and to highlight items for on-screen reports. In addition, you can assign custom values for refresh and polling intervals.

Chapter 6, "Custom Settings for Fault Management" contains procedures that are required to setup custom color settings and interval settings for Fault Management.

Refresh Managed Node Data

Fault Management provides the capability to refresh data for managed nodes either manually or automatically.

Chapter 7, "Data Refreshes" describes the refresh process and contains procedures that are required for manual refreshes.

View DEFNITY System Components

Fault Management displays configuration information for DEFINITY systems in a graphical format. The information is organized as follows: The first configuration information screen that you can view includes all the equipment contained on a managed node. From that screen, you click a graphical depiction of a system component to view details for that component.

You can continue to view more specific component details until you access the Port Information screen.

System Organization for Managed Nodes

The following table describes the organization for DEFINITY equipment in Fault Management.

Table 13. Access DEFINITY Component screens

Layer	Data Included
Switch	The switch view displays all DEFINITY cabinets and external devices associated with a selected DEFINITY. From the Switch View screen, you can view alarms and errors for all cabinets and external devices displayed.
Cabinet	The cabinet view displays a graphical depiction of a DEFINITY cabinet. When you click on a cabinet on the Switch view, a detailed view of the cabinet displays. From the Cabinet view screen, you can view alarms and errors for that cabinet.
Circuit Pack	The circuit pack view displays detailed data about a selected circuit pack. When you click on a circuit pack on the Cabinet View screen, detailed information for that circuit pack displays. From the Circuit Pack Information View screen, you can view mismatches for that circuit pack.
	1 of 2

Table 13. Access DEFINITY Component screens

Layer	Data Included
Port	The port view displays detailed data about a selected port. When you click on a port on the Circuit Pack view, detailed information for that port displays. Form the Port Information screen, you can view alarms and errors for that port.
External Devices	The external devices view displays detailed data about a selected external device. When you click on an external device icon on the Switch View screen, the External Devices screen displays. From the External Devices screen, you can access individual external devices. External devices include any equipment that uses contact closures, such as air conditioning.
	2 of 2

Chapter 8, "System Component Views" contains detailed information regarding configuration for managed nodes.

View Fault Conditions

Fault Management utilizes two methods for viewing alarms and errors information. First, each component view contains an Alarms Display graphic that identifies the number and category of alarms on that view.

Secondly, Fault Management highlights the graphical depiction of the system component with the highest level of alarm.

In addition, you can view specific alarm and error information by generating standard alarm or error reports at each component view. On these tabular reports, you can click on an item contained in the report and details specific to that item.

Chapter 9, "Fault Conditions" contains detailed information regarding available alarm and error information for managed nodes.

Generate Reports

Fault Management allows you to generate standard and custom reports.

You can generate standard reports at any component view. Standard reports provide configuration or fault information for active component view screens.

You can generate custom reports from the Report Builder feature in Fault Management. Information contained in custom reports comes from data contained in standard reports.

Once you generate these reports, you can output standard and custom reports in one of four modes:

- Output to a screen
- Highlight Objects
- Output to a printer
- Output to a file

Chapter 10, "Reports" contains procedures to create standard reports and custom reports for Fault Management. This chapter also contains procedures to generate report output.

Trouble-shooting

Chapter 11, "Troubleshooting" contains troubleshooting information specific to the Fault Management application.

Fault Management Access Procedure

We recommend that you start Fault Management after you complete the installation process to verify that the installation was successful. This section contains procedures to access and exit from Fault Management and describes the events that occur when you start the Fault Management application.

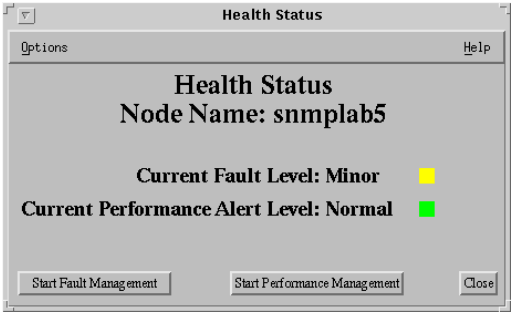
Access Fault Management

The procedure below describes how to exit from Fault Management on the Startup Screen or the Switch View.

Procedure 16. Access Fault Management

Step	Action
1	Log in to UNIX.
2	At a UNIX prompt, type one of the following: • NetView: **$OV_BIN/nv6000** • OpenView: **$OV_BIN/ovw&** ***Result:*** The system opens the Network Management System session and displays the Root map.

Procedure 16. Access Fault Management

Step	Action
3	Double-click a DEFINITY submap icon. ***Result:*** The system displays a DEFINITY submap.
4	Double-click a managed node icon. • If you installed Fault Management ***and*** Performance Management, the system displays the following screen.  • If the system displays this screen, click the **START FAULT MANAGEMENT** button. ***Result:*** The system displays splash screen and starts the Fault Management application.

Data Refresh at Startup

When you access Fault Management, you initiate a data refresh that updates system configuration and fault information. If this is your first session in Fault Management for the day, and Fault Management does not receive data from the Proxy Agent, Fault Management cannot display any cabinet, alarm, or error information.

Fault Management attempts to refresh the data in a predetermined amount of time. You can alter the amount of time Fault Management requests data before timing out.

To change this value, you must change the number of retries in the *Number Retries on SNMP Timeout* field on the Setup screen. For steps to change this value, see *Chapter 6, "Custom Settings for Fault Management"*.

If Fault Management cannot retrieve all the data in the allotted time, Fault Management does the following:

- Displays a message in the message area of the Switch View window
- Stops trying to retrieve data
- Starts with the existing cached data, from prior Fault Management sessions

Startup Messages

Startup messages display when you start Fault Management. For a complete listing of possible startup messages, see *Chapter 7, "Data Refreshes"*.

Startup messages do *not* display if the *Refresh Proxy Agent On Startup* field on the Setup screen is set to **FALSE**. To check this field, go to the Switch View in Fault Management and select **Options > Setup** from the menu bar.

Fault Management Exit Procedure

Once you successfully complete the Fault Management startup, you will need to exit from the program.

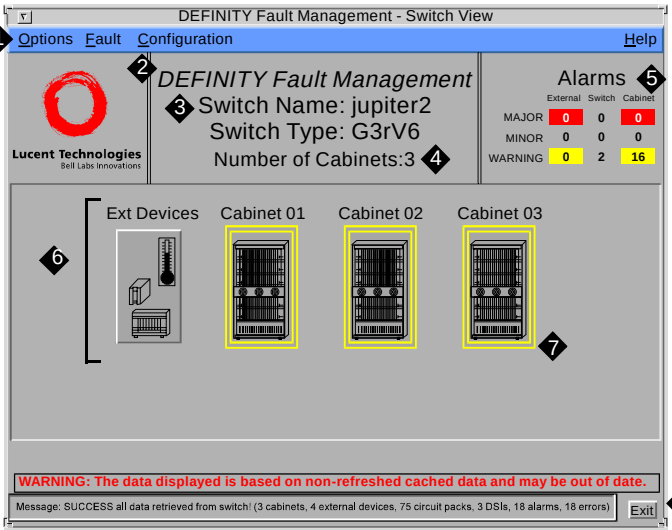
Follow the procedures below To exit the Fault Management application.

Procedure 17.

Step	Action
1	Access either the *Startup Splash* screen or the *Switch View* screen.
2	Click the **EXIT** button. ***Result:*** The system closes the Fault Management application and any associated open windows.

Fault Management Command Procedures

Each component view in Fault Management contains similar working elements. This section identifies screen elements contained in one or all component views.



1 Menu bar
2 Application Name
3 Component Name
4 Number associated with component
5 Alarms Display
6 Data Areas
7 Icon Labels
8 Buttons

Figure 15. Screen Elements

Menu Bar

The menu bar in Fault Management allows you to execute save, close, and exit. The menu bar also allows you to access the Setup screen and generate reports.

The table below contains descriptions of menu selections available in Fault Management.

Table 14. Standard menu bar selections

Field	Description
Options	Displays the following application commands: • Setup — allows you to modify certain fault settings. • Report Builder — allows you to create custom reports. • Clear Highlighting — clears highlighted screen items. • Exit — closes Fault Management.
Fault	Lists the current errors and alarms reports.
Configuration	Contains configuration information for the selected managed node. This menu is available only on the following screens: • Switch View • Cabinet View • External Devices
Help	Contains help information for the active window.

Application Name

Each screen displays the Fault Management application name.

Component Name Each screen identifies the name of the component that displays.

Component Number Each screen contains a number that identifies the number of components a type of component.

Buttons Each screen contains one of two buttons**: CLOSE** or **EXIT**. When you click the **CLOSE** button, the system closes the current view and all subwindows associated to that view.

When you click the **EXIT** button, the Fault Management application closes. The **EXIT** button appears on the Startup and Switch View screens.

Color Display Each screen utilizes colors to identify system components or alarms on a particular component.

Alarms Display

Each view in Fault Management contains a color-coded alarm box that shows the cumulative total of active alarms related to that screen.

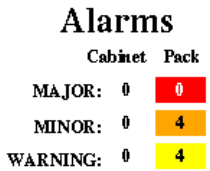


Figure 16. Alarms Display

Data Areas

Each component view contains descriptions specific to that component view. The field descriptions for fault management refer to these data areas.

Icon Labels

Three Fault Management views contain icons that represent switch components: the Switch View, the Cabinet View, and the External Devices View. Colored borders or highlighting colors may surround the labels for these icons to identify circuit pack mismatches or to identify components included in a report. The table below contains descriptions and examples of component icon labels.

Table 15. Components of the icon label

Component	Description	Example
Name	Identifies the external device or cabinet	
Background color *Specific to the Switch View*	Identifies cabinets that have a circuit pack mismatch. In this case the background color is blue. If the cabinet does not contain any circuit packs mismatches, the background color does not display. You can set the background color in the *Circuit Pack Mismatch Color* field on the *Setup screen*.	
Highlight border	Identifies external devices, cabinets, or circuit packs that Fault Management includes in a report. This border displays when you select a ***highlight*** report from the Configuration or Fault menu. You can set the color for this border in the Highlight Color field on the Setup screen.	

Hotspots

Each screen, except the Port Information View utilizes hotspots to navigate to another screen. Hotspots work as follows:

When you launch Fault Management, the Switch View displays. Once you enter the switch view, you can access cabinet views, circuit pack views, or port views by clicking on a portion of the screen designated as a hotspot. For example, if you click on a cabinet at the Switch View, a cabinet screen displays. If you click on a circuit board at the Cabinet View, a detailed description of the circuit board you clicked appears.

Example: Hotspot

The example below illustrates Fault Management hotspots.

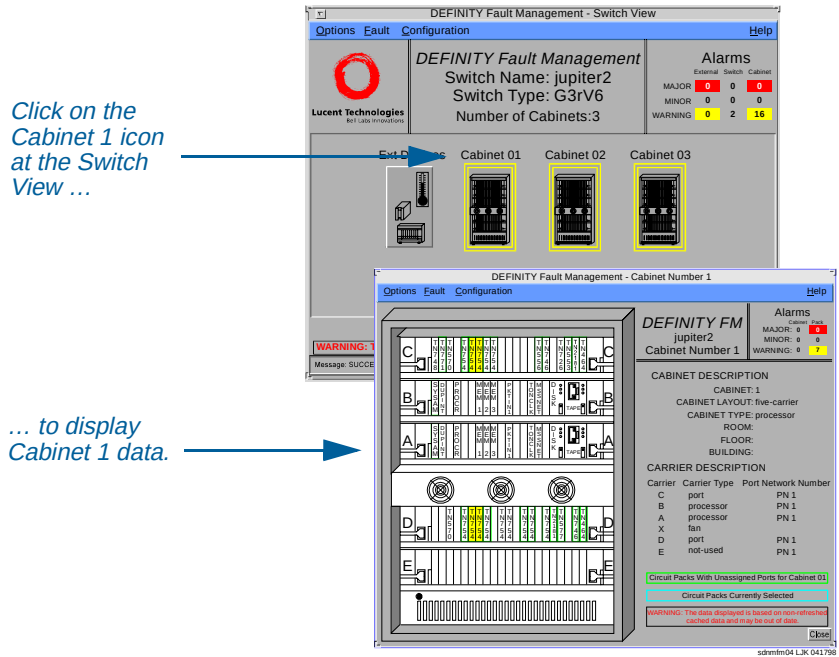


Figure 17. Fault Management hotspots

The following table identifies hotspots that are available at each component view.

Table 16. Fault Management hotspots

Screen	Hotspot	Result
Switch	Cabinet icon	Cabinet
	External devices icon	External Devices
Cabinet	Circuit pack icon	Circuit pack
Circuit pack	Port number	Port
External Devices	External device icon	Individual External Device

Scroll Bars

Fault Management uses standard scroll bars. Scroll bars display when the window cannot display all available information. If no scroll bar displays, you can view all available information on the current screen.

Accelerator Keys

Accelerator keys allow you to use the keyboard to execute a menu command. To use accelerator keys, press the Meta key and select the underlined letter on the menu bar to execute the command.

For example, you would press the Meta key and an F to select File.

Below are steps to use accelerator keys.

Procedure 18. Use accelerator keys

Step	Action
1	For top level menus, simultaneously press the Meta key and the underlined letter of the menu option. ***Result:*** The system displays a submenu.
2	To select an item at a submenu, press the underlined letter of the menu item. ***Result:*** The system executes the command that you selected.

Data Requests

You can request data from Fault Management by using the methods below:

- Keyboard entry
- Pull-down lists
- Check boxes
- Radio Buttons

Keyboard Entry You use the keyboard to type data into fields. You can copy typed entries from one screen or report and paste it into a field on another screen.

Pull-down Lists Many fields have pull-down lists that allow you to select the valid values for that field.

Figure 18. Pull-down list

Check Boxes

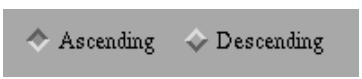
Check boxes allow you to turn-on or to turn-off an option. You can turn on as many check boxes as you want. A depressed box indicates that an option is turned on. A recessed box indicates that an option is turned off.

All of these check boxes are turned off.

Figure 19. Check boxes

Radio Buttons

Radio buttons allow you to select one option from a list of options. A depressed button indicates that an option is turned on. A recessed button indicates that an option is turned off.



The Ascending radio button is turned on.

Figure 20. Radio buttons

6 Custom Settings for Fault Management

Chapter Contents

Introduction

The Setup screen in Fault Management allows you to apply system-wide custom settings. These custom settings replace the default settings that Fault Management assigned during the installation process.

Default Settings

You can modify the following system settings:

- Color settings for alarms, circuit pack mismatches, and graphical depictions of system components
- Time intervals for receiving data from the Proxy Agent
- Startup and retry indicators
- The field delimiter for ASCII reports

Review the Setup Screen

The Setup screen contains fields for system settings that you can modify:

- Apply changes to a current setting
- Save settings permanently
- Revert to default settings
- Switch from color to grey scale
- Close the Setup screen
- Get help

Example: Setup Screen Below is a sample of a Setup screen.

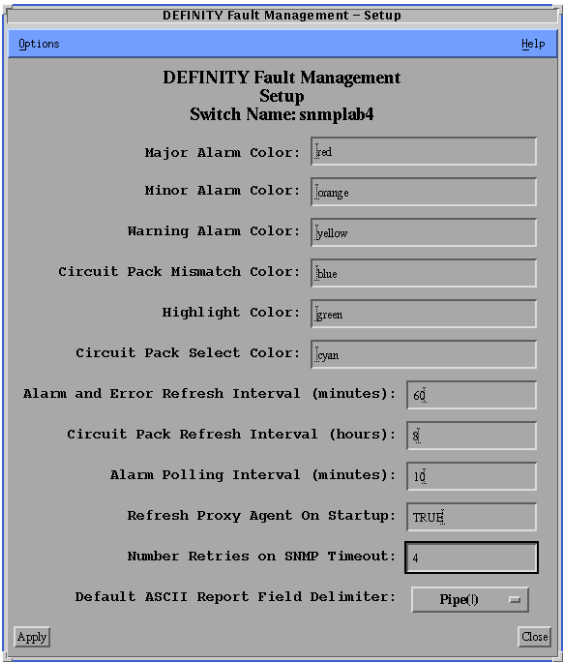


Figure 21. Setup screen

Field Descriptions

The table below contains field descriptions, default values, and valid values for the Setup screen.

Table 17. Setup screen field descriptions

Field	Description
Major Alarm Color	Sets the color used to indicate major alarms. Default: **Red** Valid Values: Any available color on your system. For a complete list, go to: **/usr/lib/X11/rgb.txt**
Minor Alarm Color	Sets the color used to indicate minor alarms. Default: **Orange** Valid Values: Any available color on your system. For a complete list, go to: **/usr/lib/X11/rgb.txt**
Warning Alarm Color	Sets the color used to indicate warning alarms. Default: **Yellow** Valid Values: Any available color on your system. For a complete list, go to: **/usr/lib/X11l/rgb.txt**
	1 of 4

Table 17. Setup screen field descriptions

Field	Description
Circuit Pack Mismatch Color	Sets the color used to highlight cabinet labels and circuit pack labels when circuit pack type conflicts arise. Default: **Blue** Valid Values: Any available color on your system. For a complete list, go to: **/usr/lib/X11l/rgb.txt**
Highlight Color	Sets the color used to highlight cabinets, circuit packs or external devices for highlight reports. Default: **Green** Valid Values: Any available color on your system. For a complete list, go to: **/usr/lib/X11/rgb.txt**
Circuit Pack Select Color	Sets the color used to indicate a selected circuit pack. Default: **Cyan** Valid Values: Any available color on your system. For a complete list, go to: **/usr/lib/X11l/rgb.txt**
	2 of 4

Table 17. Setup screen field descriptions

Field	Description
Alarm and Error Refresh Interval	The time interval in minutes for refreshing alarm and error data. Default: **60** minutes for static connections; unavailable for dynamic connections Valid Values: 5 to 1500 minutes. 0 disables the refresh.
Circuit Pack Refresh Interval	The time interval in hours for refreshing alarm and error data. Default: **8** hours for static connections; unavailable for dynamic connections Valid Values: 1 go 1000 hours; 0 disables the refresh.
Alarm Polling Interval	The time interval for polling the Proxy Agent for alarm updates. Default: **10** minutes for static connections; unavailable for dynamic connections Valid Values: 1 to 60 minutes; 0 disables the polling.
Refresh Proxy Agent On Startup	The value that designates if you want a refresh when you start Fault Management. Default: **TRUE** Valid Values: TRUE; FALSE
	3 of 4

Table 17. Setup screen field descriptions

Field	Description
Number Retries on SNMP Time-out	The number of times Fault Management attempts to retrieve refresh data from Proxy Agents during Fault Management startup. Default: **4** Valid Values: 0–10
Default ASCII Report Field Delimiter	The ASCII character used to delimit fields in a printed ASCII report. Default: **Pipe (|)** Valid Values: Comma (,) Pipe (|) Colon (:) Semicolon (;) tab
Apply button	The **APPLY** button accepts settings for a current session.
Close button	The **CLOSE** button closes the Setup screen and all setup screen subwindows.
	4 of 4

Modify the Setup Screen

To modify existing settings, use the following procedure:

Procedure 19. Modify the Setup screen

Step	Action
1	Go to the Switch View.
2	From the menu bar select: **Options > Setup** ***Result:*** The system displays Setup Screen.
3	Complete one of the following: • To revert to default settings, click: **Options > Default.** • To modify a setting, place the cursor in the field you wish to modify. Type a new value in the field. Then, press **ENTER**. ***Result:*** The system either reverts to default settings or accepts new values.
4	To test the entries, do one of the following: • At the lower left portion of the Setup screen, click the **APPLY** button • From the menu bar, click **Options > Apply** ***Result:*** The system accepts changes for the current session.

Procedure 19. Modify the Setup screen

Step	Action
5	To save your changes permanently, click: **Options > Save** ***Result:*** The system accepts changes until you initiate a new session with the Setup screen.
6	To close the Setup screen use one of the following two options: • Click the **CLOSE** button at the lower right hand corner of the screen. • Click **Options > Close** ***Result:*** The system closes the Setup screen.

2 of 2

WARNING:
If you set refresh values to zero, you disable the refresh.

Change to the Grey Scale Setting

If you have a monochrome monitor, the default color indicators display in grey scale.

If you elect to control the screen with grey scale settings rather than color settings, complete the steps contained in the table below.

Procedure 20. Change to the grey scale setting

Step	Action
1	Go to the Setup screen
2	Click: **Options > Grey Scale**.
3	Type the following in each of the color fields that you want to change: **greyxx** where xx = the percentage of grey. The higher this percentage, the ***lighter*** the grey.
4	Click **APPLY** to test all changes.
5	Click **Options > Save** to save all changes for future sessions.
6	Click **Options > Close** to exit from the Setup screen.

7 Data Refreshes

Chapter Contents

Introduction

Fault Management retrieves configuration and fault information during data refreshes. A data refresh is the process Fault Management uses to signal the Proxy Agent to update the data cache for Fault Management. Once the Proxy Agent completes the process of refreshing data from the managed nodes, Fault Management updates alarm and error information as well as configuration information.

Fault Management refreshes the following information during the refresh process:

- Alarm data
- Bulletin board data
- Cabinet data
- Configuration data
- DS1
- Error data
- External devices
- Trunk group
- Vintage data

Locate MIB Data

Refreshed data passes through the management information base (MIB). You can access data contained in the MIB by accessing one of the following directories. To print data located in this directory, use the system print command.

Table 18. MIB location

NMS	Location
NetView Trouble Tracker	**/usr/OV/snmp_mibs/g3mib.asn1** **/usr/OV/snmp_mibs/TTmib.asn1**
OpenView Trouble Tracker	**var/opt/OV/share/snmp_mibs/g3mib.asn1** **var/opt/OV/share/snmp_mibs/TTmib.asn1**

Prepare Dynamic Connections for Refreshes

Dynamic connections must be in an **up** state before data refreshes can occur. If managed nodes have dynamic connections in the **other**, **idle**, or **down** state, you can establish a connection.

Procedure

If you attempt a data refresh for dynamic connections that are in the **other**, **idle**, or **down** state, then the system displays the following message.

```
Would you like to start the connection? y/n
```

To establish a connection for dynamic connections, click **yes**.

Note: If the Proxy Agent does not transfer data to the NMS within 60 minutes, the dynamic connection returns to the **idle** state. As a result, you will not be able to refresh this data. To alter the 60-minute default time period, see *Chapter 4, Managed Nodes Administration* in your *DEFINITY Proxy Agent User Guide*.

Initiate Data Retrieval

When the Proxy Agent transmits data to Fault Management, Fault Management initiates the following processes:

- Updates the color of cabinet borders in the Switch View to indicate the cabinet with the highest severity alarm.
- Populates all open Cabinet Views with retrieved circuit pack information.
- Indicates alarm conditions by highlighting circuit packs that have the highest severity level.
- Adds alarm counts to the alarms box.

System Defaults

Fault Management attempts to refresh the data in a predetermined amount of time. You can alter the amount of time Fault Management requests data before timing out.

To change this value, you must change the number of retries in the *Number Retries on SNMP Timeout* field on the Setup screen. For steps to change this value, see *Chapter 6, "Custom Settings for Fault Management"*.

If Fault Management cannot retrieve all the data in the allotted time, Fault Management does the following:

- Displays a message in the message area of the Switch View window
- Stops trying to retrieve data
- Starts with the existing cached data, from prior Fault Management sessions

Refresh Processes

Fault Management refreshes data using four methods. These refreshes occur either automatically or manually. The four available refreshes are:

- Startup Refresh
- Configuration Data Refresh
- Alarms and Errors Data Refresh
- Bulletin Board Refresh

Startup Refresh Messages

Startup refresh occurs when you start Fault Management. The startup refresh occurs ***only*** if the *Refresh Proxy Agent On Startup* field in the *Setup screen* is set to **TRUE**. The startup refresh updates all data refresh categories.

When you start Fault Management, refresh messages display on the Splash screen. These messages contain the following information:

- The estimated time for the refresh to occur
- The refresh status if the refresh is not successful
- Notification that alerts you when a dynamic connection is not up. This message also allows you to initiate a connection.

Startup Messages

The numbered items below identify and describe refresh messages that display during startup. The corresponding table that follows these items, identifies the system conditions that are present when these messages occur.

1. `Refresh in progress, estimated delay xxx seconds, yyy seconds elapsed.`
   Where xxx is the estimated duration of the refresh in seconds and yyy is the number of seconds that has elapsed.

   If the refresh succeeds, Fault Management starts. If the refresh fails, the following message displays:
   `Refresh on Startup Failed! Continuing with Cached Data.`
2. The Switch View warning label will say
   `WARNING: The data displayed is based on non-refreshed cached data and may be out of date.`
3. If the refresh fails or the Refresh on Startup value is **FALSE**, the following message displays:
   `Bad Cache Data or No Cache Data Available.`
   The Switch View screen becomes fully functional when data becomes available.
4. If the refresh fails, a pop-up box displays with the date, time, switch name and the following message:
   `WARNING: The startup refresh failed. The data displayed is based on the data cached on the Proxy Agent. This data may be out of sync with the actual switch data. The most`

likely cause of this problem is the connection between the Proxy Agent and the DEFINITY PBX being down or turned off.

5 At the same time the Switch View Warning label will say:
WARNING: The data displayed is based on non-refreshed cached data and may be out of date.

6 A pop-up box displays:
Would you like to start the connection? If the answer is yes, the message area displays: Starting Connection, xxx seconds elapsed,
where xxx is the number of seconds that have elapsed. If the connection succeeds, the messages contained in numbers 1 and 4 of this list display. If the connection does not succeed or if you select no, then numbers 2 and 3 display.

7 A pop-up box displays:
Would you like to start the connection? If the answer is **yes**, the message area displays: Starting Connection, xxx seconds elapsed,
where xxx is the number of seconds that have elapsed. If the connection is successful, then the messages in 1 and 4 of this list display. If the connection does not succeed or if you select **no**, then the messages in 2 and 4 display.

The table below identifies the conditions that are present when startup messages appear on the screen. The numbers in the **Results** column correspond to the numbered text above.

Table 19. Startup refresh messages

Results	Connection Type	Connection Status	Cache	Refresh on Startup
1, 3, 4	static or dynamic	up or init	no	true
2, 3	static or dynamic	up or init	no	false
1, 4	static or dynamic	up or init	yes	true
2	static or dynamic	up or init	yes	false
1, 3, 4	static	off, down, or other	no	true
2, 3	static	off, down, or other	no	false
1, 4	static	off, down, or other	yes	true
2	static	off, down, or other	yes	false
2, 3	dynamic	off	no	true
2, 3	dynamic	off	no	false
2, 4	dynamic	off	yes	rule
2	dynamic	off	yes	false
				1 of 2

Table 19. Startup refresh messages

Results	Connection Type	Connection Status	Cache	Refresh on Startup
5	dynamic	idle, down, or other	no	true
2, 3	dynamic	idle, down, or other	no	false
				2 of 2

Configuration Data Refresh Procedures

The Configuration data refresh updates all circuit pack information, including circuit pack types, circuit pack locations, and port information. During a configuration data refresh, Fault Management closes all open Cabinet View and External Devices screens and their child windows.

The following information describes automatic and manual refreshes for configuration data.

Automatic Refresh

If you specified a refresh time in the *Circuit Pack Refresh Interval* field on the *Setup screen*, the system automatically performs a configuration data refresh when the refresh timer expires.

Before a scheduled refresh of circuit pack data, Fault Management prompts you for permission to start the refresh. Fault Management responds to your request as follows:

- If you click **OK**, or if you do not respond to the prompt within 20 seconds, Fault Management closes all open windows except the Switch View and updates the circuit pack data.
- If you click **NO**, Fault Management aborts the data refresh.

Manual Refresh

You can manually initiate a configuration data refresh at any time during an active Fault Management session. To refresh configuration data, complete the following steps:

Procedure 21. Manually refresh configuration data

Step	Action
1	Go to the *Switch View*.
2	Click **Configuration > Refresh Configuration Data** ***Result:*** The system completes one of the following: • Refreshes the configuration data. • Displays one of the following two messages: – If the connection status for dynamic connections is **other**, **idle** or **down**, the screen displays the following message: `Would you like to start the connection? y/n` – If the dynamic connection state is **off**, the screen displays the following message: `Connection is off. Refresh not Started.`
3	To complete the refresh for a dynamic connection in the **other**, **idle,** or **down** state, type: **y** Then, press **ENTER** ***Result:*** The system refreshes the configuration data.

Alarms and Errors Data Refresh Procedures

Alarms and errors refreshes update fault information for static connections. Fault Management performs an alarms and errors data refresh under the following conditions:

- When Fault Management receives a trap from the Proxy Agent
- When the alarm and errors refresh interval expires
- When the alarm poll detects a mismatch between the number of alarms on the NMS and the number of alarms on the Proxy Agent
- When a user manually requests a refresh

Traps

When Fault Management receives a trap from the Proxy Agent, it refreshes alarm and error data. A trap can indicate that the managed node generated a new alarm or that all alarms for DEFINITY systems cleared.

Example: Trap Below is an example of a trap messages for an external device. This example shows all fields that display on any trap message.

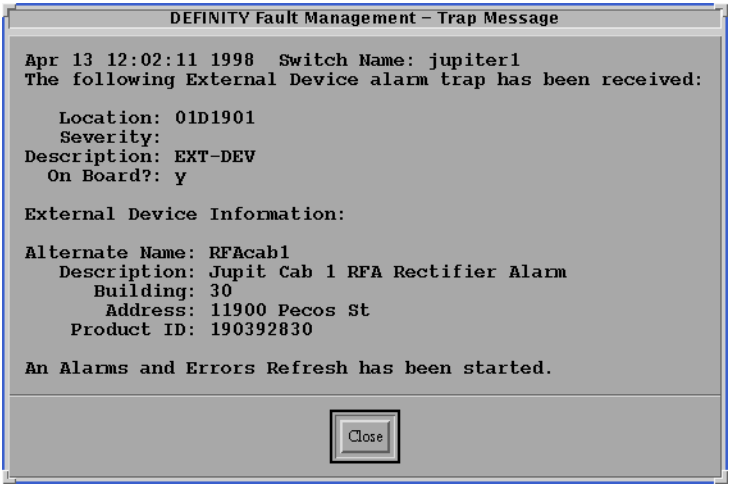


Figure 22. Trap message for an external device

Field Descriptions

The following table provides field descriptions for the sample trap message shown above.

Table 20. Field descriptions for trap messages for an external device

Field	Description
Heading Information	The first line of text, includes the date and time that the Proxy Agent received the trap.
Switch Name	The name of the node on the NMS
Location	The location of the alarm related to the trap.
Severity	One of the following alarm states: • Major • Minor • Warning
Description	The name of the maintenance object for the alarmed external device.
On Board?	The indicator that identifies whether the fault is on the associated circuit pack or on an off-board element connected to the circuit pack. Valid values are: • y = yes • n = no
	1 of 2

Table 20. Field descriptions for trap messages for an external device

Field	Description
External Device Information	A heading that identifies the fields for external devices.
Alternate Name	The name of the external device.
Description	The description of the external device.
Building	The name of the building where the external device resides.
Address	The mailing address for the building.
Product ID	The identification number for the external device.
Trap Message	The trap message indicates that an Alarms and Errors Refresh has started.
	2 of 2

Automatic Refresh

Fault Management also polls the DEFINITY system periodically for alarm and error information. The interval specified in the *Alarm and Error Refresh Interval* field on the Setup screen determines the polling frequency.

When the amount of time specified in this field expires, Fault Management initiates an alarms and errors data refresh. The refresh interval begins again when Fault Management completes the refresh.

In addition, Fault Management regularly polls the Proxy Agent for alarms related to the following Management Information Base objects:

- healthMajor
- healthWarning
- healthMinor

When this polling finds informational mismatches between the Proxy Agent and the NMS, the poll initiates an alarms and errors data refresh. The interval specified in the *Alarm Polling* field on the Setup screen determines this type of polling frequency.

Note: Fault Management updates cabinet information ***only*** during the startup refresh process. If you want to update cabinet information, you must close Fault Management and restart it from the NMS.

Manual Refresh To manually refresh alarm and error data complete the following steps:

Procedure 22. Manually refresh alarm and error data

Step	Action
1	Go to the Switch View
2	Click **Fault > Refresh Fault Data** ***Result:*** The system completes one of the following: • Refreshes the configuration data refreshes. • Displays one of the following messages: – If the connection state for dynamic connections is **other**, **idle** or **down**, the screen displays the following message: `Would you like to start the connection? y/n` – If the dynamic connection state is **off**, the following message displays: `Connection is off. Refresh not Started.`
3	To complete the refresh for a dynamic connection in the **other**, **idle,** or **down** state, type: **y** Then, press **ENTER** ***Result:*** The system refreshes the configuration data.

Bulletin Board Data Refresh Procedures

The Bulletin board refresh allows you to update the messages contained on the Bulletin Board screen. Typically, technicians who are working to resolve errors on a managed nodes post status messages on the Bulletin Board of that managed node. This allow you to monitor the progress of any corrective action.

Exception: MCU Switches

Fault Management allows you to view the contents of the bulletin board for all DEFINITY equipment ***except*** MCUs. The *Refresh Bulletin Board* and *Display Bulletin Board* submenu selections are greyed out for MCUs.

Automatic Refresh

Bulletin Board data refreshes automatically at startup if the *Refresh Proxy Agent on Startup* field on the *Setup screen* is set to **TRUE**.

Manual Refresh

To manually refresh the bulletin board during a Fault Management session, complete the following steps:

Procedure 23. Manually refresh configuration data

Step	Action
1	Go to the *Switch View*.
2	Click **Fault > Bulletin Board**
	Result: The system updates the messages on the bulletin board.

8 System Component Views

Chapter Contents

Introduction

Fault Management uses a graphical user interface (GUI) that allows you to navigate quickly through representations of DEFINITY components. Each view contains specific configuration and fault information for the components identified.

This chapter describes configuration information available at each component view.

Fault Management provides the following views:

- Cabinets included in a switch view
- A specific cabinet on the DEFINITY system
- A circuit pack on the cabinet
- A port on the circuit pack
- An external device on the DEFINITY system

Chapter 9, "Fault Conditions", contains fault information specific to each component view.

Switch View

The Switch View screen contains a graphical depiction of all the cabinets and external devices in your DEFINITY system. At the Switch View screen, you can generate configuration reports and view messages in the message area.

When you click a cabinet icon or an external device icon, a view of the cabinet or external device displays showing hardware status and configuration.

Icons for external devices ***only*** display if an external device is administered on a managed node.

Example: Switch View Screen

At the Switch View screen you will see a screen similar to the example below:

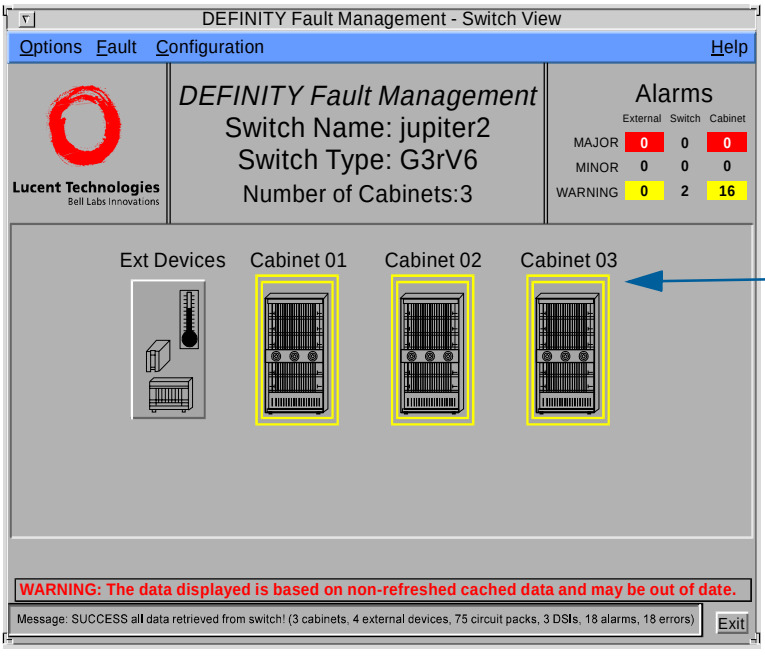


Figure 23. Switch View screen

Field Descriptions: Switch View Screen

The following table describes the fields contained on the example of the Switch View screen shown above.

Table 21. Switch View screen field description

Field	Description
Number of Cabinets	The number of cabinets that Fault Management recognizes. Valid values are: • A number from 1– 44 • Blank, if Fault Management cannot find any cabinets for the DEFINITY system.
Messages	The following types of messages: • Warning messages display when: – Fault Management cannot complete a refresh attempt. – The *Refresh Proxy Agent On Startup* field on the Setup screen is set to **FALSE**. • Status messages occur regularly when Fault Management updates status data and error data.

Configuration Reports: Switch View Screen

You may generate standard switch-related reports from the Configuration menu on the Switch View screen. The table below lists the standard reports available at the Switch View screen.

Table 22. Switch view standard reports

Configuration Menu	Description
Display Hardware/ Software Information	Displays the current release information about the DEFINITY system and Fault Management software.
Circuit Pack Inventory	Displays a summary report for the circuit packs currently installed on the system.
All Circuit Packs	Displays a detailed report for all the circuit packs that are administered or that are physically present.
Exception Circuit Packs	Displays a report for all the circuit packs that are administered on the system but are either mismatches or are not physically present.
DS1 Circuit Packs	Displays a report for all the digital signaling circuit packs that are on the system.
Refresh Configuration Data	Refreshes the information about circuit packs. You can use this command when you change the configuration of the DEFINITY system.

Cabinet View

The Cabinet View screen contains a graphical depiction of cabinets as well as data regarding the cabinet layout, the cabinet type, and the cabinet location.

The left-hand side of the Cabinet View screen displays the following components:

- Associated carriers.
- Slots and their associated slot numbers.
- Circuit pack labels for slots that contain circuit packs. The circuit pack label indicates the type of circuit pack. If the slot is administered but does not contain a circuit pack, the label is NO BRD.
- Blank slots depict slots that do not contain a circuit pack.

The right-hand side of the Cabinet View screen contains cabinet and carrier descriptions.

Procedure From the Cabinet View screen, you can open 23 circuit pack views at a time. When you open a Circuit Pack Information View screen, Fault Management highlights the corresponding circuit pack slot on the Cabinet View screen. To bring a desired circuit pack to the front, click on the corresponding circuit pack on the cabinet view.

Procedure To access a Cabinet View screen click a cabinet icon on the Switch View screen.

Example: Cabinet View Screen

The following example shows a sample of a cabinet view. Each rectangle that represents a circuit board is a hotspot regardless of the current alarm state.

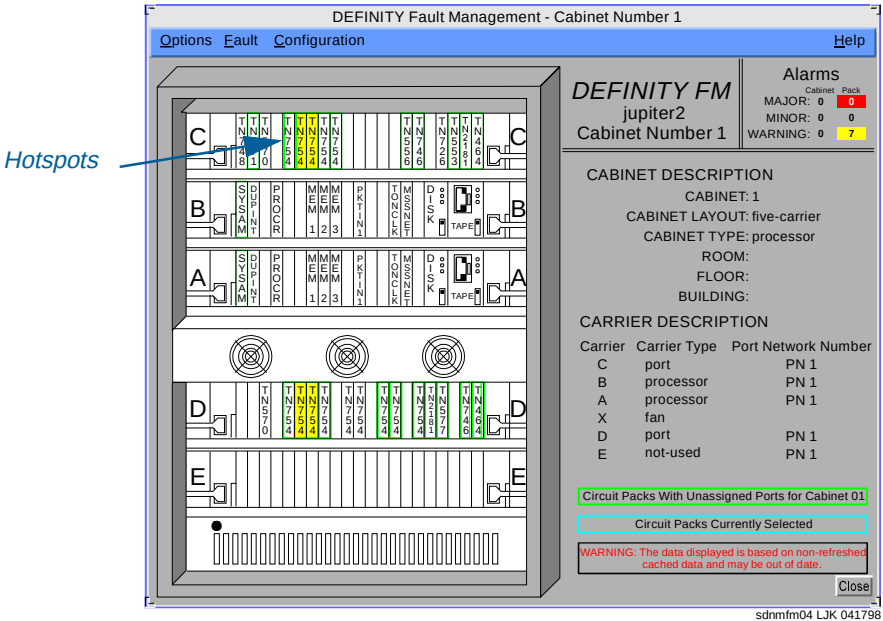


Figure 24. Cabinet View screen

Field Descriptions: Cabinet View Screen

The following table contains field descriptions for the Cabinet View screen.

Table 23. Cabinet View screen field description

Field	Description
CABINET DESCRIPTION	
CABINET	The cabinet number.
CABINET LAYOUT	The type of cabinet layout options include: • five-carrier • single-carrier-stack • enhanced-single-carrier-stack • small • very-small • compact modular cabinet (cmc)
CABINET TYPE	The type of cabinet; options include: • processor • expansion-port-network
ROOM	The room where the cabinet is located (taken from system administration.)
FLOOR	The floor where the cabinet is located (taken from system administration.)
	1 of 2

Table 23. Cabinet View screen field description

Field	Description
BUILDING	The building where the cabinet is located (taken from system administration.)
CARRIER DESCRIPTION	
Carrier	The carrier label.
Carrier Type	The type of carrier: • processor • dup-sw-node • switch-node • port • fan • expansion-control • not-used
Port Network Number	The number of the port network. The valid range is 1–44
	2 of 2

Cabinet Messages

Warning and status messages display above the Cabinet Description area and below the Carrier Description area on the Cabinet View screen.

The table below contains descriptions of messages that display on the Cabinet View screen.

Table 24. Messages on the Cabinet View screen

Message Type	Description
Incomplete Data Warning	**Location**: Displays above the *CABINET DESCRIPTION* information. This warning message displays only if you clicked on a cabinet hotspot on the Switch View screen before Fault Management retrieved all the information about circuit packs. The message disappears once Fault Management completes data retrieval.
Highlight Message	**Location**: Displays below the *CARRIER DESCRIPTION* information. This status message describes the last highlighting selection you made from the Configuration menu.
	1 of 2

Table 24. Messages on the Cabinet View screen

Message Type	Description
Circuit Pack Message	**Location**: Displays below a highlight message This status message reminds you that you selected a circuit pack.
Cached Data Warning	**Location**: Displays below the *CARRIER DESCRIPTION* information. This warning message *only* displays when the data that Fault Management displays is based on non-refreshed, cached data. The following situations can result in this warning: • Fault Management cannot complete a refresh attempt • The *Refresh Proxy Agent On Startup* field on the Setup screen is set to FALSE
	2 of 2

Configuration Reports: Cabinet View Screen

You may generate cabinet-related reports from the configuration menu on the Cabinet View screen. The table below lists the reports available from the Configuration menu and describes the actions that occur when you generate a standard report.

Table 25. Cabinet standard reports

Configuration Menu	Action
Click one of the following: Highlight Circuit Packs with > • Unassigned Ports • No Assigned Ports • No Available Ports • TTI Ports • Type Mismatch • Control Circuit Packs • Major Alarms • Minor Alarms • Warning Alarms	• Opens the appropriate report window. • Highlights the affected circuit packs on the Cabinet View screen. • Displays an informational message in the message area of the Switch and Cabinet views. This message explains the highlighting.

Circuit Pack Information View

The Circuit Pack Information View screen displays a data description of a circuit pack and identifies port connections for that circuit pack. The Circuit Pack Information View screen also identifies circuit pack mismatches.

Procedure

To access the Circuit Pack Information View screen, click on a circuit pack slot on the Cabinet View screen.

Example: Circuit Pack Information View Screen

The example below shows a sample of a Circuit Pack Information screen.

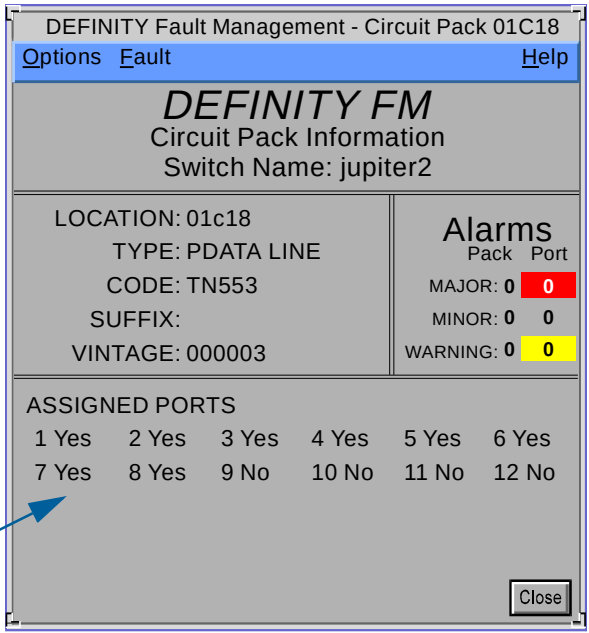


Figure 25. Circuit Pack Information screen

Field Descriptions: Circuit Packs

The following table contains descriptions for configuration data located on the Circuit Pack Information View screen. It also contains a description specific to DS1 circuit packs.

Table 26. Field Descriptions for Circuit Packs

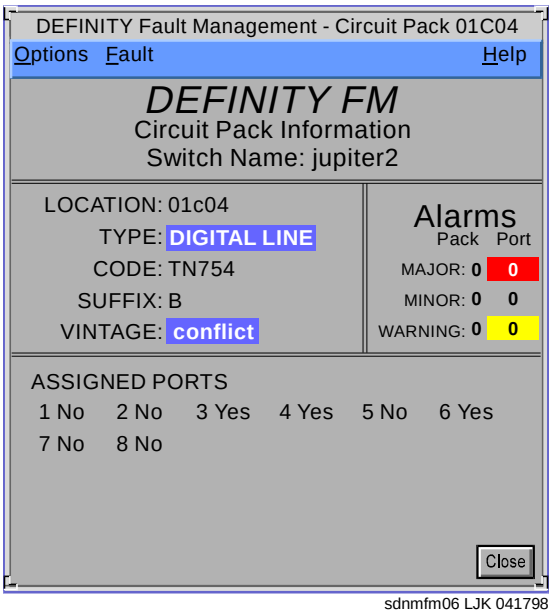
Field	Description
LOCATION	The cabinet, carrier, and slot of a circuit pack.
TYPE	The type of circuit pack. A few examples are: • Analog line • BRI line • Data line • Digital line • DS1 interface
CODE	The product code of the circuit pack.
SUFFIX	A suffix identifies a type of circuit pack.
VINTAGE	One of the following: • The release of the circuit pack. • The highlighted word CONFLICT displays if there is a mismatch between the circuit pack administration and type.
	1 of 2

Table 26. Field Descriptions for Circuit Packs

Field	Description
Assigned Ports	This configuration area lists each port on the circuit pack numbered from 1 to 32. If you use a radio controller board, you can use 0A instead of 1 and can use 0B instead of 2. • Yes = the port is assigned • No = the port is not assigned • TTI = the port is a TTI port
DS1 circuit pack data	
SIGNALING	The method for transmitting data or digital information. Displays only for DS1 circuit packs.
NAME	The DS1 name. Displays only for DS1 circuit packs.
CSU MODULE	The ID for the integrated CSU module. Displays only for DS1 circuit packs.
BIT RATE	The speed of the channels; either 2.048 or 1.544 Mbps. Displays only for DS1 circuit packs. The Default is 2.048.
	2 of 2

Example: Circuit Pack Mismatches

The Circuit Pack Information view does ***not*** contain the option to generate configuration reports. However, when circuit pack mismatches occur, the Circuit Pack Information View screen displays the following screen.



This example shows a circuit pack with mismatched type and vintage.

Note the highlighting on Type and Vintage and the word "conflict."

Figure 26. Circuit Pack Information Screen with a conflict

Port Information View

The Port Information View screen contains data for individual ports. The data that displays varies, depending on the type of equipment that connects to the port. This section contains examples and field descriptions of screens that you can view at the Port Information View screen:

- Pooled Modem
- Data Modules
- Station Information
- Trunk Group Information

Dynamic Connections

The Port Information View screen reflects data for dynamic connections in the **up** state. If the Proxy Agent does not transfer data to the NMS within the 60-minute default time, dynamic connections return to the **idle** state.

To alter the 60-minute default time period, see *Chapter 4, Managed Nodes Administration* in your *DEFINITY Proxy Agent User Guide*.

CAUTION:
If you attempt to access port information for an active Multipoint Conferencing Unit (MCU), you may not receive the data. Retry when the MCU becomes inactive.

Procedure: Access Port View from Dynamic Connection

To access the Port Information View screen from a dynamic connection, complete the following steps:

Procedure 24. Access the Port View from a Dynamic Connection

Step	Action
1	Go to the Circuit Pack Information View screen
2	Click on a port in the *Assigned Ports* data area on the Circuit Pack Information View screen. ***Result:*** The system completes one of the following: • Displays the Port Information View screen. • If the selected port corresponds to a managed node with a dynamic connection in the **other**, **idle**, or **down** state, the screen displays the following message: `Would you like to start the connection? y/n`
3	If the connection is dynamic in the **other**, **idle** or **down** state, type **y** Then, press **ENTER** ***Result:*** The system changes the connection status to **up** and displays the Port Information View screen.

Example: Tone Detector

The following figure shows the first of the available views on the Port Information View screen. Below is a sample of a tone detector. This view contains the fields that appear on all Port Information View screens.

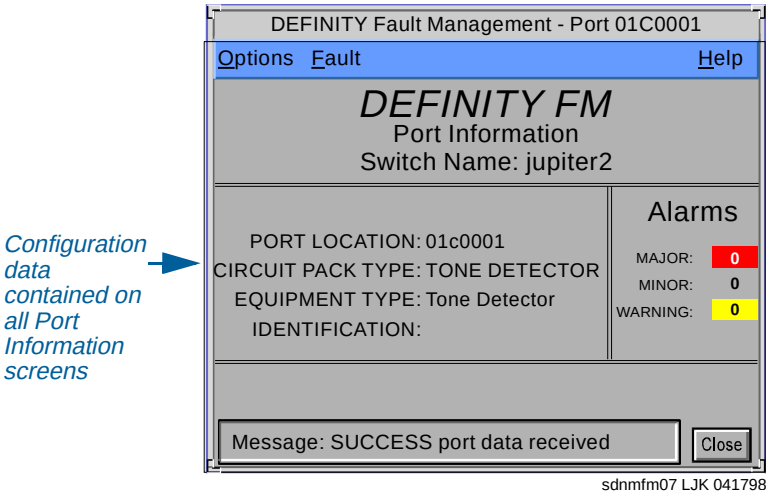


Figure 27. Port Information View screen: Tone Detector

Field Descriptions: Port Information View Screen

The following table describes configuration data fields on the Port Information View screen.

Table 27. Configuration data for the port

Field	Description
PORT LOCATION	The cabinet, carrier, slot, and port for a port. Example: 01C2004 • 01 = Cabinet • C = Carrier • 20 = Slot • 04 = Port
CIRCUIT PACK TYPE	The port is on this type of circuit pack.
EQUIPMENT TYPE	The equipment attached to the port. Example: • Station • Data Module • Integrated Announcement
	1 of 2

Table 27. Configuration data for the port

Field	Description
IDENTIFICATION	The alternate name of the port. Example: • A station extension • The trunk/group member number (Trk Gp /Mbr No)
Message	Status information for data refreshes.
	2 of 2

Example: Data Module

The example below shows a sample of Data Module Port Information view.

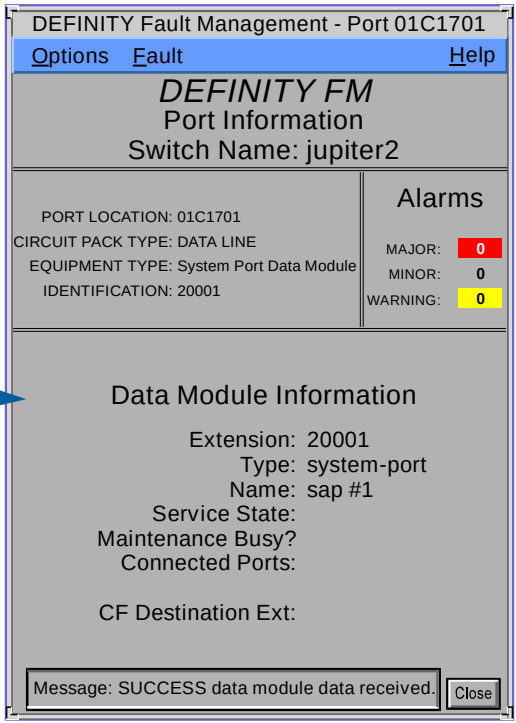


Figure 28. Port Information View screen: Data Module

Field Descriptions: Data Module

The following table describes fields that are specific to data modules.

Table 28. Field descriptions for data modules

Field	Description
Extension	The extension number for the station.
Type	The type of data module.
Name	The data module name, as administered on the DEFINITY system.
Service State	The current service state of the data module.
Maintenance Busy?	The indicator that identifies if the station is busy for maintenance purposes.
Connected Ports	The ports that are connected to the data module.
CF Destination Ext	The extension to which the DEFINITY system forwards calls.
Message	Status information for data refreshes.

Example: Station

The example below shows a sample of Station Port Information.

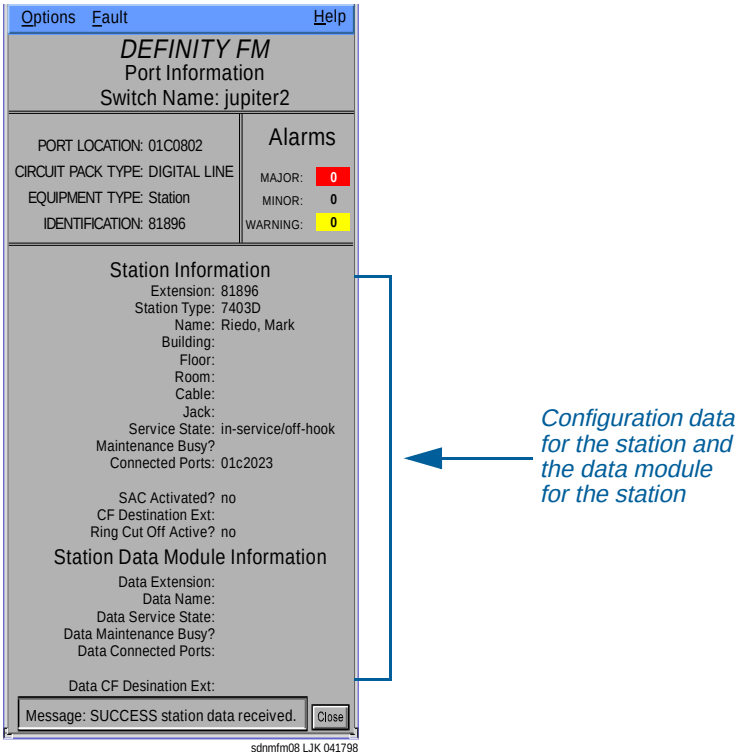


Figure 29. Port Information: Station

Field Descriptions: Station Information

The following table describes configuration data for that is specific to stations.

Table 29. Field descriptions for station information

Field	Description
Station Information	
Extension	The extension number for the station
Station Type	The type of station
Name	The station name as administered on the DEFINITY system.
Building	The building where the station resides as administered on the DEFINITY system.
Floor	The floor where the station resides as administered on the DEFINITY system.
Room	The room where the station resides as administered on the DEFINITY system.
Cable	The identifier of the cable as administered on the DEFINITY system.
Jack	The location of the jack as administered on the DEFINITY system.
Service State	The current service state of the station.
	1 of 3

Table 29. Field descriptions for station information

Field	Description
Maintenance Busy?	Indicates if the station is busy for maintenance purposes.
Connected Ports	Lists any ports that are currently connected to the station.
SAC Activated?	Indicates if the Send All Calls feature is active.
CF Destination Ext	Identifies the extension to which the DEFINITY system forwards calls.
Ring Cut Off Active?	Indicates if the Ring Cut Off feature is active.
Station Data Module Information	
Data Extension	The extension number for the data module
Data Name	The name of the data module as administered on the DEFINITY system.
Data Service State	The current service state of the data module
	2 of 3

Table 29. Field descriptions for station information

Field	Description
Data Maintenance Busy?	Indicates if the data module is busy for maintenance purposes.
Data Connected Ports	Lists any ports that are currently connected to the data module.
Data CF Destination Ext	Identifies the extension to which the DEFINITY system forwards calls.
Message	Status information for data refreshes.
	3 of 3

Example: Trunk Port Information

The example below shows a sample of Trunk Port Information.

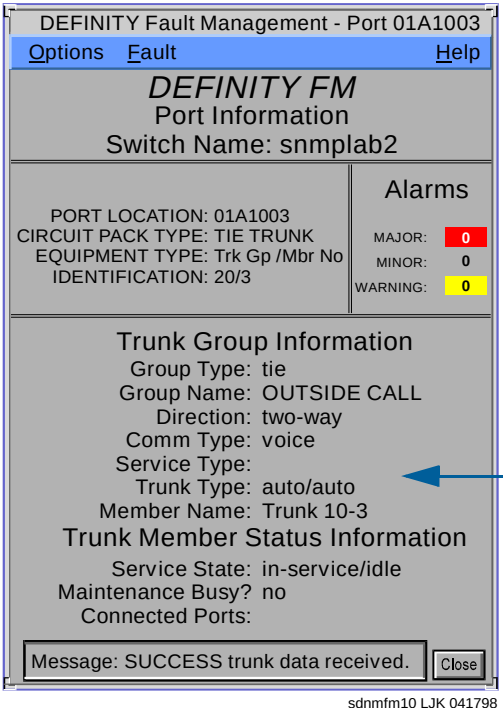


Figure 30. Port Information: Trunk

Field Descriptions: Trunk Port

The table below describes configuration data that is specific to trunk groups and trunk member status.

Table 30. Field descriptions for Trunk Ports

Field	Description
Trunk Group Information	
Group Type	The type of trunk group.
Group Name	The group name, as administered on the DEFINITY system.
Direction	The trunk direction. Example: A 2-way direction has incoming and outgoing calls.
Comm Type	The communications type.
Service Type	The service type.
Trunk Type	The type of trunk. Examples: • Voice • Data • Tie
Member Name	The member name of the trunk, as administered on the DEFINITY system.
	1 of 2

Table 30. Field descriptions for Trunk Ports

Field	Description
Trunk Member Status Information	
Service State	The current service state of the trunk.
Maintenance Busy?	Indicates if the station is busy for maintenance purposes.
Connected Ports	Lists any ports that are currently connected to the trunk.
Message	Status information for data refreshes.
	2 of 2

External Devices

An external device is hardware that you can connect to a managed node. An external device can be any equipment that uses contact closures. For example, you can administer air conditioning or door triggers on a managed node.

The External Devices screen displays icons for all external devices that you administered on a managed node. To display information about the hardware and configuration status for an external device, click an external devices icon on the Switch View screen.

Example: External Devices Screen

The example below is an External Devices screen.

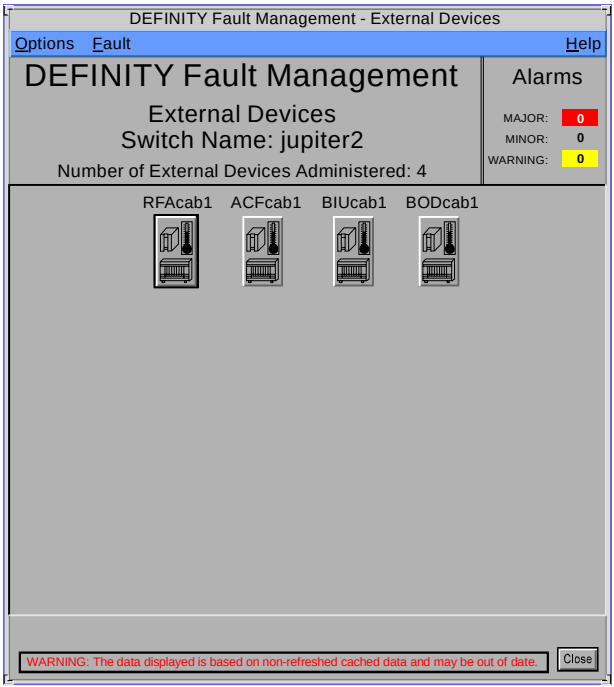


Figure 31. External Devices screen

Field Descriptions: External Devices Screen

The following table contains field descriptions for an external devices screen.

Table 31. External devices field description

Field	Description
Application Name	DEFINITY Fault Management
View Name	The screen name for an External Devices screen.
Switch Name	The name of the managed node as it appears on the NMS.
Number External Devices	The number of external devices administered on a managed node.
Messages	The External Devices screen displays two types of messages: • Highlight Reason. To explain why a label for an external devices icon is highlighted. • Cached Data Warning. Displays when the data that Fault Management displays is based on non-refreshed, cached data.

Individual External Devices

The Individual External Devices screen displays the hardware configuration and the fault status for a specific external device.

Procedure

To access an Individual External Devices screen, click on an external device icon on the External Device View.

Example: Individual External Device Screen

The following figure shows an Individual External Device screen for a voice mail system:

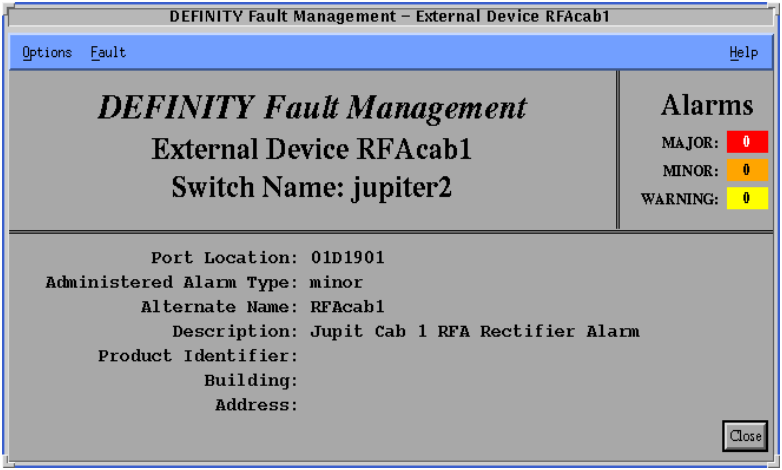


Figure 32. Individual External Device screen

Field Descriptions: Individual External Devices Screen

The following table contains configuration data contained on all Individual External Devices screens.

Table 32. Field Descriptions for the Individual External Device screen

Field	Description
Port Location	The location of the port that the external device uses.
Administered Alarm Type	The type of alarm that the DEFINITY system generates for an active alarm. Valid values are: • Major • Minor • Warning
Alternate Name	The abbreviated name for the external device.
Description	A brief description of the external device.
Product Identifier	The 10-digit product number for the external device.
Building	The building where the external device resides.
Address	The address of the building where the device resides.

9 Fault Conditions

Chapter Contents

Introduction

Fault Management monitors errors and alarms that occur on managed nodes. When a single error or an accumulation of errors occur that may require maintenance, the Proxy Agent generates an alarm and transmits the information to the Network Management System (NMS).

Fault Management translates the alarm information using a graphical user interface (GUI) to display the alarm and error information.

Fault Management provides the following alarm information:

- The location of an unresolved alarm
- The alarm severity: major, minor, or warning.
- The number of alarms in each alarm type.

View Alarm Displays

Fault Management provides two graphical formats for viewing alarms: it highlights the graphical depictions of the affected hardware or it updates the alarms display box.

Warning Display

The example below shows a Switch View that displays warnings for three cabinets.

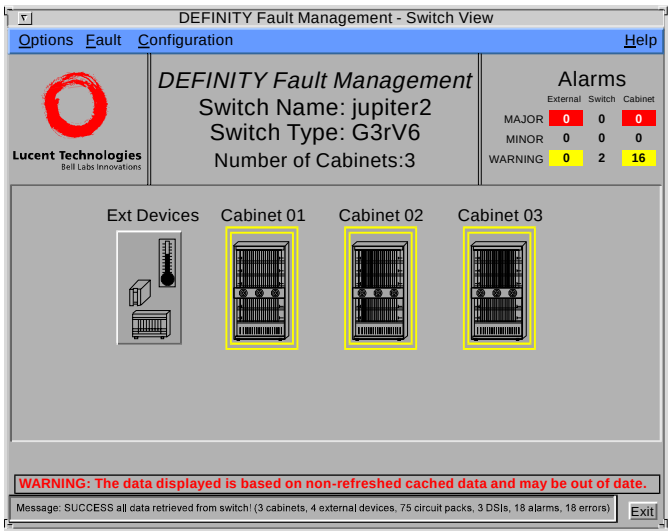


Figure 33. Cabinet with Circuit Pack alarms

Alarms Display Box

The Alarms Display Box shows the cumulative total of active alarms. The alarms display appears on the right side of all component views and shows the number of major alarms, minor alarms, and warnings.

Below is a sample of the alarms display box.

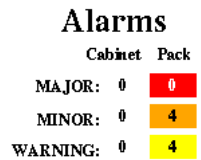


Figure 34. Alarms Display Box

View Errors

Error reports display detailed information about problems that occur on a managed node. An error report corresponds to an active Component View. Error reports identify existing errors and affected ports.

These reports show error data that is current at the time you request the report. Fault Management does ***not*** update data for a report while the report window is open. To ensure that data is current, close and then re-open any open report window.

Error reports display the same information that displays when you execute the **display errors** command, with the following exception:

Exception The standard error report does not include seconds in the *First Occur* field.

Standard Error Reports

The Fault menu, located in each Component View, allows you to select a report that displays errors for the active component view.

The following table identifies error reports that are available at each Component View.

Table 33. Standard error reports

Screen	Fault Menu Command	Report Description
Switch View	All Errors	All errors in the DEFINITY system
	Switch Level Errors	All errors that are in the DEFINITY system but are not associated with any cabinet
Cabinet View	All Errors for Cabinet #	All errors in the cabinet specified
	Cabinet Level Errors for Cabinet #	All active alarms that are in the cabinet but are not associated with any circuit pack
Circuit Pack Information	All Errors for Circuit Pack #	All errors on the circuit pack specified
	Circuit Pack Level Errors for Circuit Pack #	All errors that are on the circuit pack but are not associated with a port
Port Information	All Errors for Port #	All errors for the port that you selected
		1 of 2

Table 33. Standard error reports

Screen	Fault Menu Command	Report Description
External Devices View	All External Device Errors	All errors for all external devices
Individual External Device	Display Errors For External Device <name>	All errors for the external device specified
		2 of 2

Example: All Errors Report

The example below is an All Errors Report that you can generate at the Switch View.

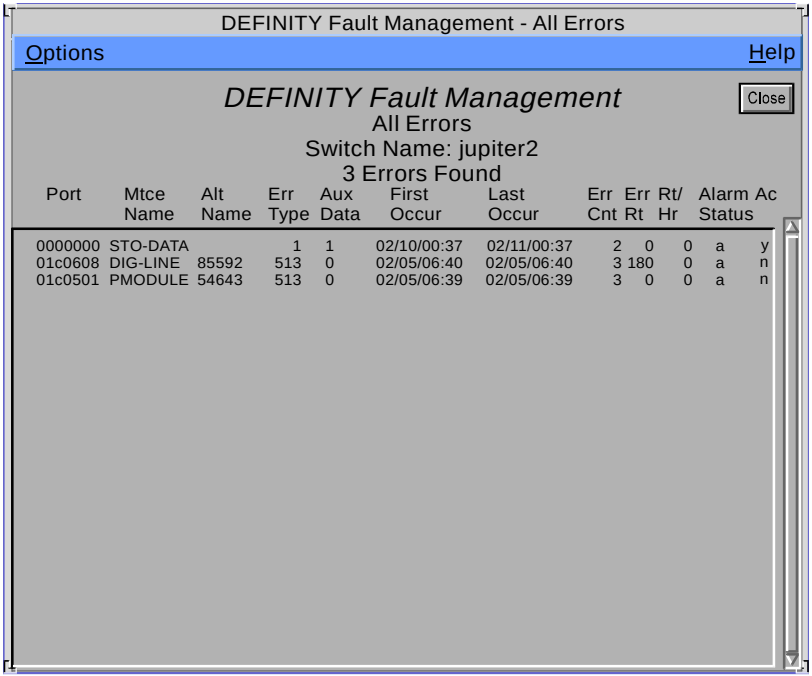


Figure 35. Error report for all errors for a cabinet

Field Descriptions: Errors Report

The following table provides a description for the fields contained in a standard error report.

Table 34. Field descriptions of error reports

Field	Description
Errors Found	The number of errors related to active alarms at that level
Port	The alphanumeric ID of the location of the alarmed object. Zeros in this field indicate the alarmed object is not connected to a port. For example, the port may be connected to a printer.
Mtce Name	Maintenance Name. The logical name of the maintenance object.
Alt Name	Identifies the maintenance object. • If the object is a station, this field contains the extension number. • If the object is a trunk, this field contains xxx/yyy, where: – xxx = the trunk group number – yyy = the member number • If the object is a private CO line, this field contains P/nnn, where: – P = private – nnn = the line group number
	1 of 3

Table 34. Field descriptions of error reports

Field	Description
Err Type	Error Type. The code identifying the type of problem. Only the error number displays because the error code is generally specific to the individual maintenance object and the total number of error codes may be extensive.
Aux Data	Auxiliary Data. Additional information concerning the error condition of the maintenance object. As with the error type, this data is specific to the maintenance object type. However, unlike the error type, only the most recent value of the auxiliary data is kept for each error type in the log.
First occur	First occurred. The month, day, hour, and minute that the system first recorded the error.
Last occur	Last occurred. The month, day, hour, and minute that the system first recorded the most recent error. If the system cannot retrieve the time of day the error occurred, a dummy date in the format 00/00/00:00, displays to distinguish it from reliable data.
	2 of 3

Table 34. Field descriptions of error reports

Field	Description
Err Cnt	Error Count. The total number of times that the error type has occurred for this maintenance object. The maximum number allowable is 255. If 255 displays in this field the actual error count may be higher.
Err Rt	Error Rate. The average rate at which the errors have occurred from the first occurrence to the present occurrence. The maximum number allowable is 255. If 255 displays in this field the actual error count may be higher.
Rt/Hr	Rate per Hour. An approximate rate that this error occurred in the last hour. The maximum number allowable is 255. If 255 displays in this field the actual error count may be higher.
Alarm Status	The status of the maintenance object in the error and alarm reports. This field indicates displays an a if active alarm is present.
Ac	Active. Indicates whether the maintenance subsystem considers this error to be active and indicative of a problem. • n = no • y = yes
	3 of 3

Procedure: Generate Error or Alarm Reports

To generate an error or alarm report, complete the following steps:

Procedure 25. Generate standard error or alarm reports

Step	Action
1	Open the component view for the hardware you want to examine.
2	Click **Fault** from the menu bar. Then, select the desired report from the list provided ***Result:*** The system generates and displays the report you selected.
3	To close the report, click **CLOSE** on the active report.

At any open error report, you can obtain more specific information about an error.

Description: Additional Error Information

The following table identifies and describes the additional information you can view when you click on a field contained in an error report.

Table 35. Display additional error information

Field	Displayed Screen	Description
Port	• Cabinet View • Circuit Pack Information • Port Information	Screens with information related to the port display. For example, if the port field value is: • 0000000, then the object is not connected to a port and the Switch View displays • 01, then the Cabinet View displays • 01c19, then the Cabinet View and Circuit Pack Information screen display. • 01c1903, then the Cabinet View, Circuit Pack Information, and Port Information screens display
Any field ***except*** Port	Error Description	The Error Description screen provides an individual error description and you can enter a note about the error.

Procedure: Generate Additional Report Information

To obtain additional information, click on one of the fields located in the error report.

When you click on any field except *Port*, the system displays an Error Description screen.

Example: Error Description Screen

The Error Description screen contains individual error descriptions about an individual error contained in an error report. At the error description screen you can enter and save a note regarding the error.

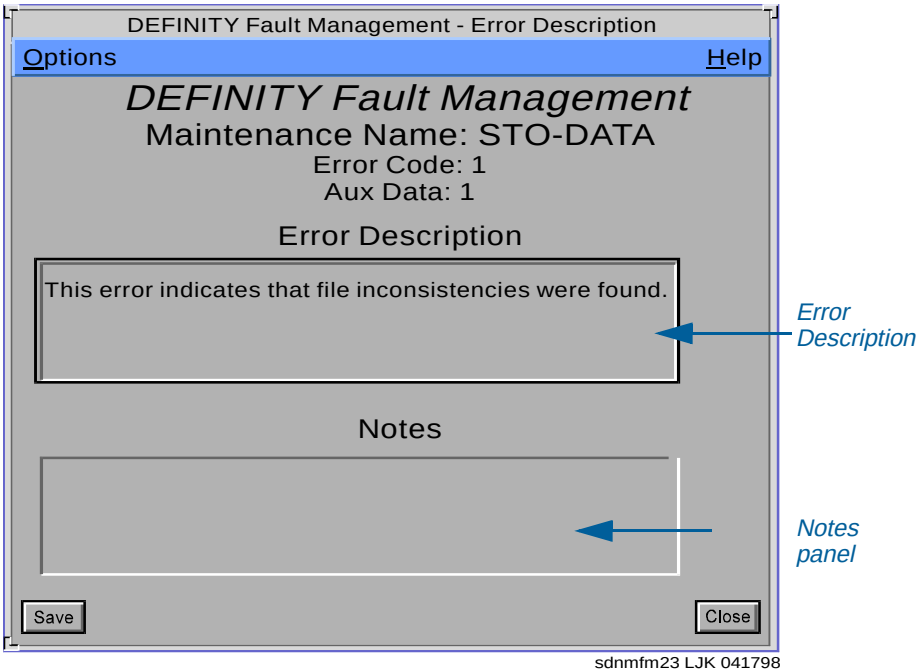


Figure 36. Error Description screen

Field Descriptions: Error Description Screen

The following table contains field descriptions for the Error Description screen.

Table 36. Field descriptions for the Error Description screen

Field	Description
Options	You can select two options from this menu: • Save to save the current data • Close to exit the screen
Help	Provides help information for the active window
Application Name	DEFINITY Fault Management
Maintenance Name	The name of the maintenance object that contains the error
Error Code	The code that identifies the error
Aux Data	Any auxiliary data about the error condition
Error Description panel	The Error Description panel contains a brief description of the error you selected.
Notes panel	The Notes panel provides a place for you to enter comments about the error.

Procedure: Modify Error Description Screen

To modify an Error Description screen, complete the following steps.

Procedure 26. Modify the Error Description screen

Step	Action
1	Display an error report window.
2	Click a value in any field **except** *Port*. ***Result:*** The system displays an Error Description screen.
3	To add, modify, delete a message do one of the following: • To add a note, type up to 5 lines of text or up to 255 characters. The Notes panel accepts all characters except the pipe (|) symbol. • To modify an existing message, highlight any existing text you wish to delete. Then, press **BACKSPACE**. Place the cursor where you wish to add data. Then, type a message. • To delete a note highlight the note. Then, press **BACKSPACE**.
4	Click **SAVE** to accept changes.

View Alarms

Alarms reports contain detailed alarm information about alarms that occur on a managed node. You can use the alarm report to identify managed nodes that may require maintenance.

These reports show alarm data that is current at the time you request the report. Fault Management does ***not*** update data for a report while the report window is open. To ensure that data is current, close and then re-open any open report window.

Options for Standard Alarm Reports

The Fault menu, located in each Component View, allows you to select a report that displays alarms for the active Component View.

The following table identifies and describes alarm reports available at each Component View.

Table 37. Standard Alarm Reports

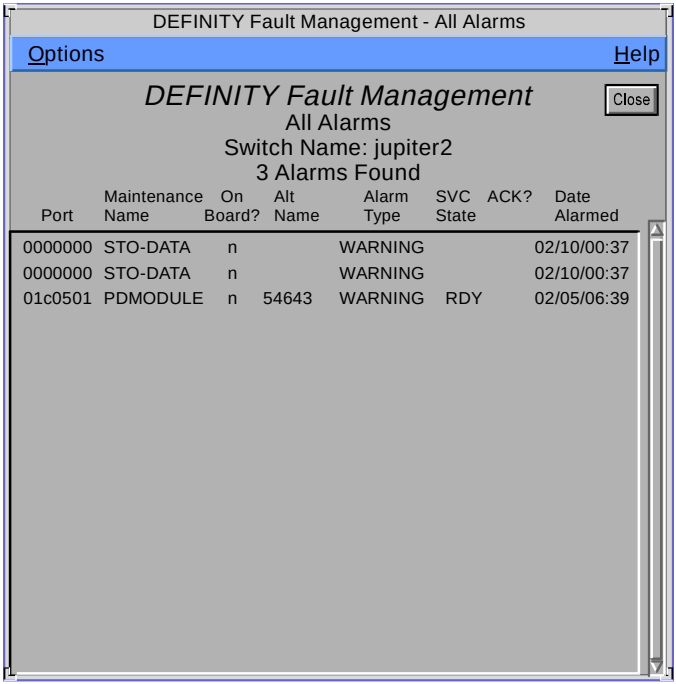
Screen	Fault Menu Command	Report Description
Switch View	All Alarms	All active alarms on the managed node
	Switch Level Alarms	All active alarms that are on the managed node, but that are not associated with a cabinet

Table 37. Standard Alarm Reports

Screen	Fault Menu Command	Report Description
Cabinet View	All Alarms for Cabinet #	All active alarms in the cabinet
	Cabinet Level Alarms for Cabinet #	All active alarms located in the cabinet that are not associated with any circuit pack
Circuit Pack Information	All Alarms for Circuit Pack #	All active alarms on the circuit pack
	Circuit Pack Level Alarms for Circuit Pack #	All active alarms located on the circuit pack that are not associated with a port
Port Information	All Alarms for Port #	All active alarms for the port
External Devices View	All External Device Alarms	All active alarms for all external devices that are connected to the DEFINITY system
Individual External Device	Display Alarms For External Device <name>	All active alarms for the external device specified.
		2 of 2

Example: Standard Alarm Report

When you select an alarm report from the Fault menu a standard alarm report appears. The example below shows a sample alarm report for a switch.



sdnmfm21 LJK 071498

Figure 37. Alarms report for all alarms at the Switch View

Field Descriptions: Alarms Reports

The following table provides a description for the fields contained in a standard alarm report.

Table 38. Fields on the alarms reports

Field	Description
# Alarms Found	The number of active alarms
Port	The alphanumeric ID location of the alarmed object. Zeros in this field indicate the alarmed object is not connected to a port (for example, a system printer). Data for this report sorts by port ID number.
Maintenance Name	The logical name of the maintenance alarmed object
On Board?	The location of the detected fault. • y = The fault is on the associated circuit pack • n = The fault is not associated with this circuit pack, but is associated with an off-board element.
	1 of 3

Table 38. Fields on the alarms reports

Field	Description
Alt Name	Additional data to identify the maintenance object. • If the object is a station, this field contains the extension number. • If the object is a trunk, this field contains xxx/yyy, where: xxx = the trunk group number yyy = the member number • If the object is a private CO line, this field contains P/nnn, where: P = private nnn = the line group number
Alarm Type	The fault severity as follows: • MAJOR • MINOR • WARNING
	2 of 3

Table 38. Fields on the alarms reports

Field	Description
Svc State	The current service state of the station and trunk port: • RDY = ready for service • OUT = out of service • IN = in service • Blank = there is no service state associated with the port
Ack?	The indicator that identifies whether INADS has acknowledged the alarm. • y = yes • n = no • Blank = the alarm has not and will not be reported to INADS
Date Alarmed	The month, day, hour, and minute the alarm condition occurred
	3 of 3

Procedure: Additional Alarm Report Information

To obtain additional information, click on one of the fields located in an alarms report. The following table identifies and describes the additional information you can view when you click on a field in an alarms report.

Table 39. Display additional alarm information

Field	Displayed Screen	Description
Port	• Cabinet View • Circuit Pack Information • Port Information	Screens with information related to the port display. For example, if the port field value is: • 0000000, then the object is not connected to a port and the Switch View displays • 01, then the Cabinet View displays • 01c19, then the Cabinet View and Circuit Pack Information screen display. • 01c1903, then the Cabinet View, Circuit Pack Information, and Port Information screens display

View Bulletin Board

You can view the messages contained on the Bulletin Board screen. Typically, technicians who are working to resolve errors on a managed nodes post status messages on the Bulletin Board of that managed node. This allow you to monitor the progress of any corrective action a technician makes.

Exception: MCU Switches

Fault Management allows you to view the contents of the bulletin board for all DEFINITY equipment ***except*** MCUs.

Example: Bulletin Board

The example below shows a sample of a Bulletin Board screen.

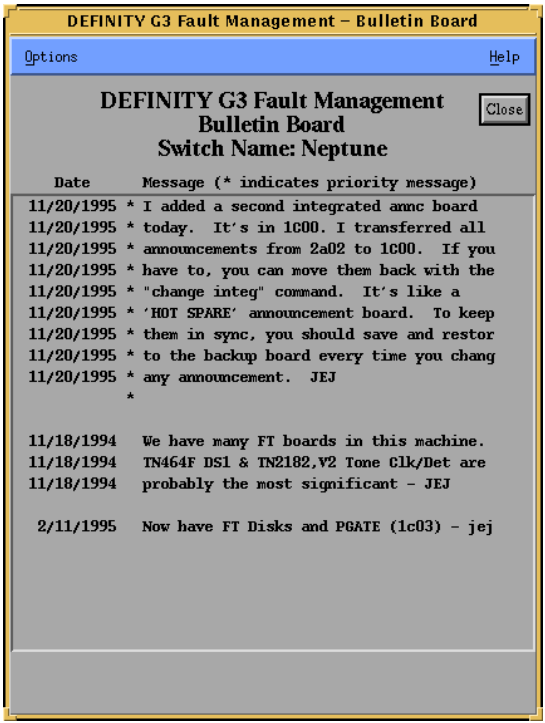


Figure 38. Bulletin Board

Field Descriptions: Bulletin Board

Table 40. Menu bar and field descriptions for the Bulletin Board

Menu Command and field	Description
Options	You can select two options from this menu: • Save to save the current data • Close to exit the screen
Help	Help information for the active window
Application Name	DEFINITY Fault Management
Report Name	Bulletin Board
Switch Name	The name of the DEFINITY system as it appears on the Network Management System (NMS) when the system is administered as a node on the network. This information is passed from the NMS.
Date	The date of the message
*	Indicates a high-priority message
Message	The bulletin message

Procedure: Open the Bulletin Board

To open the Bulletin Board screen, complete the following steps:

Procedure 27. Open the Bulletin Board

Step	Action
1	Go to the *Switch View.*
2	Select: ***Fault > Display Bulletin Board***. ***Result:*** The system displays the Bulletin Board screen.

10 Reports

Chapter Contents

Introduction

With Fault Management, you can create standard, system-generated reports, or custom reports.

You can generate standard reports from any component view. Standard reports provide configuration or fault information for the active component view.

You can create custom reports from the *Report Builder* screen in Fault Management. You build and format custom reports from information contained in standard reports.

Once you define the report specifications, you can output standard and custom reports in one the modes below:

- Output to a screen
- Output to a printer
- Output to a file

Create Standard Reports

Fault Management comes with standard fault and configuration report capabilities. These reports display as tables or as highlighted, graphical displays.

You use the same procedures to generate both types of reports.

Example: Table report

The figure below contains an example of a table report for a DS1 circuit pack shown below.

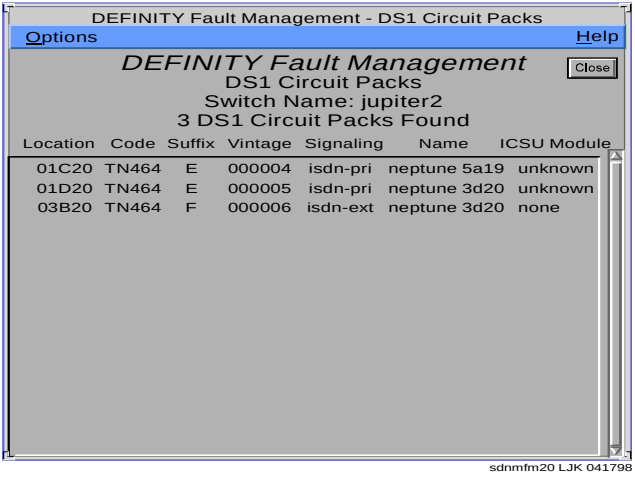


Figure 39. DS1 Circuit Pack report

Field Descriptions: DS1 Circuit Packs

The following table contains field descriptions for the DS1 Circuit Pack report.

Table 41. Field descriptions for DS1 circuit pack reports

Field	Description
# DS1 Circuit Packs Found	The number of DS1 circuit packs that match report criteria.
Location	The circuit pack cabinet, carrier, and slot. ***Note:*** Click on this field to display more information.
Code	The product code for the circuit pack.
Suffix	The suffix of the circuit pack.
Vintage	One of the following: • The release of the circuit pack. • The highlighted word CONFLICT; if there is a mismatch between the circuit pack administration and type.
Signaling	The type of signaling administered.
Name	The name assigned to the DS1 circuit pack as it was administered on the DEFINITY system.
ICSU Module	The ICSU (Integrated Call Service Unit) module that is attached to the circuit pack.

Example: Highlighting Report

Highlighting reports display colored borders that surround graphical depictions of system components. You can generate highlighting reports at the Switch view or the Cabinet view.

The example below identifies circuit packs with unassigned ports.

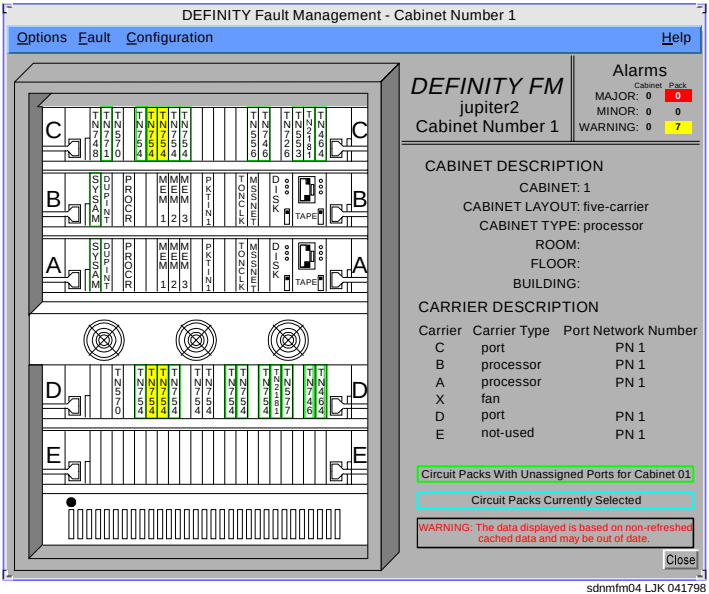


Figure 40. The Cabinet View displaying highlighting

Circuit packs with unassigned ports are highlighted.

The color and the message identify the filter.

Procedure: Create Standard Reports

The table below contains procedures to generate, save, and close a standard report.

Procedure 28. Create a standard report

Step	Action
1	Access one of the component view screens (Switch, Cabinet, External Devices).
2	From the Menu bar, select a standard report for the system configuration or existing faults: • Click **Configuration > Report choice** • Click **Fault > Report choice** ***Result:*** The system displays the selected report.
3	To save a data screen report, click **Options > Save** ***Note:*** You cannot save a highlighting report. ***Result:*** The system saves the report.
4	To close a report, select one of the options below: • For a data screen report, click **Options > Close** • For a highlighting report, click **Options > Clear Highlighting** ***Result:*** The system closes the report.

Create Custom Reports

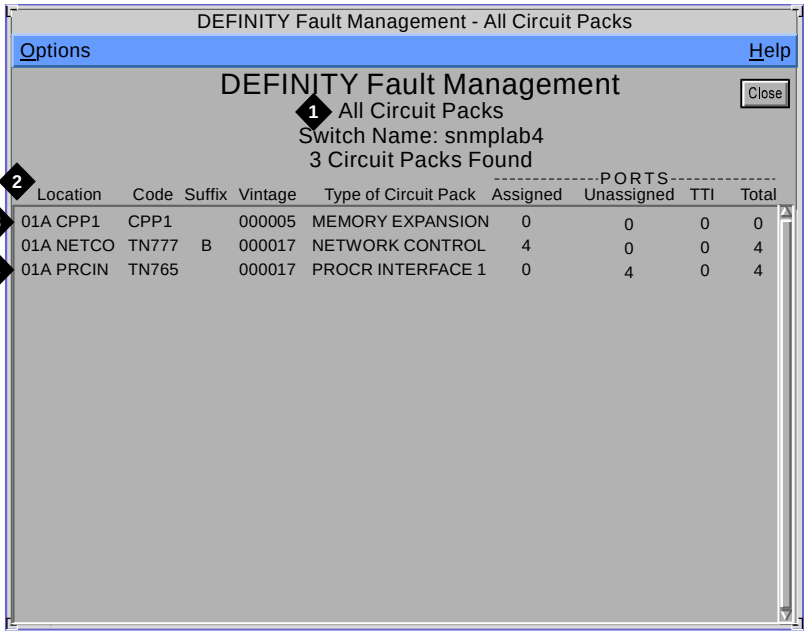
Fault Management provides the Report Builder feature to allow you to create custom reports. With the Report Builder you can create up to 10 permanent custom reports and an unlimited number of reports for one-time use.

You generate custom reports from one of four standard reports listed below:

- Alarms. For a sample, see *Figure 37 on page 207*.
- Circuit packs. For a sample, see *Figure 41 on page 223*.
- DS1 Circuit packs. For a sample, see *Figure 39 on page 218*.
- Errors. For a sample, see *Figure 35 on page 195*.

Example: Standard Report

The example below identifies values to use in a Report Builder screen.



1 Table to Search
2 Field Name
3 Value
4 To Value

Figure 41. Circuit Pack report

Example: Report Builder Screen

You would use the example above to complete a Report Builder screen. The example below shows a Circuit Pack report that was used to complete this screen.

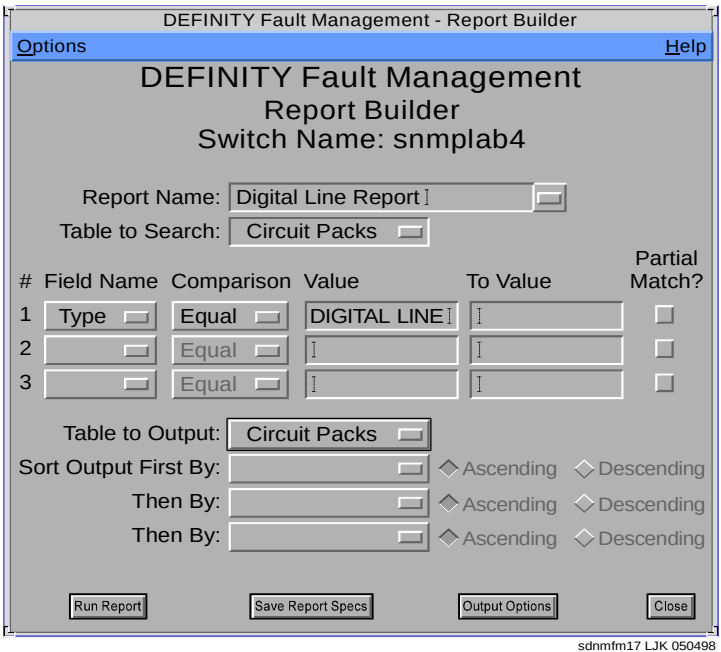


Figure 42. Completed Report Builder screen

Field Descriptions: Report Builder

The table below contains descriptions for the fields on the Report Builder screen.

Table 42. Fields on the Report Builder

Field	Description
Report Name	The name of the report. You can enter up to 55 characters, or select an existing report from the pull-down list.
Table to Search	The name of the standard report that you want to search. You must select one of the following values from the pull-down list: • Alarms (default) • Circuit Packs • DS1 Circuit Pacts • Errors
Field Name	The name of the field contained in the standard report that you want to search. You may leave this field blank or select any field listed on the pull-down list The field names listed on the pull-down list match the fields contained in the report of your *Table to Search* selection. You can select up to three **Field Names** for each custom report that you design.
	1 of 4

Table 42. Fields on the Report Builder

Field	Description
Comparison	The type of comparison you wish to generate between your selection in the *Field Name* field and the corresponding *Value* and *To Value* fields. You can select from two valid values in the pull-down list: • Equal (default) • Range
Value	The information you must complete if you wish to make a comparison. The entry must come from data that is located in the *Field Name* that you selected. The following guidelines will help you make your choice. • If you set the *Comparison* field to **Equal**, then Fault Management retrieves all values that match the value in this field. • If you set the *Comparison* field to **Range**, then Fault Management retrieves all data that fall in the range created by this entry and the entry in the *To Value* field. • If you set the *Comparison* field to **Range**, and if you leave the *To Value* field blank, then Fault Management retrieves all data equal to or greater than the entry in this field.
	2 of 4

Table 42. Fields on the Report Builder

Field	Description
To Value	You must type an entry in this field from data contained in the *Field Name* that you selected. The following guidelines will help you make your choice. • If you set the *Comparison* field to **Range**, then Fault Management retrieves all data that falls in the range created by this entry and the entry in the *Value* field. • If you set the *Comparison* field to **Range**, and if you leave the *Value* field blank, then Fault Management retrieves all data equal to or less than the value in this field.
Partial Match?	*Partial Match?* allows Fault Management to retrieve values that only partially match the contents of the *Value* and *To Value* fields. ***Note:*** If you need an exact match, make sure this check box is ***off***.
	3 of 4

Table 42. Fields on the Report Builder

Field	Description
Table to Output	This field determines your report format. The *Table to Output* field pull-down list includes the following choices: • Alarms (default) • Circuit Packs • DS1 Circuit Packs • Errors
Sort Output First By Then By Then By	The three sort output fields contain pull-down lists. You select the sort parameters for the report from this list. You must select either the **ascending** or **descending** sort option for each parameter. The default is **ascending**.
	4 of 4

Procedure: Create a Custom Report

Follow the procedure below to create a custom report.

Procedure 29. Create a custom report

Step	Action
1	Access one of the component views listed below: • Switch View • Cabinet View • External Devices View
2	In the *Menu* bar, select **Options > Report Builder**. ***Result:*** The system displays the *Report Builder* screen.
3	In the *Report Name* field, complete one of the options below to name the report: • Type a ***new*** report name in the field (maximum of 55 characters) • Click the pull-down list and select an ***existing*** report name from the list
4	In the *Table to Search* field, click the pull-down button and select a ***table*** from the pull-down list.

Procedure 29. Create a custom report

Step	Action
5	In the fields below, input the ***search parameters*** for the custom report. You can select a maximum of three field names for the search parameters. To select an option from a list, click the pull-down button and click the selection. **Line # 1** `Field Name`: Select a field name from the list `Comparison`: Select **Equal** (default) or **Range** (see the value fields below) from the list `Value`: Type the value that ***starts*** the range for the search `To Value`: Type the value that ***ends*** the range for the search `Partial Match?`: Click the button to ***allow*** partial matches of the data in the value fields. **Optional**. For Lines 2 and 3, input the appropriate search parameters for each field name to be included in the custom report.

Procedure 29. Create a custom report

Step	Action
6	In the *Table to Output* field, click the pull-down button and select one layout options listed below: • Alarms (default) • Circuit Packs • DS1 Circuit Packs • Errors
7	For all three *Sort Output* fields, complete the steps below in each field, if appropriate: `First By`: Select an option from the list. Click **Ascending** (default) or **Descending** `Then By`: (optional) Select an option from the list. Click **Ascending** (default) or **Descending** `Then By`: (optional) Select an option from the list. Click **Ascending** (default) or **Descending**
8	To create the custom report, click **RUN REPORT**. ***Result:*** The system displays the generated report on the screen.
9	To save the report specifications, click **SAVE REPORT SPECS**. ***Result:*** The system permanently saves report specifications.

Procedure 29. Create a custom report

Step	Action
10	To access the *Output Options* screen, click **OUTPUT OPTIONS.** ***Result:*** The system displays the *Output Options for Report Builder* screen. Refer to *"Select a Report Output Option" on page 236* for other options.
11	To exit the *Report Builder* screen, click **CLOSE.** ***Result:*** The system closes the *Report Builder* screen.
	4 of 4

Procedure: Change a Custom Report

You can change any of the specifications for an existing report. The only field that you ***cannot*** change is the name in the *Report Name* field.

Follow the procedure below to change the report specifications for an existing report.

Procedure 30. Change a custom report

Step	Action
1	Access one of the system views listed below: • Switch View • Cabinet View • External Devices View
2	In the *Menu* bar, select **Options > Report Builder**. ***Result:*** The system displays the *Report Builder* screen.
3	In the *Report Name* field, click the pull-down button and select the report to be changed from the list. ***Result:*** The system displays the selected report.
4	Change any of the report specifications ***except*** the name of the report.
5	To create the new report, click **RUN REPORT**. ***Result:*** The system generates the report.

Procedure 30. Change a custom report

Step	Action
6	To save the changed specifications, click Save Report Specs. ***Result:*** The system permanently saves the report specifications.
7	To access the *Output Options* screen, click **OUTPUT OPTIONS.** ***Result:*** The system displays the *Output Options for Report Builder* screen. Refer to *"Select a Report Output Option" on page 236* for other options.
8	To exit the *Report Builder* screen, click **CLOSE.** ***Result:*** The system closes the *Report Builder* screen.

Procedure: Delete a Custom Report

Follow the procedures below to delete an existing report. I

Procedure 31. Delete a custom report

Step	Action
1	Access one of the system views listed below: • Switch View • Cabinet View • External Devices View
1	In the *Menu* bar, select **Options > Report Builder**. ***Result:*** The system displays the *Report Builder* screen.
2	At *Field Name*, click the pull-down button and select the report to be deleted. ***Result:*** The system displays the selected report.
3	From the menu bar select **Options > Delete** ***Result:*** The system deletes the report.
4	To exit the *Report Builder* screen, click **CLOSE.** ***Result:*** The system closes the *Report Builder* screen.

Select a Report Output Option

The *Report Output* screen contains three types of output options for both standard and custom reports:

- Output to a screen
- Output to a printer
- Output to a file

The screen also contains the Highlight Objects feature. This feature highlights the system components, at each level on the Fault Management screens, that appear on the report.

This section contains procedures to select the output option for both standard and custom reports.

Example: Output Options Screen

The figure below is an example of the *Output Options for Report Builder* screen.

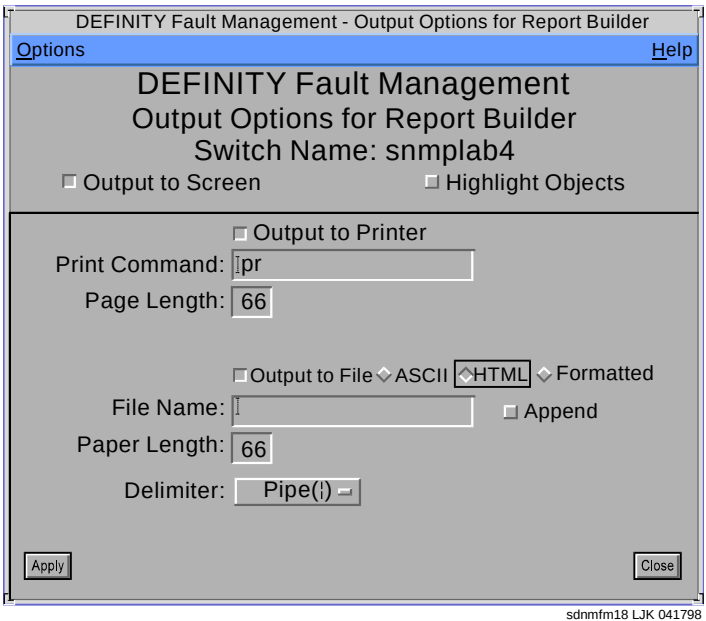


Figure 43. Example of the Output Options for Report Builder screen

Field Descriptions: Output Options screen

The following table contains field descriptions for the Output Options for Report Builder screen.

Table 43. Field descriptions for Output Options for Report Builder

Field	Description
Menu Bar	**Options > Apply** Generates the report based on the entries you make in the fields. • If you open the Output Option screen from the Report Builder screen, then the **Apply** command saves the current information and closes the screen. • If you select **Apply** from a report window, then the command sends the report to the selected output destination and closes the screen. **Options > Close** Closes the Output Options screen without saving your entries. **Help** Contains help messages for the Output Options screen.
Application Name	Displays a Help window.
Window Name	Title for the screen: Output Options for [**report name**]
	1 of 4

Table 43. Field descriptions for Output Options for Report Builder

Field	Description
Switch Name	The name of the managed node as administered on the Proxy Agent.
Output to Screen	The system displays the report in a new window.
Highlight Objects	Highlights the system components, at each level on the Fault Management screens, that appear on the report.
Output to Printer	The option that sends the report to a printer. You complete the fields below to select the ***printer*** as the output option: `Print Command`: [**printer command**] `Page Length`: **66** (default for letter-size paper)
	2 of 4

Table 43. Field descriptions for Output Options for Report Builder

Field	Description
Output to File	The system writes the report to a file. You complete the fields below to select the ***file*** as the output option: `Output to File`: Click the box to select this option `ASCII, HTML, Formatted`: Click ***one*** of the file format options `File Name`: Type the [**path for the file name**] `Append`: Click this box to ***add*** the new report data to an existing file without overwriting the current data. The system appends the new data at the end of the file. `Paper Length`: **66** (default for letter-size paper) `Delimiter`: **Pipe (|)** [default for ASCII reports]. Click the pull-down button to select a different delimiter.
	3 of 4

Table 43. Field descriptions for Output Options for Report Builder

Field	Description
APPLY	The button that saves the output selections for the selected report.
CLOSE	The button that closes the Output Options screen.
Messages	The message area on the Output Options screen. The system displays the messages below if the following conditions occur: • If you neglect to type data into required fields, Fault Management displays a prompt message after you click **APPLY**. • If Fault Management fails to append or to write a file as you requested, the system displays a failure message. You can change your field entries and try again.
	4 of 4

Procedure: Select a report output option

Follow the procedures below to select an output options for a standard or custom report.

Procedure 32. Select a report output option

Step	Action
1	Access the *Report Builder* screen.
2	In the *Report Name* field, • Select a report from the pull-down list • Click **DISPLAY REPORTS** ***Result:*** The system displays the *Output Options* for the selected report.
3	Click the **Highlight Objects** box to highlight the system components, at each level on the Fault Management screens, that appear on the report. ***Note:*** You must click the Highlight Objects box each time you change the report specifications on the *Report Builder* screen. ***Result:*** The system highlights the system components.

Procedure 32. Select a report output option

Step	Action
4	***Screen Option*** Complete the steps below to select the output to screen option: • Click the **Output to Screen** box • Click the **Apply** button ***Result:*** The system displays the report in a new window.
5	***Print Option*** Complete the steps below to select the output to printer option: • Click the **Output to Printer** box • In the *Print Command* field, type [**print command**] • In the *Page Length* field, change the **66** lines default for letter-size paper, if appropriate • Click the **Apply** button ***Result:*** The system sends the report to the designated printer.

Procedure 32. Select a report output option

Step	Action
6	***File Option*** Complete the steps below to select the output to file option: • Click the **Output to File** box • Click ***one*** of the file formats below: – **ASCII** – **HTML** – **Formatted** • In the *File Name* field, type [**path for the file name**] • Click the **Append** box to add the report data to the file. If you want to overwrite the existing data in the file, then do ***not*** click the Append box. • In the *Page Length* field, change the **66** lines default for letter-size paper, if appropriate • In the *Delimiter* field, change the **Pipe (|)** delimiter, if appropriate • Click the **Apply** button ***Result:*** The system saves the report specifications to the file.
7	Click the **Close** button to exit the screen.

11 Troubleshooting

Chapter Contents

Introduction

Fault Management generates messages to notify you when errors occur within Fault Management. The messages display at the bottom of the Switch View and Port View. Messages also appear in pop-up boxes during Fault Management startup.

This chapter identifies the messages that appear most often. A description of each message along with corrective actions follows each message.

Many of the corrective actions occur on the Proxy Agent. To take these corrective actions, you will need to telnet to the Proxy Agent. See for steps to telnet to the Proxy Agent. Then, refer to *The DEFINITY Proxy Agent User Guide* to complete some corrective actions. The actions that require Proxy Agent interaction are in ***bold italics***.

If you receive a message that does not appear in this chapter, you can call the Lucent Technical Services Organization at **1 (800) 242-2121** for assistance.

Switch View Messages

The following error messages display in the message area of the Switch View:

Refresh Failures

Error messages display in the message area of the Switch View when Fault Management fails to complete a successful Alarms and Error Refresh or Circuit Pack Refresh. Below are descriptions of Alarms and Errors Refresh failures and Circuit Pack Refresh Failures.

Alarms and Errors

Message `ERROR: Alarms and Errors Refresh failed.`

Description The Alarms and Errors Refresh has failed.

Action

1. Check the connection status between the Proxy Agent and the managed node. The connection must be up.
2. Check the Managed Node screen on the Proxy Agent to ensure the DEFINITY system is administered.
3. Retry the refresh.

Circuit Pack

Message `ERROR: Circuit Pack Refresh failed.`

Description The circuit pack refresh has failed.

Action

1. Check the connection status between the Proxy Agent and the DEFINITY system. The connection must be up and allowing the Proxy Agent to communicate with the NMS.
2. Check the Managed Node screen on the Proxy Agent to ensure the DEFINITY system is administered.
3. Go to the Setup screen and set **refresh on startup** to TRUE. A TRUE value causes the Proxy Agent to refresh all cached data.
4. Restart Fault Management.

Data Errors

This section contains examples of errors specific to the Switch View that occur when Fault Management does not successfully retrieve data. Data errors occur when data is inaccurate, incomplete, or does not reach Fault Management at all. The errors are divided into the following categories:

- *Proxy Agent Response Messages*
- *HP OpenView Messages*
- *Cabinet data Message*
- *Out-of-date data Messages*

Proxy Agent Response Messages

Message `ERROR: Bad response from agent while requesting <data type>.`

Description The application received a bad response from the Proxy Agent while requesting the specified data.

Action

1. Check to see whether the connection between the Proxy Agent and the DEFINITY system is up.
2. Ensure that the Proxy Agent is running and communicating with the NMS.
3. Check the Managed Node screen on the Proxy Agent to ensure the DEFINITY system is administered.
4. Go to the Setup screen and set **refresh on startup** to TRUE. A TRUE value causes the Proxy Agent to refresh all cached data.
5. Restart Fault Management.

Message `ERROR: Bad response from the Proxy Agent.`

Description The Fault Management application received a bad response from the Proxy Agent while requesting data.

Action

1. Check to see whether the connection between the Proxy Agent and the DEFINITY system is up.
2. Ensure that the Proxy Agent is running and communicating with the NMS.
3. Check the Managed Node screen on the Proxy Agent to ensure the DEFINITY system is administered.
4. Retry the operation.

HP OpenView Messages

The following messages display only on HP OpenView:

Messages

```
ERROR: No response from agent (requesting <data type>).
ERROR: No response from agent while requesting <data type>.
ERROR: No response from agent.
```

Description

The Proxy Agent did not respond to a request for SNMP data on the HP OpenView platform.

Action

1. Check to see whether the connection between the Proxy Agent and the DEFINITY system is up.
2. Ensure that the Proxy Agent is running and communicating with the NMS.
3. Check the Managed Node screen on the Proxy Agent to ensure the DEFINITY system is administered.
4. Retry the operation.

MIB Message

Message

```
ERROR: Could Not Get <MIB object> from Agent
```

Description

Fault Management received an error when Fault Management requested specified data from the DEFINITY system. For example, this can occur when you request data for an unassigned port, or if the connection between the DEFINITY system and the Proxy Agent is down.

Action

1. Check to see whether the connection between the Proxy Agent and the DEFINITY system is up.
2. Ensure that the Proxy Agent is running and communicating with the NMS.
3. Check the Managed Node screen on the Proxy Agent to ensure the DEFINITY system is administered.
4. Go to the Setup screen and set *the Refresh on Startup* field to TRUE. A TRUE value causes the Proxy Agent to refresh all cached data when you start Fault Management.
5. Restart Fault Management.

Cabinet data Message

Message `ERROR: No Cabinet Data Received.`

Description No cabinet data was received from the Proxy Agent. The Fault Management application cannot run.

Action

1. Check to see whether the connection between the Proxy Agent and the DEFINITY system is up.
2. Ensure that the Proxy Agent is running and communicating with the NMS.
3. Check the Managed Node screen on the Proxy Agent to ensure the DEFINITY system is administered.
4. Go to the Setup screen and set **refresh on startup** to TRUE. A TRUE valid causes the Proxy Agent to refresh all cached data.
5. Restart Fault Management.

Out-of-date data Messages

Message

```
Warning: The data displayed is based on
non-refreshed cached data and may be out of
date.
```

Description

One of the following conditions is true:

- The connection between the Proxy Agent and the DEFINITY system was not up when you started Fault Management.
- The last refresh failed.
- The Refresh Proxy Agent on the *Startup* field on the Setup screen is set to FALSE.

Action

1. Re-establish the connection to the Proxy Agent.
2. Do one of the following, as required:
   - Restart Fault Management.
   - Refresh the alarms and errors data and the configuration data.

Check the following common causes for a disconnect:

- The modem connected to the Proxy Agent to see if it is working.
- The phone connected to the Proxy Agent to see if it has a dial tone.
- The login and password for the Proxy Agent to ensure that they are match the login and password administered on the managed node
- Check the login and password on the Proxy Agent Communications form.
- Check to see if the DEFINITY management port is available. To check this:
  - Call the modem from a voice station to see if the management port produces a modem tone.
  - Try to login to the DEFINITY management port from another terminal and modem.
  - Telnet to the Proxy Agent to see if the NMS can access the Proxy Agent.

- Check the Proxy Agent running status. If the Proxy Agent remains disconnected from the DEFINITY system after you check all of these items, call the Technical Service Center for assistance.

Configuration Errors

Configuration errors appear on the Switch View when a switch type is either incompatible with or unknown to Fault Management.

Incompatible Switches

Message `ERROR: Incompatible switch types cannot continue.`

Description The switch type is incompatible with switch types supported by Fault Management. The switch type may have been administered incorrectly on the switch.

Action Administer a switch type on the Proxy Agent that is compatible with Fault Management.

Unknown Switches

Message `ERROR: Unknown switch type. Cannot continue.`

Description The Fault Management application does not recognize the switch type received from the Proxy Agent and therefore cannot continue.

Action Administer a switch type on the Proxy Agent that Fault Management recognizes.

Port Messages — Data Errors

This section contains examples of errors specific to the Port View that occur when Fault Management does not successfully retrieve data. Data errors occur when data is inaccurate, incomplete, or does not reach Fault Management at all.

These following types of messages display in the message portion of the Port View:

- *Timing Error*
- *Proxy Agent Response Messages*

Timing Error

Message	`Please Try Later.`
Description	You requested the port data while another data request was in progress.
Action	Wait for the current data request to finish executing. Then, request the port data again.

Proxy Agent Response

Message	`ERROR: Could Not Get Port Data from Agent.`
Description	An error occurred when Fault Management requested port data from the DEFINITY system. This can happen if you request data for an unassigned port. This can also happen if the connection between a managed node and a Proxy Agent is **down**.

Action Check the connection between the Proxy Agent and the managed node.

Message `Not Available`

Description Fault Management is not receiving a data from the Proxy Agent.

Action

- Check the connection between the Proxy Agent and DEFINITY system. Make sure the connection is up.
- Increase the value in the Number Retries on *SNMP Timeout* field on the *Setup* screen.

Messages Specific to HP OpenView

The following data error displays only in HP OpenView at the Port View:

Message `ERROR: No response from the agent.`

Description The Proxy Agent did not respond to a request for SNMP port data.

Action

1. Check to see if the connection between the Proxy Agent and the DEFINITY system is up,
2. Check the Proxy Agent for the following:
   - The Proxy Agent must be running
   - Check the Managed Node screen on the Proxy Agent to ensure the DEFINITY system is administered.

Pop-up Messages

Refresh failures and Configuration errors display in pop-up message boxes. Refresh failures can display during any refresh session. Configuration pop-up messages display on the Managed Node list and the Setup screen.:

Refresh Failures

Error messages display in pop-up screens when Fault Management fails to successfully complete one of the following refreshes:

- *Startup Refresh*
- *Alarms and Errors Refresh*
- *Circuit Pack Refresh*
- *Bulletin Board Refresh*
- *Configuration Data Refresh*

This section contains messages for refresh failures that appear in pop-up screens.

Startup Refresh

Message

```
WARNING: The startup refresh failed. The data
displayed is based on the data cached on the
Proxy Agent. This data may be out of sync with
the actual switch data.

The most likely cause of this problem is the
connection between the Proxy Agent and the
DEFINITY PBX being down or turned off.
```

Action

1. Re-establish the connection to the Proxy Agent.
2. Restart Fault Management.

Alarms and Errors Refresh

Message

```
There is already an Alarms and Errors refresh in
progress. If you still want to request another
refresh, please wait until the current one is
complete.
```

Action Wait for the current refresh to complete before requesting another one.

Message

```
There is currently a data request in progress.
Please try the Alarms and Errors Refresh again
later.
```

Action Wait for the data refresh to complete before requesting the refresh.

Message

```
WARNING: The Alarms and Errors refresh has
failed. The data displayed is based on the data
cached on the Proxy Agent. This data may be out
of sync with the actual switch data.
```

Description

The most likely cause of this problem is one of the following:

- The connection between the Proxy Agent and the DEFINITY system is down.
- The connection between the Proxy Agent and the DEFINITY system is turned off.

Action

1. Check to see if the connection between the Proxy Agent and the DEFINITY system is up
2. Check to see that the Proxy Agent is running and communicating with the NMS.
3. Check the Managed Node screen on the Proxy Agent to ensure the DEFINITY system is administered.
4. Retry the refresh.

Circuit Pack Refresh

Message `There is already a Circuit Pack refresh in progress. If you still want to request another refresh, please wait until the current one is complete.`

Action Wait for the current refresh to complete before requesting another one.

Message `There is already a Circuit Pack refresh in progress. Please do not press any cabinet buttons until it is done.`

Action Wait until the circuit pack refresh begins to receive circuit pack data before clicking on a cabinet icon.

Message `WARNING: The Circuit Pack refresh has failed. The data displayed is based on the data cached on the Proxy Agent. This data may be out of sync with the actual switch data.`

`The most likely cause of this problem is the connection between the Proxy Agent and the DEFINITY PBX being down or turned off.`

Action

1. Check to see if the connection between the Proxy Agent and the DEFINITY system is up.
2. Check to see if the Proxy Agent is running and communicating with the NMS.
3. Check the Managed Node screen on the Proxy Agent to ensure the DEFINITY system is administered.
4. Retry the refresh.

Bulletin Board Refresh

Message

```
There is currently a data request in progress,
please try the Bulletin Board Refresh again
later.
```

Action

Wait for the current refresh to complete before requesting another one.

Message

```
WARNING: The Bulletin Board refresh has failed.
The data displayed is based on the data cached
on the Proxy Agent. This data may be out of sync
with the actual switch data.

The most likely cause of this problem is the
connection between the Proxy Agent and the
DEFINITY PBX being down or turned off.
```

Action

1. Check to see if the connection between the Proxy Agent and the DEFINITY system is up
2. Check to see if the Proxy Agent is running and communicating with the NMS.
3. Check the Managed Node screen on the Proxy Agent to ensure the DEFINITY system is administered.
4. Retry the refresh.

Configuration Data Refresh

Message

```
There is currently a data request in progress.
Please try the Configuration Data Refresh again
later.
```

Action

Wait for the data request to complete before requesting the refresh.

Configuration Errors

Managed Node List

Message

```
The application found no managed nodes to
display.
```

Action

- Check for Proxy Agent and network connectivity.
- Check to see that the Proxy Agent is running.
- Fault Management must be **release 2.0.**

Setup Screen

Message

```
ERROR: Could not open resource file to save the
Setup Information. The values have not been
saved.
```

Action

1. Make sure that DG3FMDIR is either not set or is set to a valid directory where the file resides.
2. Make sure that the appropriate resource file exists.
   - For NetView: /usr/OV/OneVision/DG3FM/DG3FMdefaults
   - For OpenView: /opt/OV/OneVision/DG3FM/DG3FMdefaults
3. Check the permissions on the file. Fault Management must be able to write to the file.
4. Restart Fault Management.

Startup Messages

The following messages display in the upper left-hand portion of the screen during Fault Management startup.

Memory

Message `Usage: dg3fm host_name community_name [switch_name].`

Description Fault Management started with incorrect parameters. The DEFINITY icon selection name and the name in the SNMP The SNMP configuration entry for the DEFINITY system may not match. This messages displays only in OpenView.

Action

1. In the Network Management System (NMS) platform, select **Options > SNMP Configuration**. Correct the DEFINITY name.
2. Restart Fault Management.

Incorrect Parameters

Message `DEFINITY Fault Management: out of memory!`

Description Fault Management could not allocate enough memory to run.

Action Do one or more of the following:

- Delete some windows
- Close some active programs
- Add memory to the NMS computer

Startup Failure

Message `Refresh on Startup Failed! Continuing with Cached Data.`

Description One of the following conditions is true:

- The connection between the Proxy Agent and the DEFINITY system was not up when you started Fault Management.
- The last refresh failed.

Action

1. Re-establish the connection to the Proxy Agent.
2. Do one of the following, as required:
   - Restart Fault Management.
   - Refresh the alarms and errors data and the configuration data.

Check the following common causes for a disconnect:

- The Proxy Agent's capacity to dial out by checking the following:
  1. The modem status. The modem must be working.
  2. Check the phone line for a dial tone.
- The Proxy Agent must have a current, correct login, and correct password for the DEFINITY system.
- You must have set your permissions correctly on the DEFINITY system?
- To check the login and password on the Proxy Agent Communications form.

- A DEFINITY management port must be available. Call the modem from a voice station to check for a modem tone.
- Login to the DEFINITY management port from another terminal and modem?
- Telnet to the Proxy Agent to see if the NMS can access the Proxy Agent.
- Check to see that the Proxy Agent is running.

  If the Proxy Agent remains disconnected from the DEFINITY system after you check all of these items, call the Technical Service Center for assistance.

Index

Lucent Technologies
Bell Labs Innovations

DEFINITY® Performance Management Release 2.0

User Guide

J58890UC L107
PG-5E677
585-229-808, Issue 1
November 1998

Contents

About This Book

Chapter Contents

Introduction

This chapter contains helpful information about the documentation and the Lucent resources available to customers for the **DEFINITY Network Management Release 2.0** products, which include:

- DEFINITY Proxy Agent
- DEFINITY Fault Management
- DEFINITY Performance Management
- DEFINITY Network Management Common Software

The ***User Document Set*** section contains the complete list of installation guides and user guides that are delivered on CD-ROM. This section also includes an overview of this book, the target audience for this book, and the format conventions used in the procedures.

The ***Lucent Resources*** section includes essential information about the Project Provisioning Package which contains:

- System requirements for hardware and software
- Ordering information
- Installation options
- Custom services
- Lucent and customer responsibilities

An account executive can provide customers with a copy of the Project Provisioning Package upon request.

User Document Set

The ***User Document Set*** for Release 2.0 is delivered on a separate CD-ROM. The CD-ROM contains all the installation and user guides for the **DEFINITY Network Management Release 2.0** products, including:

- DEFINITY Proxy Agent Installation Guide
- DEFINITY Proxy Agent User Guide
- DEFINITY Fault Management Installation Guide
- DEFINITY Fault Management User Guide
- DEFINITY Performance Management and Common Software Installation Guide
- DEFINITY Performance Management User Guide

The ***installation guides*** for the products specifically cover the procedures to install and set up the software so that the product is ready to use. Generally, only an experienced network manager should install and set up the software.

The ***user guides*** for the products describe the functions, screen, and procedures to operate and manage the software. Once the software is set up, then users should refer to the user guides to operate and administer the product.

Installation procedures

The insert on the CD-ROM contains the procedures to install the guides. The ***Readme*** file on the CD-ROM also contains the complete installation procedures.

Main Menu

After you install the guides, you can access the books from the **Main Menu.**

The **Introduction** section on the Main Menu contains procedures for navigating between the books and searching for specific information.

The **Comments** section contains an evaluation form. You are encouraged to submit the form with your suggestions for improvement ***and*** comments on the useful elements of the documentation.

DEFINITY Performance Management User Guide

The ***DEFINITY Performance Management User Guide Release 2.0*** contains the explanation and procedures to manage the day-to-day operations of the software and related external devices.

The user guide is divided into two sections:

- Section 1 Network Management Systems (NMS) includes chapters 1 through 3. For an overview of the chapters, refer to *Chapter 1, "NMS Overview"*.
- Section 2 DEFINITY Performance Management includes the rest of the chapters in this guide.

The chapters in the NMS overview are laid out by functions and are organized by the primary tasks to operate the software, including:

- Login and access procedures
- System help and navigation features
- Administration procedures to add, change, and delete data
- Operational procedures to manage the software features and functions

The user guide is an essential resource for users who are unfamiliar with the purpose and operation of the product.

Audience

The user guide is particularly helpful to those that use Performance Management as part of their routine duties. The guide is also intended for:

Customers, including:

- Network managers
- System administrators
- Technicians

Lucent personnel, including:

- Service providers and technicians
- Sales teams
- Training and Education
- Translation Services

Format Conventions

The format conventions used in this book are visual cues to help users identify the type of action they should take to execute the steps in the procedures.

The use of the format conventions are consistent throughout all the books in the ***User Document Set*** for this release.

Table 1. Format Conventions

Convention	Description
Bold text	Indicates that you should type the **bold text** exactly as shown. Example: Type **display status**
	(1 of 4)

Table 1. Format Conventions

Convention	Description
[**Bold text in brackets**]	Indicates that you should type **discrete** data that is specific to your system, ***without*** the brackets. Discrete data can be any of the following: • Managed node name • Name of a directory or file • Drive name • Any data that is ***not*** a default option Examples: • Type [**d**] **install** • Type your [**password**] • Select the [**managed node name**] from the Help list.
Function keys	Appear in bold letters and indicate that you should press that key on the keyboard to execute a specific action. Examples: • Press **Enter** (also refers to the **Return** key) • Press **Tab** • Press **Esc**
	(2 of 4)

Table 1. Format Conventions

Convention	Description
Series of Menu Options **File > Save**	The greater than (**>**) symbol indicates that your should select an option from a series of menus. For example, Click **File > Save** means that you should: • Click on the first menu (File). • Then click on the second option (Save) from the second menu. The term ***select*** is used in place of ***click*** if: • A program does not accept mouse commands. or • You need to choose an option from a Help list. To select an option from a Help list: • Use the arrow keys or TAB key to move the cursor to the option on the list. • Then press **ENTER** to select the option.
	(3 of 4)

Table 1. Format Conventions

Convention	Description
Result paragraph	Describes the result of an action taken in a step, as described in the following example: ***Result:*** The system displays the MAIN MENU. A results paragraph may also contain a message or a prompt in `constant width` font. A prompt sets up the action to be taken in the next step. ***Result:*** The system displays the command window that contains the prompt: `Do you wish to continue? y/n`
	(4 of 4)

Lucent Resources

Lucent Technologies provides customers with a variety of planning, consulting, and technical services.

The ***account executives*** are the customers' primary source to obtain information and explore custom options to meet the customers' specific business needs.

The sections below briefly describe the services that are available to customers.

Project Provisioning Package

The ***Project Provisioning Package*** for this release contains the specific recommendations and specifications to plan and install the ***DEFINITY Network Management*** products.

A copy of the Project Provisioning Package is posted on the DEFINITY Solutions website. You can access the website at:

http://www.bcs.lucent.com/sales_market/definity/sysmgmt/dfm.htm

Customers can also request a copy of the package from their account executive.

The package is intended to clarify the responsibilities of the customer and Lucent during the installation project. The package contains the following information:

- Installation options (see below)
- Connectivity diagrams
- Ordering information
- Pre-installation hardware and software requirements

- Installation schedule and responsibilities
- Platform acceptance test
- Post installation verification and acceptance

The Provisioning Package also contains detailed explanations of the three (3) implementation options that are available to customers:

1. Customer installation of the NMS platform and DEFINITY Network Management products.
2. Lucent Technologies Technical Support Center (TSC) installation of the DEFINITY Network Management products.
3. Lucent Technologies NetCare® Network Consulting Group installation of a complete turn-key system for the Network Management System (NMS).

Options two and three are further explained in the sections below.

Technical Support Center (TSC)

The Technical Support Center (TSC) is part of the Technical Support Organization (TSO).

You can call the Technical Support Organization (TSO) at the toll-free number below and follow the prompts to reach the TSC:

TSO 1-800-242-2121

The Technical Support Center (TSC) works with account executives and customers to install and support the DEFINITY Network Management products.

Both the customer and TSC perform the Post Installation Verification and Acceptance Test of Performance Management.

Time and materials charges

If customers choose to install the DEFINITY Network Management products themselves, then the TSC is not responsible for the installation of the product software.

If the customers do not install and set up the system according to the guidelines in the Project Provisioning Package, then the TSC will bill the customers for support on a time and materials basis.

NetCare Network Consulting Group

The NetCare® Network Consulting Group is part of the Professional Services Organization. NetCare is available to work with customers to design and build a turn-key Network Management System.

Customers can select all or any combination of the NetCare services summarized below:

- Plan and design a custom network system
- Purchase and configure the Network Management System (NMS)
- Install and integrate the DEFINITY Network Management software products on the NMS platform
- Train users on the operation and management of the software tools

Account executives can provide customers with additional information about NetCare and other custom services.

Year 2000 Compliance

The Business Communication System (BSC) part of Lucent Technologies makes the following statement with respect to any product manufactured and sold by Lucent BCS in connection with a product's operation in the year 2000.

Any product or version/release of a product that is introduced as generally available on or after September 30, 1996, will be year 2000 compliant or Lucent BSC will make it year 2000 compliant at our cost.

Any other product, depending on the specific product and its release or version, will fit into one of the following categories:

- The product is year 2000 compliant.
- If the product is not year 2000 compliant, Lucent BCS will provide an upgrade path to a generally available release that is year 2000 compliant at a reasonable cost to the customer.
- If the product is not year 2000 compliant, and no upgrade path to a generally available release that is year 2000 compliant is available, Lucent BCS will evaluate whether there are potential modifications to the product that will make it year 2000 compliant, and if Lucent BCS determines that such modifications are economically practical, Lucent BCS will offer such modifications to the customer at a reasonable cost.
- If the product is not year 2000 compliant, and if Lucent BCS determines that it is not economically practical to make the product year 2000 compliant, Lucent BCS will inform the customer of this fact and offer migration options at a reasonable cost.

1 NMS Overview

Chapter Contents

Introduction

The Network Management System (NMS), and the DEFINITY Proxy Agent, along with DEFINITY Performance Management, facilitate centralized management of DEFINITY systems. To maintain this centralized management, Performance Management complies with Simple Network Management Protocol (SNMP). While the DEFINITY Proxy Agent is SNMP compliant, it operates remotely and connects to multiple managed nodes concurrently.

SNMP Information Exchange

SNMP specifications define how Performance Management and DEFINITY systems exchange information. The information exchange works like this:

1. Proxy Agents receives a call to request data.
2. Proxy Agents receive data from managed nodes.
3. Proxy Agents manage the information with a Management Information Base (MIB).
4. Proxy Agents use SNMP protocol to translate the information into data that the NMS can read.
5. Proxy Agents forward alert and threshold data to the NMS.
6. The NMS translates and displays the information on submaps that depict DEFINITY systems.

NMS Submaps

On these maps, the NMS creates icons that represent managed nodes and Proxy Agents and also creates lines to represent connections between each Proxy Agent and its associated managed nodes. The NMS has the capability to produce three different submap options to depict a DEFINITY system. This allows you to organize managed nodes by geographic location or in a customized fashion as well as with one all-encompassing, generic map.

The icons on these submaps change colors to identify alarm states for Proxy Agents and alerts for managed nodes. The lines change colors to indicate changes in the connection states between Proxy Agents and their associated managed nodes.

ThIs chapter contains the following information:

- Descriptions of NMS capabilities
- Commands used to access information in the NMS
- Steps to access the NMS
- Steps to exit from the NMS

System Requirements

Introduction

The ***Project Provisioning Package*** for this release contains the ***specific*** recommendations and specifications to plan and install the Performance Management software.

The package also defines the terms and conditions for the three installation options:

- Customer installation
- Technical Support Center (TSC) installation services
- NetCare® Network Consulting Group installation of a complete ***turn-key*** system

Refer to *"Lucent Resources" on page 17* for more information.

Hardware Requirements

You should work with your Lucent account executive to determine the hardware requirements that your organization needs to meet its business and performance specifications.

Software Requirements

The DEFINITY Performance Management application operates with the following software:

- DEFINITY Proxy Agent, Release 2.0
- Network Management System (NMS) platform
- DEFINITY Fault Management, Release 2.0 (optional)

Supported Systems

Release 2.0 of Performance Management ***only*** supports DEFINITY G3 PBX releases G3V4 through DEFINITY ECS release R6

Network Management Products

The DEFINITY Performance Management 2.0 product ***only*** supports the network management products listed below:

- DEFINITY Proxy Agent 2.0
- DEFINITY Fault Management 2.0

NMS Platforms

The DEFINITY Performance Management 2.0 product supports the following Network Management System (NMS) platform:

HP OpenView Releases 4.11, 5.0, and 5.01 installed on Solaris Release 2.5.1

NMS Capabilities

Introduction

The Network Management System (NMS) provides an overall view of DEFINITY systems. The NMS platform that Performance Management uses is OpenView. This section contains brief descriptions of the chapters that discuss NMS capabilities.

NMS Submap Administration

Chapter 2, "NMS Submap Administration" describes the 3 submap options available on the NMS. This chapter also contains procedures that are necessary to set up maps on the NMS.

NMS Alert Notification

Chapter 3, "NMS Alerts" describes Proxy Agent alarm states and managed node alert states. This chapter also identifies alert notification methods available at the NMS level and contains procedures that are necessary to access alert information.

NMS Command Procedures

Introduction

Each icon or connection line on an NMS submap provides access to information about managed nodes or connections. In addition, each icon provides access to one of the following applications:

- Proxy Agent
- Performance Management

Access the NMS

To access the NMS, do the following:

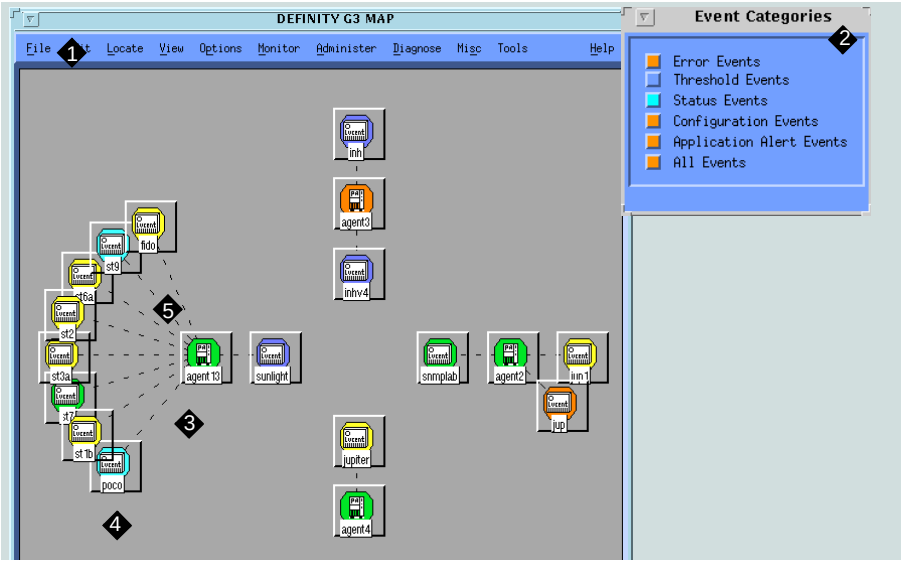
1. Log in to NMS.
2. At a UNIX editor prompt, type **$OV_BIN/ovw&** and press **Enter**.

   Result: The system opens the NMS application
3. Double-click a DEFINITY icon.

   Result: The system opens a DEFINITY submap.

Screen Components

The following example is a generic submap with screen components that display on any submap.



1 Platform-specific Menu Bar
2 Application Alert Event Log
3 Proxy Agent Icon
4 Managed Node Icon
5 Connection Line

Figure 1. DEFINITY Generic Submap

Menu Bar

To access submenus for DEFINITY equipment, click a DEFINITY managed node icon. Then, click **Performance > DEFINITY**

Result: The system displays the DEFINITY submenu.

The selections that are available on this submenu vary based upon the graphical element you selected. Items that are ***not*** available display in grey.

Application Alert Event Log

The Application Alert Event Log contains a running record of actions that occur on the NMS.

The following example shows activity that occurred in the All Events category.

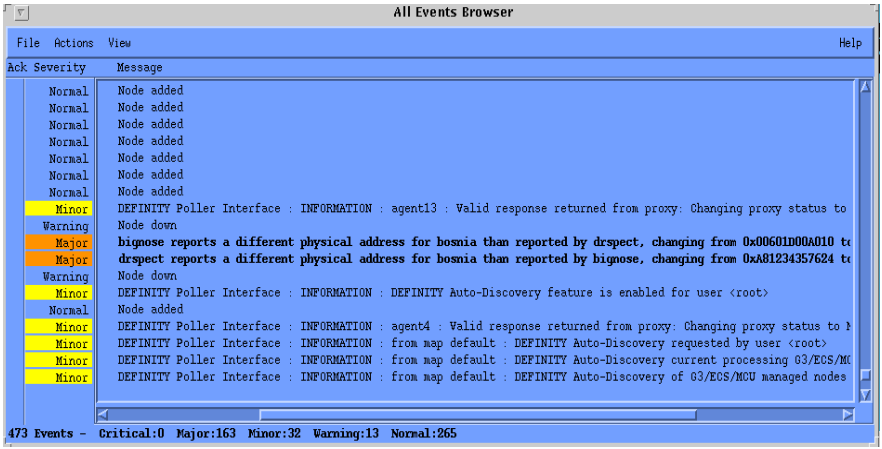


Figure 2. Application Event Alert Log — All Events

Proxy Agent Icon

When you select a Proxy Agent Icon, DEFINITY submenu options reflect commands that are available for that Proxy Agent. You can also double-click the Proxy Agent icon to initiate a telnet session to the Proxy Agent application.

You can also select the Proxy Agent Icon. Then, press the third mouse button to display a menu that contains commands available for the Proxy Agent.

Managed Node Icon

When you select a managed node Icon, DEFINITY submenu options reflect commands that are available for that managed node. You may also double-click a managed node icon to start the Performance Management application.

You can also select a managed node icon. Then, press the third mouse button to display a menu that contains commands available for the DEFINITY managed node.

Connection Line

When you select a connection line, the DEFINITY submenu options reflect commands that are available for that connection. You may also double-click the connection line to display the Connection Status screen.

You can also select a connection line. Then, press the third mouse button to display a menu that contains commands available for connections.

Exit from the NMS

To exit from the NMS, complete the following steps:

1. Close all programs associated with the NMS.
2. At the main window, click **Map > Exit**.

   Result: The system closes the NMS application.

2 NMS Submap Administration

Chapter Contents

Introduction

The Network Management System (NMS) provides graphical user interface (GUI) capabilities that allow you to view alarms for Proxy Agents and alerts for managed nodes. You can view the connection status between Proxy Agents and their associated managed nodes.

The NMS creates three network submaps to display this information. These submaps include:

- Generic
- USA
- Custom

This chapter contains the following NMS submap procedures:

- Select Submap options
- Modify submap information on the Proxy Agent
- Modify submap information in the Override Location file

Auto-Discovery

Using the Auto-Discovery feature, the NMS performs the following functions to translate data from the Proxy Agent into these submaps:

- Searches for Proxy Agent and managed node data
- Adds Proxy Agent icons and managed node icons to designated DEFINITY submaps
- Shows connections between Proxy Agents and managed nodes

To utilize Auto-Discovery you must assign Auto-Discovery passwords and set up the Auto-Discovery feature.

Set Auto-Discovery Passwords

The default installation setting for Fault Management grants access to Auto-Discovery for all users. Users who have access to Auto-Discovery can modify NMS read/write submaps.

If you wish to restrict Auto-Discovery access, you must assign Auto-Discovery passwords. Anyone who has root level access can restrict individual or group access to Auto-Discovery.

Procedure

To set auto-discovery passwords, do the following:

1. To administer Auto-Discovery passwords, type the following and press **Return**:
   /opt/OV/OneVision/DG3Poll/AD_Passwds

   Result: The system displays the Auto-Discovery passwords administration file.

2. In the first field, type one of the following options in upper case and press the **Spacebar**:
   - **L** for an individual user
   - **G** for groups of users

3. In the second field, type one of the following in lower case and press Return:
   - individual [**unix login id**]
   - group [**unix group id**]

   Result: The system designates user access to Auto-Discovery.

SECURITY ALERT:

Unauthorized users who attempt to access Auto-Discovery receive a message in the Application Alert Event Log that provides authorization status for each user. The NMS displays the Application Alert Event Log on all NMS screens.

Set up Auto-Discovery

To set up NMS submaps, you must activate Auto-Discovery. Activating Auto-Discovery allows the NMS to create submaps from information that was transmitted from Proxy Agents.

Setting up Auto-Discovery on a public network differs from the process of setting up Auto-Discovery on a private network. This section contains procedures for both network types.

Public Networks

If you have a public network, perform the following procedure to set up Auto-Discovery. This procedure activates Auto-Discovery for the first time and during any active, network session.

To activate Auto-Discovery, click **Performance > DEFINITY > Execute Auto-Discovery**

Result: The system searches for Proxy Agents and associated managed nodes.

Private Networks

If you have a private network, you must complete the following steps to ensure that the Proxy Agent and NMS can communicate effectively. The entries you type in the NMS must ***exactly*** match the entries that you typed in the Proxy Agent.

1. From the menu bar in the Network Management System, click **Options > SNMP Configuration**.

   Result: The system opens the SNMP Configuration window. Existing managed nodes appear at the top portion of the screen.

2. Turn off the **USE PROXY TO ACCESS TARGET** button, if it is selected.
3. Type information in the fields below. Do ***not*** change any other fields.
   - *Target* — Proxy Agent [**host name or IP address**] The name that resides in the host file.
   - *Community* — [**community name**] The name you administered for the private network on the Proxy Agent C*hange Network Managers Screen*.
   - *Set Community* — [**g3pa**] Identical to the Set Community data administered on the Proxy Agent C*hange Network Managers Screen*.
4. Click **ADD**. Then, click **OK**.
5. To activate Auto-Discovery, click **Performance > DEFINITY > Execute Auto-Discovery**

   Result: The system searches for Proxy Agents and associated managed nodes.

Select Network Submap

The NMS provides three submap options that allow you to organize your DEFINITY system in three different ways. You can organize your DEFINITY systems in the following ways:

Note: For information on modifying submaps and the Location File, go to *"Modify NMS Submaps" on page 61*.

NMS Submap Options

- Generic submap. The Generic submap is the system default. This submap provides point-to-point connections and displays an overview of your DEFINITY system.
- USA submap. The USA submap allows you to organize your DEFINITY system by geographic location in the United States. The USA submap allows you to drill down to state submaps.
- Custom submap. The custom submap allows you to organize your DEFINITY system according to your specific business needs. The Custom submap allows you to place icons on a user-specified submap.

This section provides the following information about submaps:

- Advantages for using each submap
- Graphical views of each submap
- Procedures to access submaps

Root Level Icons

The system displays the Root map when you log in to the NMS. Icons representing NMS submaps display on this screen. The example below shows DEFINITY submap icons that appear on the Root map.

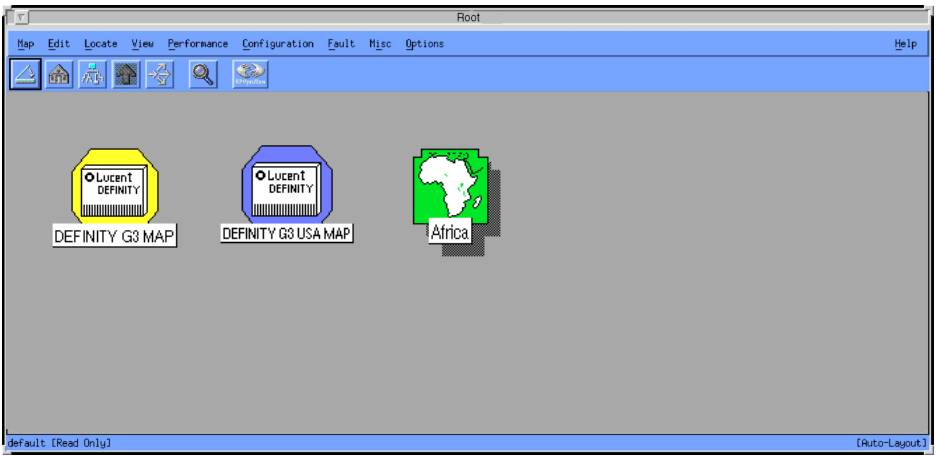


Figure 3. NMS Root map

Generic Submap

The generic submap uses a point-to-point layout to display an overview of all Proxy Agents and their associated managed nodes. The generic submap icon resides on the open map and at the root level of the NMS.

You double-click the DEFINITY generic submap icon on the Root map to open the DEFINITY submap shown below.

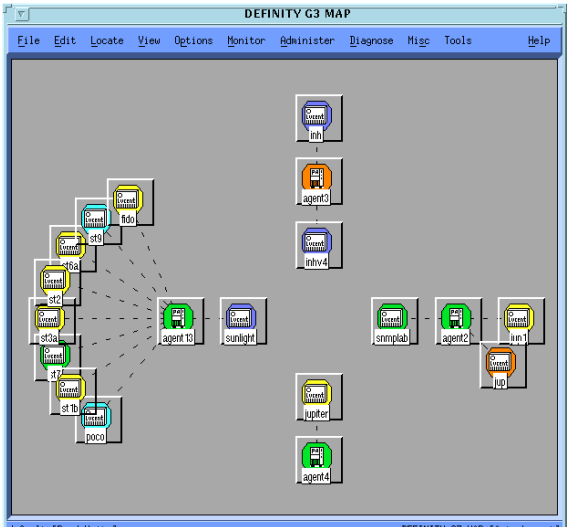
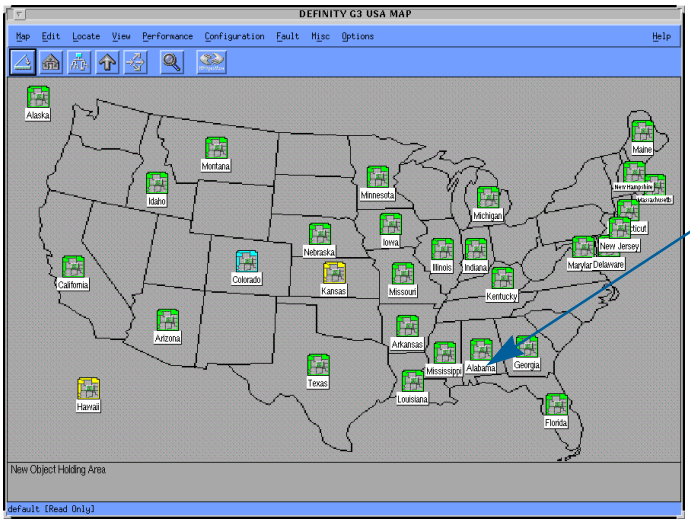


Figure 4. Example of a DEFINITY submap

USA Submap

The USA submap allows you to view your DEFINITY system by geographic location. Managed nodes and Proxy Agent objects appear on the state that you administered in the Proxy Agent.

You double-click the DEFINITY USA submap icon on the Root map to open the DEFINITY USA submap shown below:



Double click an icon in a state to open a submap that displays all DEFINITY objects in that state.

Figure 5. Example of a DEFINITY USA submap

State submap

You double-click a managed node icon on a USA submap to display a state submap similar to the map shown below.

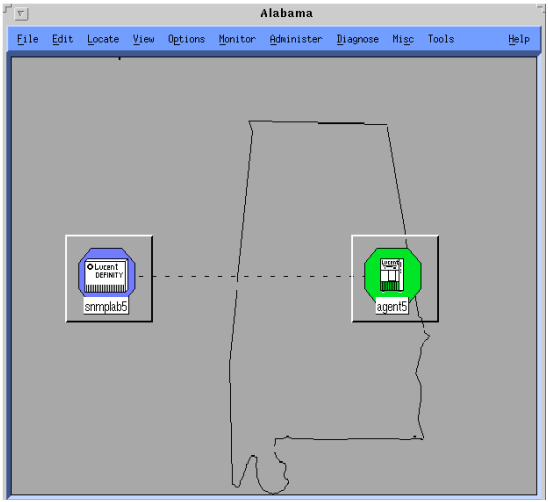


Figure 6. Example of a state submap

Custom Submap

Custom submaps allow you to manage the DEFINITY system at a more specific level than the other submaps. For example, you can organize information according to business territories or according to the type of DEFINITY systems that you manage.

To create a custom submap similar to the example below, you must administer a custom map on the Proxy Agent *Managed Nodes* screen or the Location file. For information on modifying submaps and the Location File, go to *"Modify NMS Submaps" on page 61*.

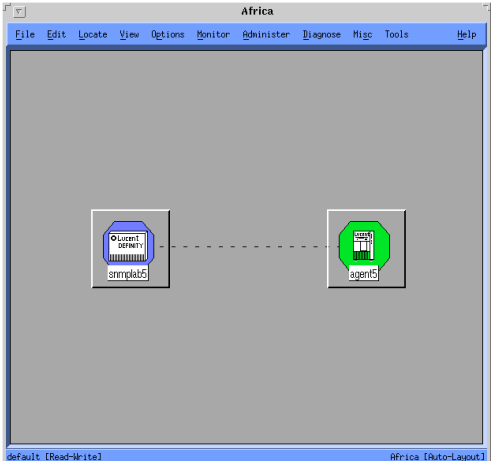


Figure 7. Example of a custom submap

Connections

Introduction

The NMS allows you to view two types of connections and to view the status of each connection. The two types of connections that you can administer are: static or dynamic. The status of each of these connections reflects the activity of that connection.

From the NMS, you can connect managed nodes to Proxy Agents, disconnect managed nodes from Proxy Agents, and verify the status of a connection.

This section contains:

- Graphical depictions of connections as they appear on network submaps
- Descriptions that contrast the differences between static and dynamic connections
- Descriptions of the six connection status
- Procedures to establish connections
- Procedures to drop connections
- Methods to verify connection status

View Types of Connections

To view connection types, you must go to a DEFINITY submap. At the submap, you will see one of the following types of connections:

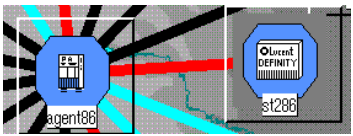


Figure 8. Sample OpenView 5.0 static connection

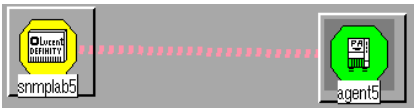


Figure 9. Sample OpenView 5.0 dynamic connection

Figure 10. Sample OpenView 4.11 static connection

Figure 11. Sample OpenView 4.11 dynamic connection

Connection types

The Proxy Agent now supports both ***static*** and ***dynamic*** connections to managed nodes.

You can assign up to **150** dynamic connections on the MANAGED NODES screen. The Proxy Agent only supports **30** active connections at a given time. The 30 active connections can be a combination of static and dynamic connections.

Static connections

A ***static*** connection maintains a ***continuous*** communication link between the Proxy Agent and the managed node.

We recommend that you select the static connection to monitor ***critical*** managed nodes for 24 hours per day, 7 days per week.

Dynamic connections

A ***dynamic*** connection maintains a ***temporary*** communication link between the Proxy Agent and the managed node.

We recommend that you select the dynamic connection to monitor ***less critical*** managed nodes on an as-needed basis.

Any Simple Network Management Network Protocol (SNMP) request or alarm on a managed node will initiate a dynamic connection. The dynamic connection will stay up as long as the Proxy Agent is actively processing SNMP requests and then ***time-out*** after a specified period.

The NMS does ***not*** poll for health data if a dynamic connection is assigned to a managed node.

Identify Connection Status

Each connection line appears in one of six colors that represent the six status options for connections. If you do not wish to use the system default colors, you may assign a custom color by modifying values in the **$APP_DEF/OVw** file. The table below describes connection status.

Table 2. NMS connection status

Status on OpenView	Default Color	Connection Status
OVw*warningStatusLineColor	Cyan	Off
OVw*marginalStatusLineColor	Yellow	Init
OVw*downStatusLineColor	Red	Down
OVw*downStatusLineColor	Red	Other
OVw*upStatusLineColor	Black	Up
OVw*testingStatusLineColor	Pink	Idle

Connect a Managed Node

OpenView allows you to establish connections between a Proxy Agent and a managed node with the following steps:

1. Click on the line that represents a connection between a Proxy Agent and a managed node.
2. Click **Performance > DEFINITY > Start Connection**

Result: The system changes the connection line to yellow while it is trying to make the connection. If the connection is successful, the line changes to black. If unsuccessful, the line changes to red.

Disconnect a Managed Node

OpenView also allows you to disable a managed node from a Proxy Agent.

CAUTION:

If you disable a managed node, you place it in a status of **off**. To use this connection in the future, you must enable the connection on the Proxy Agent or start the connection.

To disable a managed node from a Proxy Agent, do the following:

1. Click the line that represents a connection between a Proxy Agent and a managed node.
2. Click **Performance > DEFINITY > Stop Connection**

   Result: The system changes the connection line to cyan when the managed node disconnects.

View the Status of a Connection

During any active NMS session, you can access details about a selected connection.

To view details about a connection available on the Connection Status screen, do the following:

1. Click the line that represents a connection between a Proxy Agent and a managed node.
2. Click **Performance > DEFINITY > Connection Status**

   Result: The system displays the Connection Status screen for the selected connection.

Example: Connection Status screen

The information you can view on a Connection Status screen is similar to the example shown below.

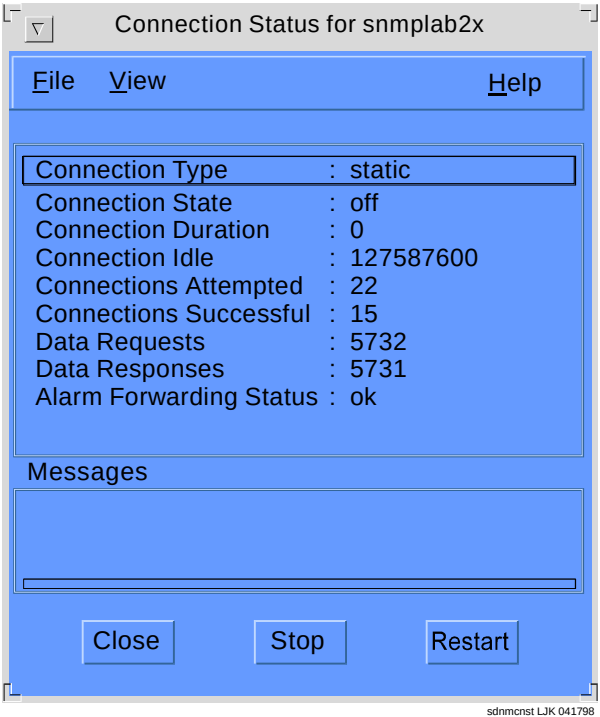


Figure 12. Sample Connection Status

Field Description

The following table provides descriptions for the connection details available on the Connection Status screen.

Table 3. Field descriptions for Connection Status screen

Field	Description
Connection Status	Identifies the selected status for the connection. The connection status can be: **init**, **up**, **down**, **off**, **idle**, or **other**.
Connection Type	Identifies static and dynamic connections.
Connection Duration	The length of time that a connection is in the **up** status.
Connection Idle	The length of time that a connection is in the **idle** status.
Connections Attempted	The number of times the Proxy Agent attempted to connect to the managed node.
Connections Successful	The number of successful connections from the Proxy Agent to the managed node.
Data Requests	The number of data requests from a Proxy Agent to a managed node.
	(1 of 2)

Table 3. Field descriptions for Connection Status screen

Field	Description
Data Responses	The number of times a managed node responds to a data request from a Proxy Agent.
Alarm Forwarding Status	Displays **ok** if the alarm status transmitted successfully. Displays **failed** if the alarm status did not transmit successfully.
	(2 of 2)

Verify Static Connection Status

Proxy Agents maintain continuous contact with their associated managed nodes to transfer current data to the Network Management System (NMS). Lack of data or incorrect data can indicate that a connection problem exists.

The NMS provides two methods to verify connection status: Icon states and a Managed Node Lists screen.

Icon States

Connection icons provide the current connection status for a managed node. You can determine the connection status of a managed node by viewing managed node icons on one of the three network submaps. See *Table 2 on page 50* for details.

Open a Managed Node List screen

You can display a screen that lists all managed nodes that connect to a Proxy Agent. This list contains the connection status for each managed node.

To open a managed node list, do the following:

1. Select a Proxy Agent icon from the network submap.
2. Click **Performance > DEFINITY > Show Managed Nodes**

Result: They system displays the Managed Node List for Proxy Agent displays.

Example: Managed Node List screen

When you open a managed node list, you will see a screen similar to the Managed Node List for Proxy Agent below.

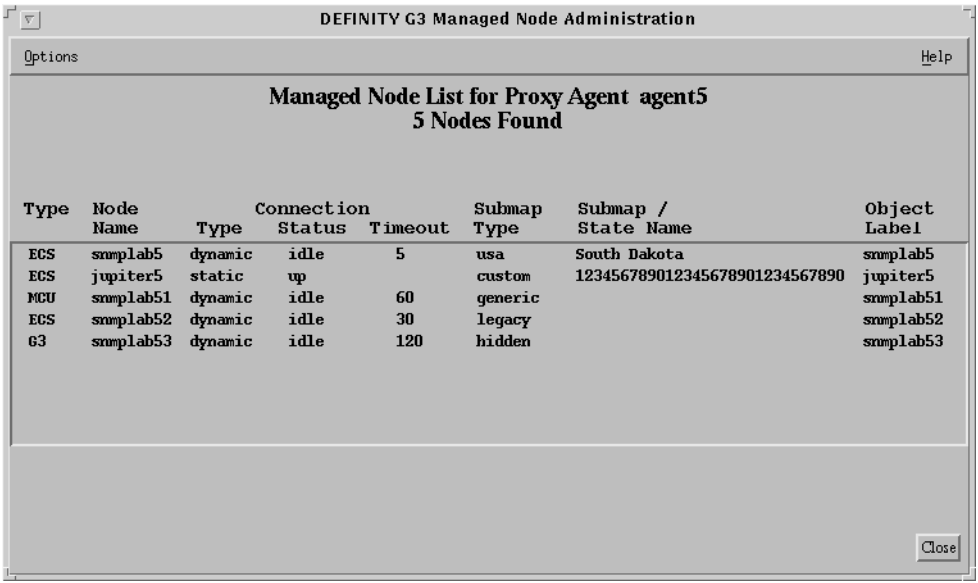


Figure 13. Managed Node List

Field Descriptions

The table below contains field descriptions for the Managed Node List for Proxy Agent screen shown above.

Table 4. Field descriptions for Managed Node List for Proxy Agent screen

Field	Description	Example
Type	The type of switch (ECS, G3, MCU).	ECS
Node Name	The managed node name as administered in the Proxy Agent.	snmplab2
Connection Type	The type of connection: **static** or **dynamic**	dynamic
Connection	The status of the connection: **up**, **down**, **off**, **idle**, **other**, or **init**.	up
Timeout	Timeout refers to the time administered on the Managed Node screen on the Proxy Agent. This value indicates that the Proxy Agent must transfer data to the NMS before the allotted time expires.	5
Submap	The type of submap: Generic, USA, or Custom	Custom
		(1 of 2)

Table 4. Field descriptions for Managed Node List for Proxy Agent screen

Field	Description	Example
Submap Location	The type of submap associated with either the USA or Custom submap	1234567890
Object Label	The system name of the managed node. The object label does not need to match the name administered in the Proxy Agent.	snmplab2
		(2 of 2)

Modify NMS Submaps

If you wish to modify location or connection information for a submap, you can edit the *Location Override* file from a text editor or can modifying the *Default Location* screen on the Proxy Agent.

Modify the Location Override File

In the *Location Override* file, you can change location information for managed nodes or hide managed nodes. The changes you administer in the *Location Override* file do ***not*** change the information contained in the Proxy Agent. This functionality allows multiple NMS users to view the same information in different formats.

Directions for modifying the *Location Override* file are contained within that file. To modify the *Location Override* file, do the following:

1 At a UNIX prompt, type **/opt/OV/OneVision/DG3Poll/Location** and press **Return.**

Result: The system opens the *Location Override* file.

2 Follow the directions contained in the *Location Override* file.

3 NMS Alerts

Chapter Contents

Introduction

The Network Management System When Performance Management performs a data collection, or when the Network Management System (NMS) performs a poll, the NMS color-codes managed node icons to identify alerts for those managed nodes.

When the NMS polls Proxy Agents and discovers an alarm for a Proxy Agent, the NMS color-codes the associated Proxy Agent icons to reflect alarm states.

Performance Management comes with the facility to notify you by pager or by email when alerts occur. You may also install the add-on software, TeleAlert or Remedy to provide more notifcation capabilities.

This chapter describes the:

- Icon states for Proxy Agents
- Icon states for managed nodes
- Alert notification methods

Identify NMS Alerts

Introduction

When a Proxy Agent has an alarm or a managed node has an alert, the NMS colors the corresponding icon to indicate the severity of the alarm or alert. When multiple alarms or alerts that have more than one level of severity occur, icon colors represent the most severe alarm or alert.

See *"Icon States" on page 56* for details on icon states.

This section contains information that identifies icon states for Proxy Agents and managed nodes and describes the events that change an icon state.

Identify Proxy Agent Icon States

Proxy Agent alarms occur when alarm forwarding fails or when an authentication failure occurs. Because alarms manifest as colored icons, the following section refers to alarm states as icon states.

Each state of a Proxy Agent icon represents a condition that exists between a Proxy Agent and a managed node. The NMS platform assigns the names of these states. The table below describes Proxy Agent icon states that occur in OpenView.

Table 5. Proxy Agent icon states

OpenView State Name	Description
Normal	The Proxy Agent is communicating with the NMS.
Warning	The Proxy Agent is communicating with the NMS but the NMS received an Authentication Failure trap sent by the Proxy Agent.
Major	The Proxy Agent failed to forward alarms to the administered destination.

Events that Change Proxy Agent States

The color of a Proxy Agent icon changes when polling events or trap events indicate a change in the Proxy Agent alarm status.

Proxy Agent icon states change when OpenView polls a Proxy Agent and receives one of the unacceptable results identified in the table below.

Table 6. Polling changes for Proxy Agent icon alarm states

Result of poll	Default polling interval (min)	New State
AlarmForward = Failed	5	Major
Proxy Agent does not exist or does not respond	5	Unknown

If the icon is in the **New** state and a subsequent poll finds an acceptable response, the icon returns to the **Normal** state.

Identify Managed Node Icon States

Managed node alerts arise when unacceptable conditions occur on a managed node. Because alerts manifest as color-coded icons, the following section refers to alert states as icon states.

The state of a managed node icon represents the current alert for that managed node. The NMS platform assigns the names of these states.

The table below describes managed node icon states that occur in OpenView.

Table 7. Managed node icon alert states

OpenView State Name	Definition
Normal	The managed node has no alert.
Warning	The managed node has at least one warning alert.
Minor	The managed node has at least one minor alert.
	(1 of 2)

Table 7. Managed node icon alert states

OpenView State Name	Definition
Major	The managed node has at least one major alert.
Unknown	One of the following conditions is true: • Communication between a Proxy Agent and a managed node is unstable; therefore, the Proxy Agent cannot indicate the status or health of the managed node. • The NMS cannot communicate with the Proxy Agent and, therefore, cannot determine the status of the managed node. • A dynamic connection that has not received a fault status update or a major or minor alert.
	(2 of 2)

Events that Change Managed Node Icon States

The color of a managed node icon changes when Performance Management conducts a data collection that identifies an alert level. Below is a description of the alert levels you might encounter.

Data Collection. Performance Management collects data on a user-specified basis. This information is specific to managed nodes with static connections in an **up** state. When an unacceptable health condition arises, that managed node icon accepts the icon state described in the table below.

Table 8. Performance data collection change managed node icon states

Result of poll	New icon state
g3healthMajor > 0	Major
• g3healthMinor > 0, and • g3healthMajor = 0	Minor
• g3healthWarning > 0, and • g3healthMajor = 0, and • g3healthMinor = 0	Warning
• g3healthMajor = 0, and • g3healthMinor = 0, and • g3Warning = 0	Normal
	(1 of 2)

Table 8. Performance data collection change managed node icon states

Result of poll	New icon state
Proxy Agent does not exist or does not respond	Unknown
Connection status is not **up**	Unknown
	(2 of 2)

NMS alert Notification Methods

Introduction

The Performance Management installation process allows you to install a script that forwards alert information to a pager or to email. You can also install add-on software such as TelAlert or Remedy that provide additional methods for notifying you when alerts occur.

Alert Notification Options

The following methods for receiving alert notification are available to you through the NMS:

Table 9. NMS alert Notification Methods

Software	Notification Type	Description
Performance Management	CU Pager	Pages the system administrator and sends a code that identifies the alert.
Performance Management	email	Sends an email message to the system administrator that contains pertinent alert information.
TelAlert	Alpha Page	Pages the system administrator and sends a code that identifies the alarm or error type. The alpha page also confirms when the system administrator received the page. The page repeats until the system administrator responds to the page.
		(1 of 2)

Table 9. NMS alert Notification Methods

Software	Notification Type	Description
TelAlert	Voice Page	Sends a voice page to the system administrator and sends a code that identifies the alert. The voice page also confirms that the system administrator received the page. The page repeats until the system administrator responds to the page.
TelAlert	Audix	Calls the system administrator's audix and leaves a voice message containing alert information.
Remedy	Ticket	Interfaces with Performance Management to provide historical information for alerts.
		(2 of 2)

Set Up Alert Notification

To setup alert notification, identify the notification method that meets your business needs, then complete the following procedure.

1. Select an Alert Notification method.
2. At a UNIX editor, type the following and press **ENTER**:
   /opt/OV/OneVision/bin/Samples

   Result: The system displays a list of script files.
3. Type one of the script file names below:
   - TA_AlphaPage
   - TA_VoicePage
   - TA_Audix
   - CU_Pager
   - Notify_Email
   - ARS_Ticket

   Result: The system displays procedures for the selected script.
4. Complete the procedures included in the file.
5. Write and quit the file.

4 Performance Management Overview

Chapter Contents

Introduction

As one of a collection of Business Communication System (BCS) management applications, the Performance Management system enables you to monitor the performance of the managed nodes (DEFINITY switch) in your DEFINITY system using an industry standard SNMP-based Network Management System (NMS). The system collects switch performance data, primarily usage peaks, from the DEFINITY Proxy Agent through SNMP. Using Performance Management, you can retrieve that performance data and generate various types of reports, which can then be viewed on the screen in various formats or exported to other applications.

Features

Performance Management provides the following capabilities:

- **Data collection**
  Where you specify the type of data, time of collection, and length of storage for data to be collected from each managed node.
- **Exception thresholds**
  Where you specify thresholds, or tolerance levels, for processor occupancy and trunk group grade of service. When the thresholds are exceeded, a performance alert appears on the screen.
- **Performance reports**
  Where you can define what managed nodes and associated components should be tracked, what the report output should look like, and whether the report output should go to the screen, a printer, or a file.

- **Report schedule**
  Where you specify when a report should run, either immediately or at a later scheduled time.
- **Alerting**
  Icons on the screen that indicate any violations of exception thresholds or alerts, such as when the system fails to collect performance data as scheduled, or when the system fails to generate a scheduled report.
- **Graphical User Interface (GUI)**
  A graphic representation of what is going on with the system, including various tools to help you navigate and use the system easily.

Background

Performance Management replaces the DEFINITY Monitor I product. It provides the same capabilities as Monitor I, except for the following reports:

- Force Management Alternatives
- Access Endpoint report
- PRI Endpoint report

System Requirements

The Project Provisioning Package for this release contains the specific recommendations and specifications to plan and install the Performance Management software.

Installation Options

The provisioning package also defines the terms and conditions for the three installation options:

- Customer installation
- Technical Support Center (TSC) installation services
- NetCare® Network Consulting Group installation of a complete turn-key system

Refer to *"About This Book" on page 8* for more information about the Project Provisioning Package.

Hardware Requirements

You should work with your Lucent Account Executive to determine the hardware requirements that your organization needs to meet its business and performance specifications.

Software Requirements

The DEFINITY Performance Management application operates with the following software:

- DEFINITY Proxy Agent, Release 2.0
- DEFINITY Network Management Common Software, Release 2.0
- Network Management System (NMS) platform
- DEFINITY Fault Management, Release 2.0 (optional)

Supported Products

NMS Products

The DEFINITY Performance Management 2.0 product supports the following network management products:

- DEFINITY Proxy Agent 2.0
- DEFINITY Fault Management 2.0

NMS Platforms

The DEFINITY Performance Management 2.0 product supports the following Network Management System (NMS) platforms:

- HP OpenView Releases 4.11, 5.0, and 5.01 installed on Solaris Release 2.5.1

Supported Systems

Release 2.0 of Performance Management only supports DEFINITY G3 PBX release 4 and DEFINITY ECS releases 5 through 6.

Access Performance Management

You should start Performance Management after you complete the installation process to verify that Performance Management is installed correctly.

Procedure

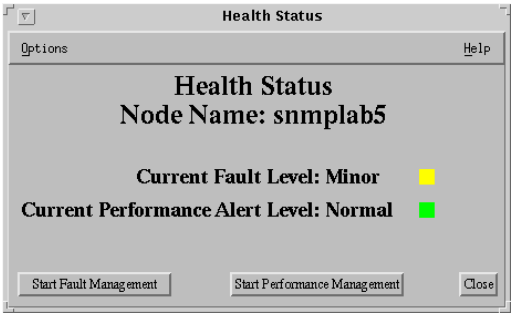
To access Performance Management, do the following:

1. Log in to UNIX.
2. Start the operating system software.
3. At a UNIX editor, type one of the following and press **Return**:
   - For NetView, type **$OV_BIN/nv600**
   - For OpenView, type **$OV_BIN/ovw&**

   Result: The system opens the Network Management System software and displays the **Root** map.
4. Double-click a DEFINITY submap icon.

   Result: The system displays a DEFINITY submap.
5. Double-click a managed node icon.

   Result: If you installed Performance Management ***and*** Fault Management, the system displays the following screen.



6 If the system displays this screen, click **Start Performance Management**.

Result: The Performance Management application starts and displays the Performance Management main window.

Exit Performance Management

To exit Performance Management, do one of the following:

- Click **File > Exit** from the main window of Performance Management
- Exit the NMS session

The system closes Performance Management and any associated open windows. Prior to exiting, Performance Management will check for unsaved changes, and, if any exist, give you the chance to save them.

Exit the NMS session

To exit the NMS session, close all programs associated with the NMS. At the main NMS window, click **Map > Exit.** The system closes the NMS application.

5 Basic Screen Components

Chapter Contents

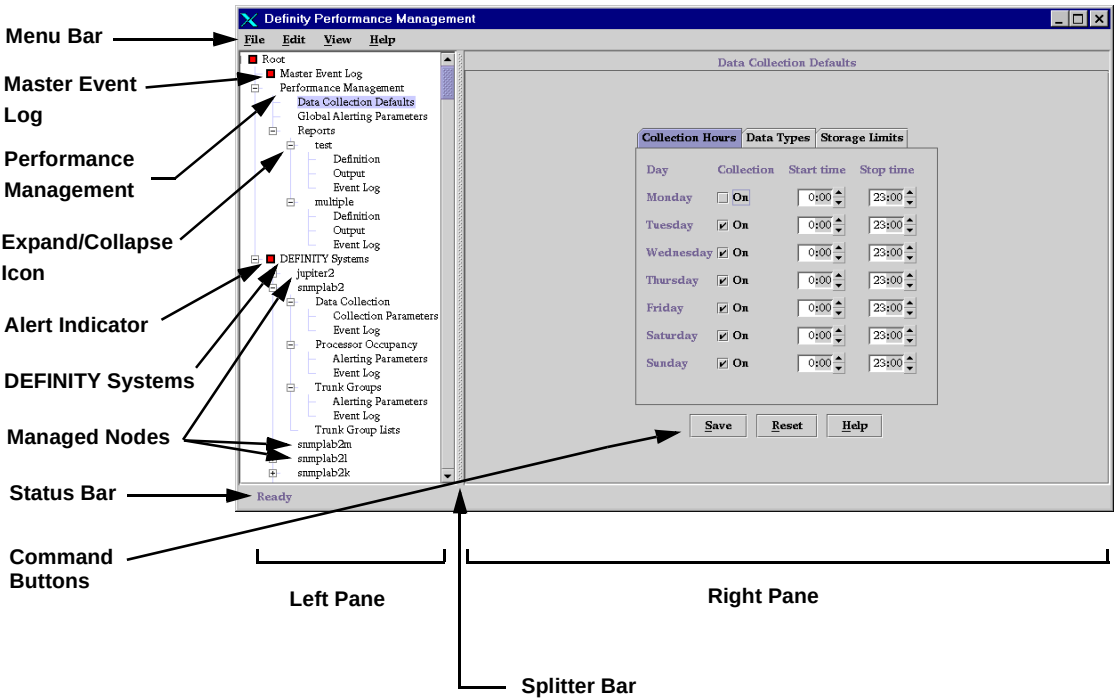
Introduction

Performance Management uses a graphical user interface (GUI) as a way to access the tasks you need to perform in order to measure system performance. The GUI consists of various screens, buttons, and other navigational tools, in conjunction with your mouse, to enable you to access all of the reporting capabilities the system provides.

This chapter describes the basic elements of the Performance Management system that you can see and use in monitoring system performance.

Screen Components

The following sample screen shows the basic screen components of the main window of the Performance Management application. See the table following the screen for a description of each component.


Menu Bar
Master Event Log
Performance Management
Expand/Collapse Icon
Alert Indicator
DEFINITY Systems
Managed Nodes
Status Bar
Command Buttons
Left Pane
Right Pane
Splitter Bar
Definity Performance Management
File Edit View Help
Root
Master Event Log
Performance Management
Data Collection Defaults
Global Alerting Parameters
Reports
test
Definition
Output
Event Log
multiple
Definition
Output
Event Log
DEFINITY Systems
jupiter2
snmplab2
Data Collection
Collection Parameters
Event Log
Processor Occupancy
Alerting Parameters
Event Log
Trunk Groups
Alerting Parameters
Event Log
Trunk Group Lists
snmplab2m
snmplab2l
snmplab2k
Data Collection Defaults
Collection Hours
Data Types
Storage Limits
Day
Collection
Start time
Stop time
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
On
0:00
23:00
Save
Reset
Help
Ready

Component Description

Component Name	Description
Menu bar	Displays pull-down menus for performing basic tasks. Go to *"Menu bar" on page 92* for more details.
Master Event Log	Displays the Master Event Log pane, which shows all events for all managed nodes. Go to *Chapter 8, "Event Log"* for more details.
Performance Management	Displays three nodes for managing the performance of the system.
Expand/collapse icon	Hides or shows more options below the current node. Go to *"Nodes" on page 94*.
Alert indicator	Visual indicator of any system problems. Go to *"Alert Indicators" on page 95*.
DEFINITY Systems	Displays a tree node for all managed nodes.
Managed nodes	Node representing DEFINITY switches. Go to *"Managed Nodes" on page 97* for more details.

Component Name	Description
Command buttons	Buttons that are common on all screens. Go to *"Command Buttons" on page 97* for more details.
Status bar	Indicates the status of the system. Go to *"Status Bar" on page 98* for more details.
Left pane	The left part of the main window that contains icons and nodes. Go to *"Main Window" on page 88* for more details.
Splitter bar	Separates the left and right pane. Go to *"Splitter Bar" on page 98* for more details.
Right pane	The right part of the main window that contains the display screens. Go to *"Main Window" on page 88* for more details.

Main Window

The main window is the initial screen you see when you access Performance Management. The main window has the same look and feel as the Microsoft Windows Explorer tree, where there are two sides to the screen, a left (pane) and a right side (pane). The difference is that in Performance Management, the right side displays a display screen related to what is selected in the left side, whereas in Windows the right side displays more directory structure based on what is selected in the left side.

Left Pane

The left side of the main window is a pane that graphically displays the hierarchy of the Performance Management application. It consists of various nodes and alert icons, as shown in the preceding screen. When you can single-click on a node in the left pane, the right pane changes to reflect the corresponding display screen for that selection.

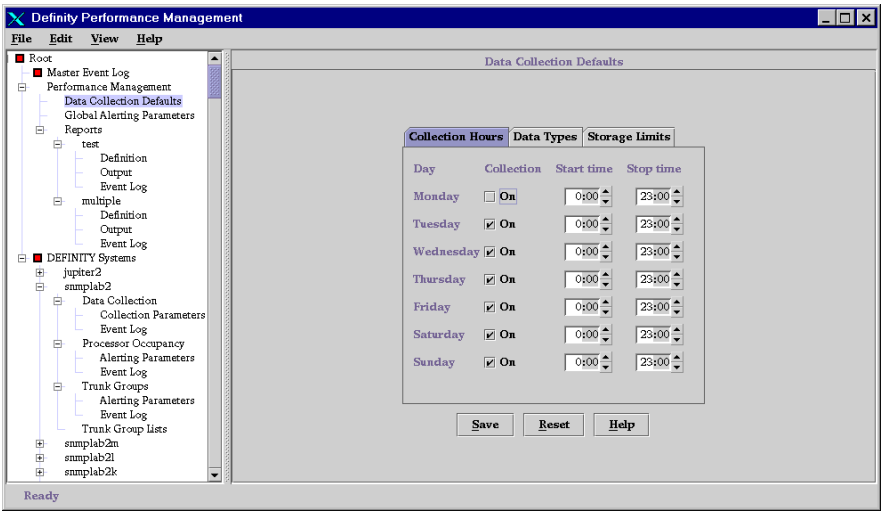
Within the tree, you can click on the plus (+) sign to see the contents for that node, or you can click on the minus (-) sign to hide the contents of the node. In this way you can drill down from a high level to lower levels of options and details.

Right Pane

The right pane is a display screen that changes according to the node or icon selected in the left pane. It is the part of the main window where you specify all of the settings for the system. It can also contain nodes that branch off from whatever is selected in the left pane.

Double-clicking on a node in the right pane does the same thing as single-clicking on a node in the left pane; the corresponding display screen for that selection appears.

For example, if you click the Data Collection Defaults node in the left pane, the right pane displays the Data Collection Defaults pane, as shown below:



Saving Information

Whenever you save any information by clicking the **Save** button, you are saving not only the setting for the currently displayed tab, but all of the current settings for all of the tabs in the display screen.

About Panes

Depending on what you select in the left pane, the right side of the main window (the right pane) can display any of the following specific panes. These panes and examples are described in more detail in the rest of this document as part of the description of the task they correspond to.

Pane	Description
Root	Highest level pane; starting point for using the system.
Master Event Log	Displays the Master Event Log pane that shows all events for all managed nodes.
Performance Management	Contains tree nodes for defining default report parameter thresholds.
Data Collection	Display screen for defining data collection parameters.
Global Alerting Parameters	Display screen for defining alerting parameters used throughout the system.
Reports	Contains a node for each report defined in the system.
Report	Contains nodes for defining a report and viewing its output.

Pane	Description
DEFINITY Systems	Contains a node for each managed node known by Performance Management.
DEFINITY	Contains nodes for setting thresholds to measure the performance of a specific managed node.
Data Collection	Contains nodes for defining data collection parameters for a managed node.
Processor Occupancy	Contains nodes for defining alerting and event log parameters for measuring processor occupancy performance.
Trunk Groups	Contains nodes for defining alerting and event log parameters for measuring trunk group performance.

Menu bar

The options available through the pfmenu bar are described as follows:

Menu	Option	Description
File	New	Creates a new component as appropriate for the task being performed.
	Expand	Expands the selected node on the pane.
	Up One Level	Displays the parent of the selected node. For example, if you the Master Event Log is highlighted, clicking Up one Level will highlight the Root node.
	Exit	Exits Performance Management.
Edit	Delete	Deletes the currently selected component.
View	Refresh	Redraws the screen.

Menu	Option	Description
Help	Topics	NA
	Current Panel	Online help for the currently-displayed pane
	About Definity Performance Management 2.0	Software version and date

Nodes

Nodes represent the options available in your system. There are three basic nodes available from the Root pane. The Root pane is the starting point for performing all Performance Management tasks, since all other nodes branch off from these three nodes. Click once on the Root node in the left pane to expand it to show the following nodes:

Node	Description
Master Event log	Represents the master log of events for all inactive and active objects. See *Chapter 8, "Event Log"* for more information.
Performance Management	Represents the Performance Management application. Expands to show more nodes where you can define system-wide parameters.
DEFINITY Systems	Represents nodes for the DEFINITY managed nodes.

Expandable Nodes

Within the “tree” of nodes and icons in the left pane, you can show (expand) or hide (collapse) the options below the node by clicking on the plus sign or the minus next to the node, where:

- A plus (+) sign means the node is collapsed and can be expanded; clicking on it expands the node to show any sub-components.
- A minus (-) sign means the node is expanded and can be closed; clicking on it collapses all of its sub-components.

Alert Indicators

Alert indicators are visual cues of any problems in the DEFINITY system. Alerting is also used by the NMS to indicate any problems associated with a specific managed node. There are different levels of alerts that have corresponding warnings, as indicated by the shape and color of the alert indicator. You can tell at a glance by looking at the alert indicators in the left pane where problems are and the severity of the problem.

Color Scheme

Changing the colors on your terminal can affect the look of your icons. See your system administrator or account executive for help.

Related Information

See *Chapter 9, "Set Alerting Parameters"* for more alert information.

Alert Levels and Icons

The levels of alerts, in order of increasing severity, are shown in the following table:

Alert Level	Alert Icon you see in left window pane
Warning	
Minor	

Alert Level	Alert Icon you see in left window pane
Major	
Critical	

Managed Nodes

Expanding the DEFINITY Systems node by clicking on it displays all of the nodes for each switch, or managed node, known by the Performance Management system.

Command Buttons

The command buttons that appear at the bottom of the right pane do the following:

Button	Purpose
Save	Updates the database with the current settings. For display screens that have tabs, saves the current settings for all of the tabs, not just the current tab.
Reset	Discards any changes and resets the pane with the most recently saved settings.
Help	Displays online help for the currently-displayed pane.

Status Bar

This is a message area at the bottom of the main window. Depending on the circumstances, it displays a status indicator for any processing that lasts more than two seconds.

Splitter Bar

The splitter bar separates the right and left panes. To change the size of either pane, drag the splitter bar that separates the two sides until the desired size is displayed.

6 Specify Collection Parameters

Chapter Contents

Introduction

One of the features of Performance Management is the ability to track the performance of a managed node through reports you can generate for various aspects of the system. In order to run reports that help track the system, you must first specify the data to collect for those reports.

This chapter describes how to collect report data in the following ways:

- Specify default collection parameters that are used across all managed nodes
- Specify customized collection parameters for a specific managed node
- Specify when data should be collected
- Specify what types of data to collect
- Specify how long collected data should be stored

Saving Changes

You can save all of the collection parameters for all of the tabs one time making the changes to each tab, then click **Save** when you have finished with all of the tab settings.

Specify Default Data Collection Hours

Introduction

This procedure describes how to specify the default days and times Performance Management should collect data for the entire Performance Management system. These are the default values that will used unless custom values have been specified for a specific managed node as described in *"Specify Collection Hours for a Specific Managed Node" on page 104*.

Retrieve Stored Data

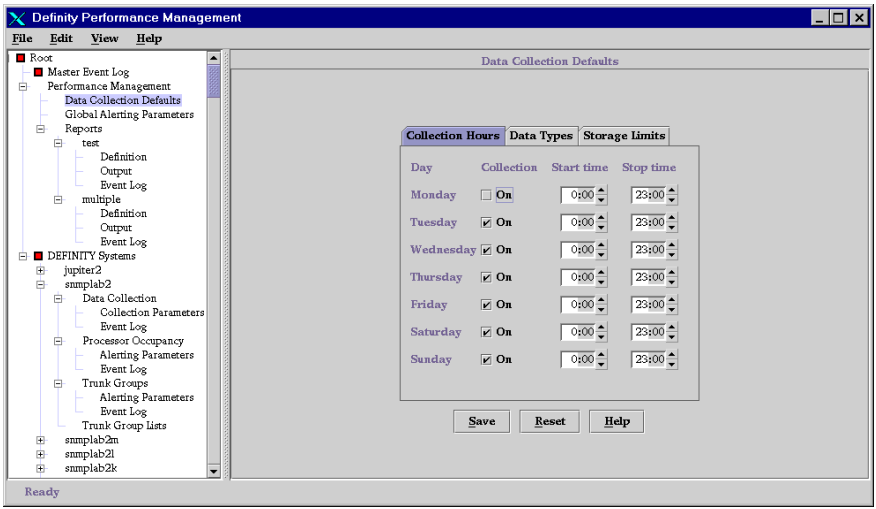
To retrieve stored data, go to *Chapter 7, "Administer Reports"*.

Procedure

To specify default collection hours, do the following:

1 Click **Performance Management > Data Collection Defaults**.

Result: Displays the Data Collection Defaults pane, with the **Collection Hours** Tab displayed.



2 Do any of the following:

- To turn the collection on, put a checkmark in the On box next to the appropriate days of the week by clicking in the box. To turn the collection off, remove the checkmark by clicking on the box that has the checkmark for the appropriate days of the week.
- To specify the start or stop time for the collection, click in the Start or Stop time box and type a new time in military hours, or click the up or down arrow keys to move up or down in hourly increments.

Note: Since collection times are hourly, you cannot specify minutes.

3 Click **Save** to save the settings, or make changes to each tab as necessary and then click **Save**.

Specify Collection Hours for a Specific Managed Node

Introduction

This procedure describes how to specify what days and times Performance Management should collect data for a specific managed node. Once you specify collection hours for a specific managed node, those are the current values until changed.

Retrieve Stored Data

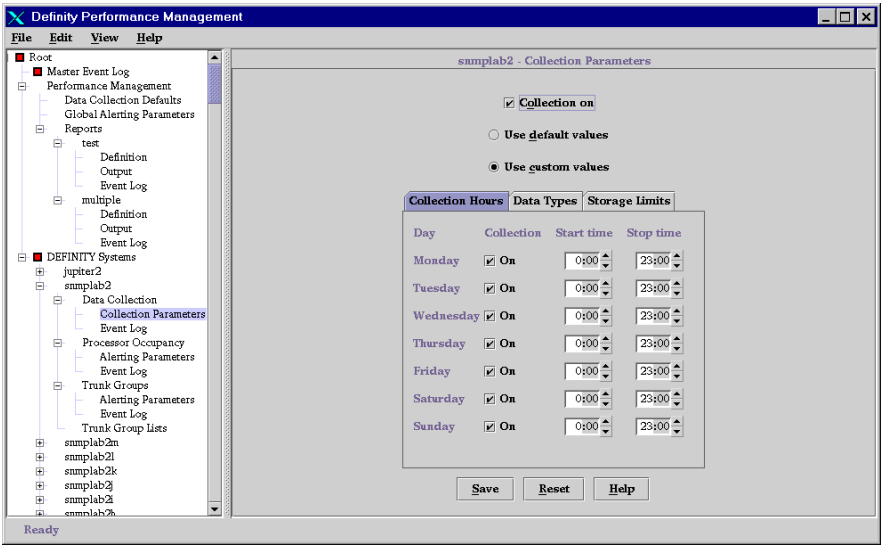
To retrieve stored data, go to *Chapter 7, "Administer Reports"*.

Procedure

To specify collection hours, do the following:

1 Click **DEFINITY Systems >** [**specific DEFINITY**] **> Data Collection > Collection Parameters**.

Result: Displays the Collection Parameters pane for the managed node you want to collect data for.



2 Do you want to collect data for this managed node?

- If yes, put a checkmark in the box next to the Collection on field by clicking **Collection on**.
- If no, leave the box blank.

3 Do one of the following:

- To use the default values set up for the entire DEFINITY system, click **Use default values**. You cannot change any of the collection values if this option is selected.
- To specify specific collection values for this managed node, click **Use custom values**. When you select this option, the collection days are enabled so that you can select which days to collect.

4 Do any of the following:

- To turn the collection on or off for a day of the week, click the On box for any of those days.
- To specify the starting or stop time for the collection, click in the Start or Stop time box and type a new time in military hours, or click the up or down arrow keys to change the time in hourly increments.

Note: You can only specify collection times in hourly increments.

5 Click **Save** to save the settings, or make changes to each tab as necessary and then click **Save**.

Specify Default Data Types

Introduction

This procedure describes how to specify the types of default data to collect for the entire Performance Management system. Although the data types selected here will be the default types for the entire DEFINITY system, you can change the data types for a specific managed node as described in *"Specify Data Types for a Specific Managed Node" on page 109*. Depending on what is supported by the managed node you are trying to measure, you can collect data on the following basis:

- Hourly
- Daily peaks
- Weekly peaks

Retrieve Stored Data

To retrieve stored data, go to *Chapter 7, "Administer Reports"*.

Procedure

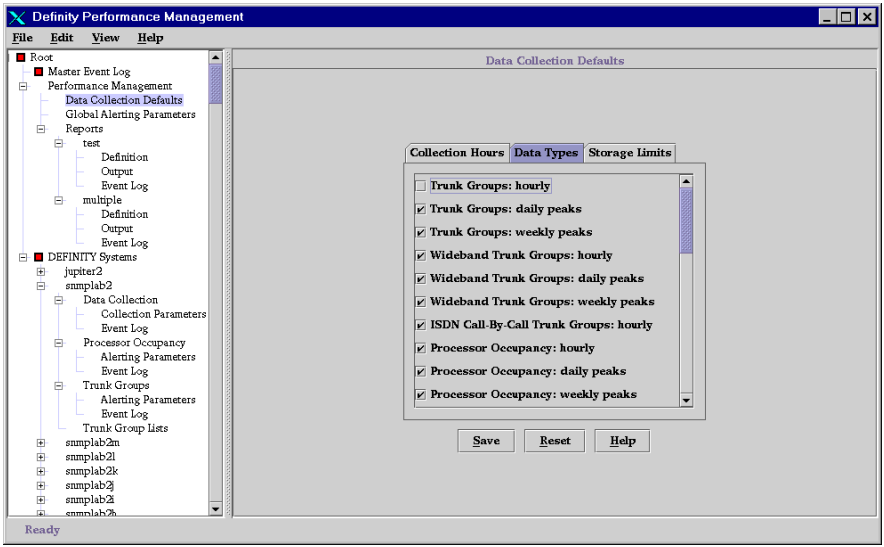
To specify default data types of data to collect, do the following:

1 Click **Performance Management > Data Collection Defaults**.

Result: Displays the Data Collection Defaults pane.

2 Click the **Data Types** tab.

Result: Displays the **Data Types** tab.



3 Put a check mark next to each data type you want to report on by clicking in the appropriate box. Note that for some data types you can also select peaks on an hourly, daily, or weekly basis.

4 Click **Save** to save the settings, or make changes to each tab as necessary and then click **Save**.

Specify Data Types for a Specific Managed Node

Introduction

This procedure describes how to specify the data types to collect for a specific managed node. Depending on what is support by the managed node you are trying to measure, you can collect data on the following basis:

- Hourly
- Daily peaks
- Weekly peaks

Retrieve Stored Data

To retrieve stored data, go to *Chapter 7, "Administer Reports"*.

Procedure

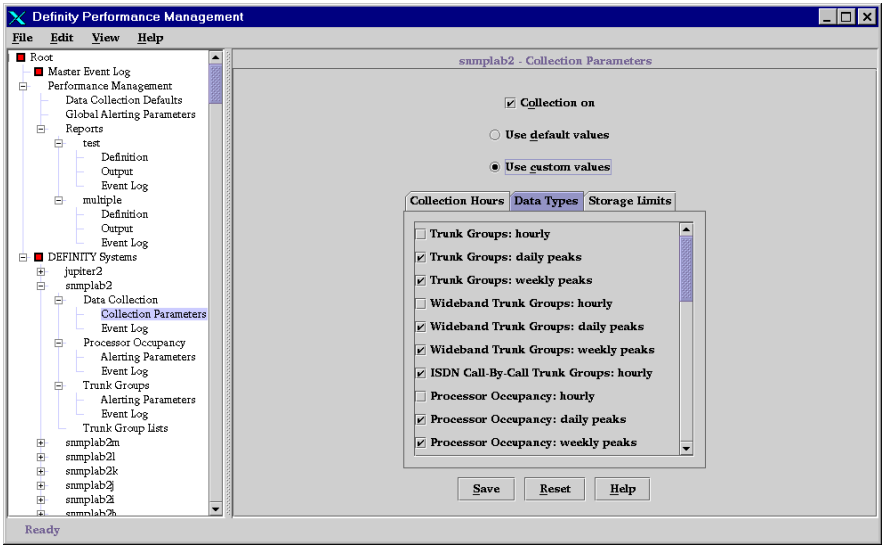
To specify data types for a specific managed node, do the following:

1 Click **DEFINITY Systems >** [**specific DEFINITY**] **> Data Collection > Collection Parameters**.

Result: Displays the Collection Parameters pane for the managed node you want to collect data for.

2 Click the **Data Types** tab.

Result: Displays the **Data Types** tab.



3 Do you want to collect data for this managed node?

- If yes, click **Collection on**.
- If no, leave the box blank. If you select no, you will not have any data to report on.

4 Do one of the following:

- To use the default values set up for the entire DEFINITY system, click **Use default values**. You cannot change any of the collection values if this option is selected.
- To specify specific collection values for this managed node, click **Use custom values**. When you select this option, the collection days are enabled so that you can select which days to collect.

5 Put a check mark next to each data type you want to report on by clicking in the appropriate box. Note that for some data types you can also select peaks on an hourly, daily, or weekly basis.

6 Click **Save** to save the settings, or make changes to each tab as necessary and then click **Save**.

Specify Default Data Storage Duration

Introduction

This procedure describes how to specify system-wide default values for the length of time collected data should be stored. You can specify how long hourly, daily, and weekly data should be stored.

Retrieve Stored Data

To retrieve stored data, go to *Chapter 7, "Administer Reports"*.

Procedure

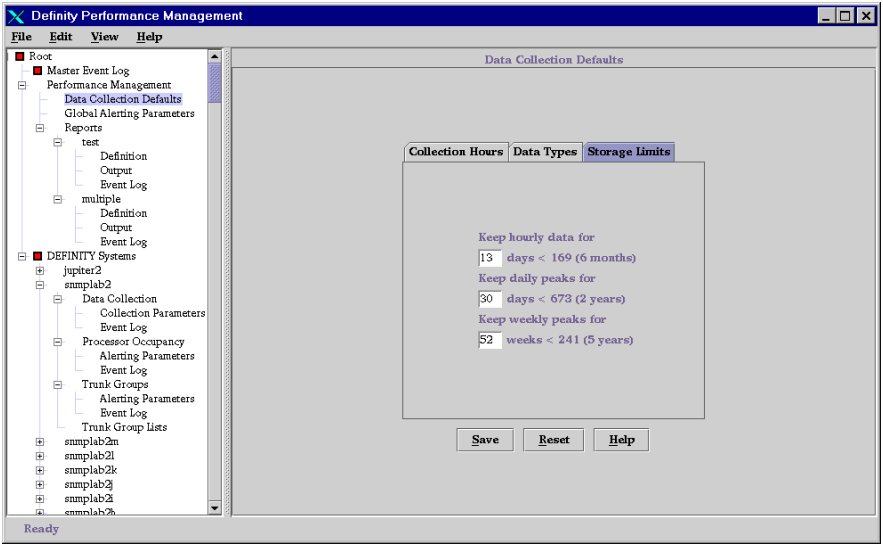
To specify the default length of time collected data should be stored, do the following:

1. Click **Performance Management > Data Collection Defaults**.

   Result: Displays the Data Collection Defaults pane.

2. Click the **Storage Limits** tab.

   Result: Displays the **Storage Limits** tab.



3 Do any of the following:

- To specify how many days to keep hourly data, enter the number of days in the Keep Hourly Data field. Maximum is six months.
- To specify how many days to keep data for daily peaks, enter the number of days in the Keep Daily Peaks field. Maximum is two years.
- To specify how many weeks to keep data for weekly peaks, enter the number of days in the Keep Daily Peaks field. Maximum is five years.

4 Click **Save** to save the settings, or make changes to each tab as necessary and then click **Save**.

Specify Data Storage Duration for a Specific Managed Node

Introduction

This procedure describes how to specify how long collected data should be stored for a specific managed node. You can specify how long hourly, daily, and weekly data should be stored.

Retrieve Stored Data

To retrieve stored data, go to *Chapter 7, "Administer Reports"*.

Procedure

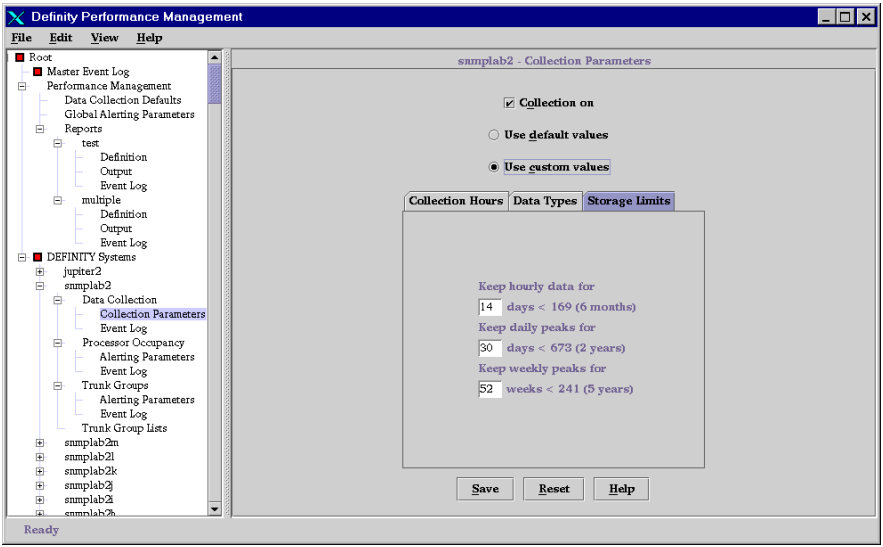
To specify how long collected data should be stored for a specific managed node, do the following:

1. Click **DEFINITY Systems >** [**specific DEFINITY**] **> Data Collection > Collection Parameters**.

   Result: Displays the Collection Parameters pane for the managed node you want to collect data for.

2. Click the **Storage Limits** tab.

   Result: Displays the **Storage Limits** tab.



3 Do you want to collect data for this managed node?

- If yes, put a checkmark in the box next to the **Collection on** field by clicking in it
- If no, leave the box blank.

4 Click **Use custom values** and go to the next step to specify specific collection values for this managed node.

5 Do any of the following:

- For data types for which hourly data is collected, type the number of days to keep the data in the Keep Hourly Data field. Maximum is six months.
- To specify how many days to keep data for daily peaks, type the number of days in the Keep Daily Peaks field. Maximum is two years.
- To specify how many weeks to keep data for weekly peaks, type the number of days in the Keep Weekly Peaks field. Maximum is five years.

6 Click **Save** to save the settings, or make changes to each tab as necessary and then click **Save**.

7 Administer Reports

Chapter Contents

Introduction

The heart of the Performance Management system is the ability to produce reports on various performance aspects of the system. In order to produce a meaningful report, you must define the report, including:

- What data fields to report on
- What managed nodes and components to report on
- What time period to report on
- What the report should look like
- Where the report should go (screen, printer, or various file types)
- When the report should run

This chapter describes how to define, store, and run a Performance Management report.

Getting Started

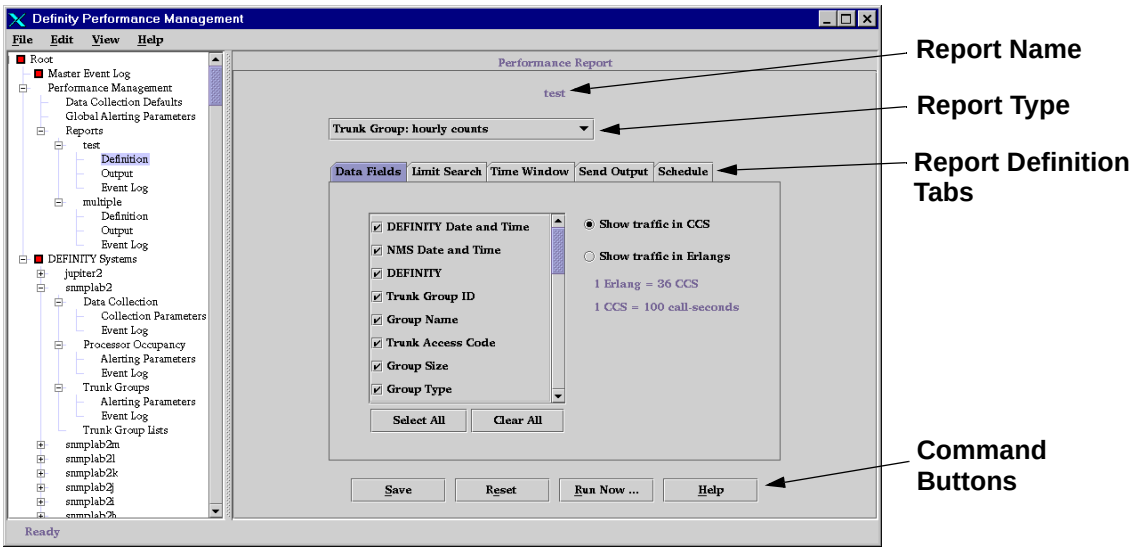
Overview

The following steps highlight the flow of tasks you need to perform in order to create, define, and store a Performance Management report.

Task (in order)	Described in...
Set up collection parameters	*Chapter 6, "Specify Collection Parameters"*
Create the report	*"Create a New Report" on page 124*
Define report parameters: • what data to report on • time span to report on • when report should run • format of report, such as a table or chart • where report output should go	*"Define Data Fields" on page 126* *"Select Managed Nodes" on page 139* *"Specify Report Interval" on page 147* *"Schedule a Report" on page 151* *"Set up Report in Table Format" on page 154* *"Set up Report in Chart Format" on page 157* *"Define Destination of Report Output" on page 163*
Run the report	*"Run a Report" on page 167*
View report output	*"Display Report Output" on page 170*
Handle the output	*"Options from a Displayed Report" on page 131*

Report Definition Pane

The Report Definition pane is the starting point for defining report parameters. The report name, report type, report definition tabs, and command buttons are always displayed on this pane.



Tab Description

Using the report definition tabs, you can do the following:

Tab	Description
Data fields	Determines which data fields to report on
Limit Search	Determines which managed nodes and components to report on
Time Window	Determines period of time to include in a report
Send output	Determines what the output of the report will look like and where report will appear
Schedule	Determines when a report will run at a later time

Command Buttons

The four buttons that appear at the bottom of the Report Definition pane are available regardless of the tab you are in, and they all perform the same function for each tab, as described in the following table:

Button	Purpose
Save	Saves the current settings.
Reset	Discards any changes to the current tab and any other unsaved changes to any other tabs for the report, and returns to the original values for the report.
Run Now	Runs the report immediately, using the current report definition parameters.
Help	Displays online help.

Create a New Report

Procedure

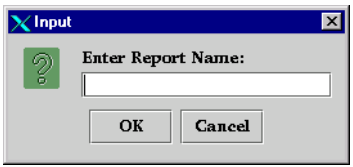
To create a new report, do the following:

1. Click the **Reports** node.

   Result: The Reports node is highlighted.

2. From the File menu on the Main Performance Management window, click **File > New**.

   Result: Displays a pop-up window for entering the report name.

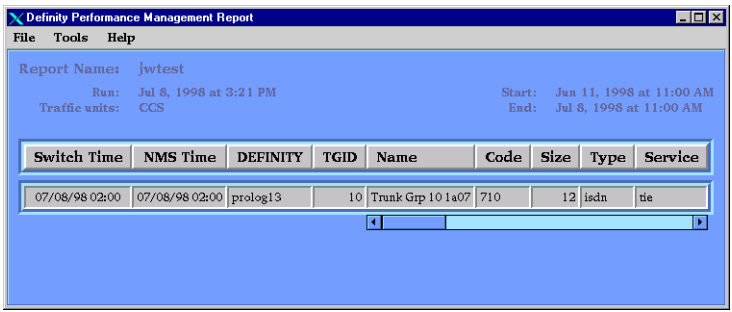


3. Type the name of the report. This is the report name as it will appear throughout the Performance Management system.
4. Click **OK**.

   Result: Displays the Report Definition Pane, which is the starting point for defining various aspects of the report, such as what report types and data fields to report on. The report name is at the top of the pane.

5 Click **Run Now** to run the report now. The report will print to the screen. If the report needs any changes, change the report definition parameters as listed in *"Getting Started" on page 120*.

Result: Displays the report based on the current report definition parameters, as shown in the following example.



Define Data Fields

This procedure describes how to specify what data fields to include in the report. You can also specify the units of traffic intensity to include.

About Secondary Data Fields

Some report types can have secondary data fields. For example, each routing pattern contains several trunk groups, and there are secondary data fields associated with each trunk group. The report will show this secondary data in a second table or graph below the primary data. On the **Data Fields** tab, primary data fields appear at the top of the list, and secondary fields appear at the bottom of the list.

Report Types

The following table lists primary and secondary report types:

Primary Report Type	Secondary Report Type	Time Scale
Attendants	Attendant positions	Hourly counts, daily peaks, weekly peaks
Hunt groups		Hourly counts, daily peaks, weekly peaks
Port network nodes		Hourly counts, daily peaks, weekly peaks
Processor occupancy		Hourly counts, daily peaks, weekly peaks

Primary Report Type	Secondary Report Type	Time Scale
Routing patterns	Routing pattern trunk groups	Hourly counts, daily peaks, weekly peaks
Security violations	Port type detail	Daily counts
Switch node links		Hourly counts, daily peaks, weekly peaks
Tone receivers	Tone receiver PN port detail	Hourly counts, daily peaks, weekly peaks
Trunk groups		Hourly counts, daily peaks, weekly peaks
Trunk groups, ISDN PRI	Service and feature detail	Hourly counts
Trunk groups, wideband		Hourly counts, daily peaks, weekly peaks
Trunks, lightly-used		Daily counts
Trunk outages		Daily counts

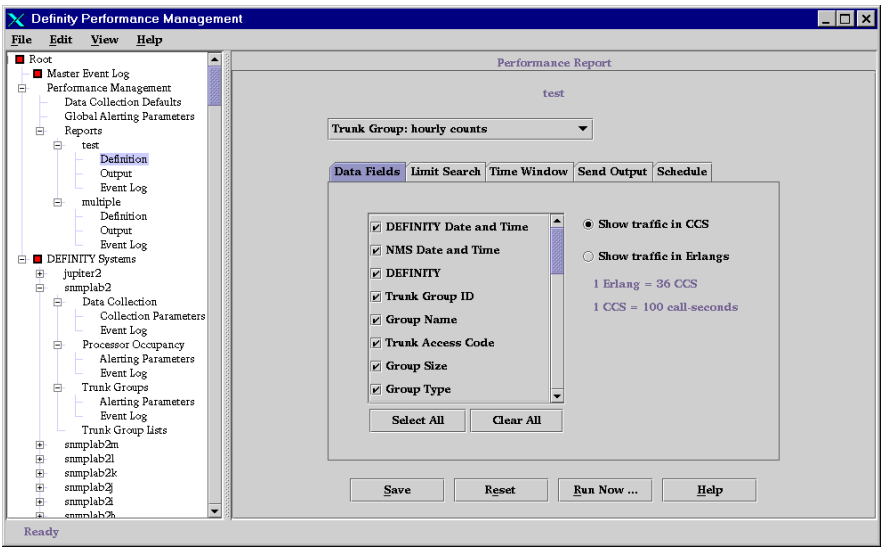
Procedure

To define data fields for a report, do the following:

1 Select **Performance Management > Reports >** [**Report name**] **> Definition**.

Result: Displays the Report Definition Pane for the report. The **Data Fields** tab is automatically selected. The left part of the tab contains all of the

data fields for that report; the right part specifies units of traffic intensity.



2 The field at the top of the pane lists the report (data) type, or DEFINITY component. Select the report type to report on from the pull-down list by clicking in the box next to the appropriate report type.

Note: Make sure that the data type you select here is also the data type that you are collecting data on as described in *Chapter 6, "Specify Collection Parameters"*. The data selected here is also the data available when you set up the format in the **Send Output** tab. The data can also be one of the types that you have already collected data on.

Result: The list of data fields in the left part of the pane changes according to the report type selected.

3 In the lower left part of the pane, put a checkmark next to each data field you want to report on.

- To select all data fields, click **Select All**.
- To clear all data fields so that none are selected, click **Clear All**.

You must select at least one data field. The data fields selected here will be the columns in the report. A report normally includes all of the key fields that identify the data, including DEFINITY name, date, time, and applicable ID, such as trunk group ID.

4 In the right box, select how traffic intensity (for example, trunk group usage or attendant talk time) should be measured by clicking in either the Show traffic in CCS field or the Show traffic in Erlangs field.

Note: CCS = hundred call-seconds; one Erlang = 36 CCS.

5 Click **Save** to save the settings.

6 Do one of the following:

- To run the report immediately using the system defaults, click **Run Now**.

Result: Displays the report on your screen using the default report parameters. To make any changes, go to the next step.

- To set up report parameters before running the report, click the **Send Output** tab and change any parameters as needed.

Result: Displays the **Send Output** tab.

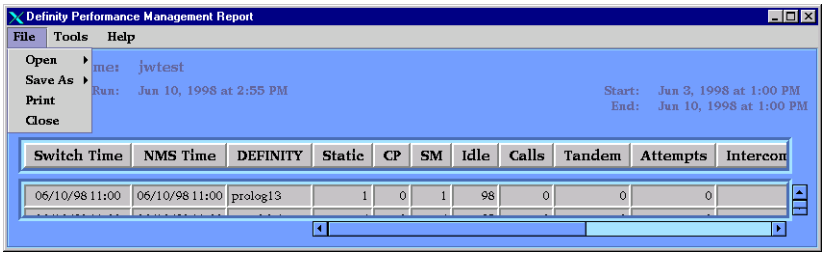
Options from a Displayed Report

You have several options once you have a report displayed on your screen. You can:

- Change the sort order of a table
- Change the format of the report from a table to a chart or vice versa
- Print the report
- Save the report as a file
- If there is secondary data, switch between views of primary and secondary data

Procedures

To perform any of the options from a displayed report, use the following table:



To...	Do this	Result
Select primary or secondary data, if the **Primary** button displays. See *"About Secondary Data Fields" on page 126* for secondary data field details.	Click **Primary** and select data from the list of options.	The data you select will appear in the report.
Change the sort order	From the Tools menu, click **Sort**.	Displays the Sort Properties window, where you can define the order in which the properties of the report will display. Go to *"Set up Report in Table Format" on page 154* for more detail. You can also change the sort order by clicking on the table heading on the report itself. That heading will be the first type of data to sort on.

To...	Do this	Result
Change the report format	From the File menu, click **Open >** [**Chart or Table**].	If **Chart** is selected, displays Chart Properties window. Go to *"Set up Report in Chart Format" on page 157* for more detail. If **Table** is selected, changes report output to a table using the sort values defined in the **Send Output** tab. Go to *"Set up Report in Table Format" on page 154* for more detail.
Print the report	From the File menu, click **Print**.	Gives the option to print an image of the report or the report. Go to *"Print a Report" on page 134*.
Save the report as a file	From the File menu, click **Save As >** [**HTML or ASCII**]. If saving as ASCII, you can also select a field separator, such as a semicolon or a colon. The separator is a single character that separates fields on a table.	Saves output of report in selected file type. Displays confirmation window with path and file name of report.

Print a Report

This procedure describes how to print so that the printed report will appear as it displays on the screen (as a report image) or in a tabular format. Although there are several ways to print a report, this procedure explains how to print a report so that the printed report looks just like it does on the screen. See *"Define Destination of Report Output" on page 163* for other methods of printing a report.

Prerequisites

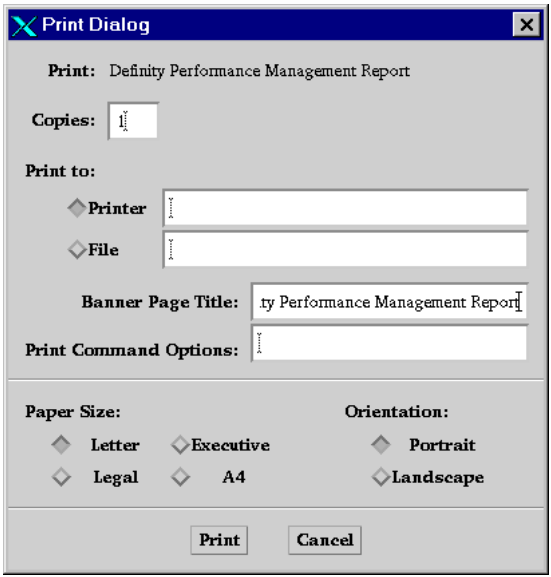
- Make sure your printers are set up and working properly, and that you have a PostScript printer in order to print a report image.
- If you do not have a working knowledge of UNIX print commands, get your UNIX administrator to help you with this procedure.

Procedure

To print a report on a printer, do the following:

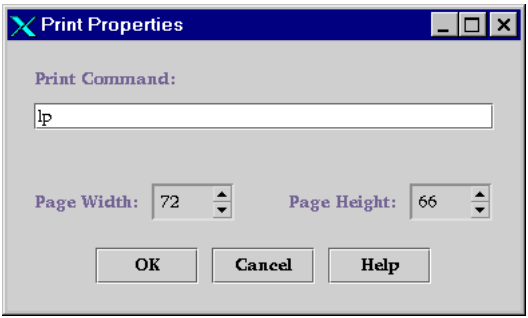
1. Display the report on your screen as described in *"Define Destination of Report Output" on page 163*.
2. Do one of the following:
   - To print the report as it appears on the screen, select **File > Reports > Print > Image**. The Print Dialog box displays. Go to step 3.
   - To print the report in a table format regardless of the way it looks on the screen, select **File > Reports > Print > Report**. The Print Properties window displays. Go to step 4.

3 To define printer detail from the Print Dialog window, enter the settings as described in the following table and click **Print**. If necessary, consult with your UNIX system administrator for system-specific information. After you click **Print**, the report will print on the designated printer.



Field	Description
Copies	Number of printed copies.
Printer	For specifying a UNIX print command. For example, the following command will produce a PostScript output file: prt -d 30N68 -1 raw
File	For creating a postscript file, using UNIX conventions.
Banner Page Title	Specifies what will appear at the top of the page of the report.
Print Command Options	For specifying additional print options.
Paper Size/Orientation	Specify size of paper to print on and whether to print in portrait or landscape mode.

4 To define printer detail from the Print Properties window, change the settings as described in the following table and click **Close**. After you click **Close**, the report will print based on the UNIX print command you specify. These values are usually set up by your UNIX system administrator, but you can change them here.



Field	Description
Print Command	The UNIX print command the system will use to print the report.
Page Width	The width of the report. The default is 72 characters for portrait mode.
Page Height	The height of the report. The default is 66 characters for portrait mode.

Select Managed Nodes

This procedure describes how to select which managed nodes in the Network Management System you want to report on. If the managed nodes have any corresponding components, you can also select which components of each system to report on.

Procedure

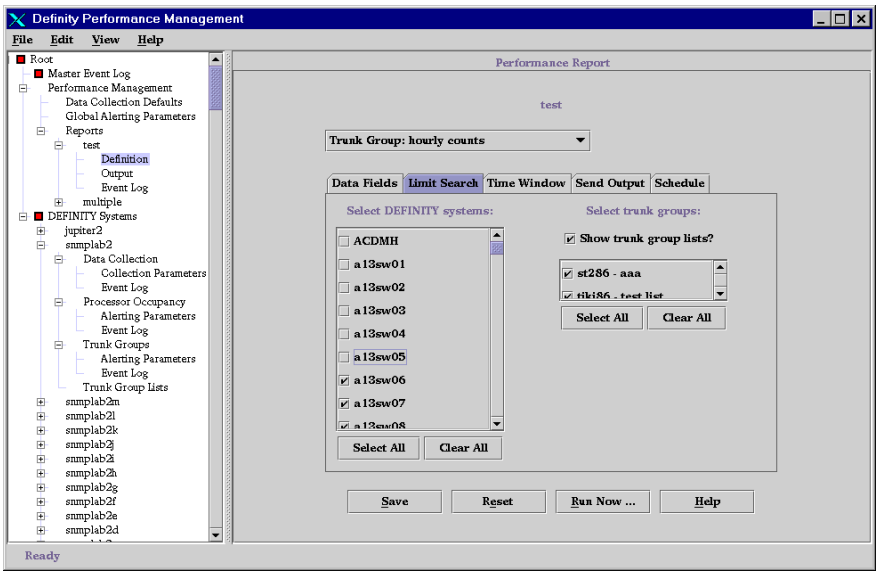
To specify which managed node to report on, do the following:

1 Click **Performance Management > Reports >** [**Report name**] **> Definition**.

Result: Displays the Report Definition Pane for that report. The **Data Fields** tab is automatically selected.

2 Click the **Limit Search** tab.

Result: Displays the **Limit Search** tab, which lists all of the managed nodes known to the Network Management System.



3 In the Select DEFINITY systems box, put a checkmark in the box next to each DEFINITY system you want to report on.

The default is all systems. You can choose any combination, but at least one system is required.

Result: If the managed node you checked has individual components, a list of those components displays in the right side of the pane. See the table following this procedure for a list of report types and corresponding components.

4 For each system selected, are there any components listed in the right side of the pane?

- If yes, go to the next step.
- If no, go to step 7.

5 If the managed node has associated individual components for the report type selected, such as tone receiver types, select which components to report on:

- To select individual components, put a checkmark next to the desired component in the selection list. The default is all components.
- If you are reporting on a trunk group, go to the next step.
- To select all components, click **Select All**.
- To clear all components so that none are selected, click **Clear All**.

For additional details about components, see the table *"Report Type and Component List" on page 142* for a list of report types and corresponding components.

6 If you are reporting on trunk groups and if there are any trunk group lists defined for that managed node, you can select an individual, multiple, or any combination of trunk group lists by clicking on the **Show trunk group lists**

button. If you choose this option, a list of any predefined trunk group lists will display. See *"Create and Modify a Trunk Group List" on page 143* for trunk group list details.

7 Click **Save** to save the settings.

Report Type and Component List

The expanded component selection list shows each component identifier with the name of its managed node. The following table lists the reports types and related component information:

Report Type	Component Information	Example
Attendants	None	none
Hunt groups	Hunt group number and name	Mercury-3 (Hot line)
Port network nodes	Port network number	Mercury-4
Processor occupancy	None	None
Routing patterns	Routing pattern number	Mercury-2
Security violations	None	None
Switch node links	Two switch node numbers	Mercury-2/3
Tone receivers	Tone receiver type	Mercury-DTMF
Trunk groups and trunks (five report types)	Trunk group number and name	Mercury-29 (Portland)

Create and Modify a Trunk Group List

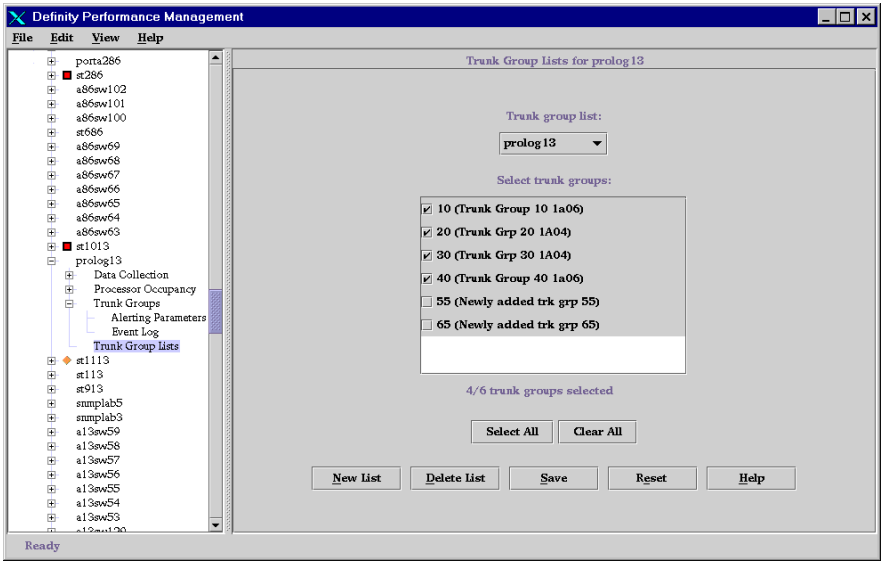
Trunk group lists are useful if you have a large number of trunk groups to manage and you want to streamline the process of setting up a report to be generated. For example, you can specify that the same trunk group list be used for several report definitions. Changing the trunk group list will then change all reports using the list. This procedure describes how to create, modify, and delete a trunk group list.

Create a List

To create a new trunk group list, do the following:

1 Click **DEFINITY Systems >** [**specific DEFINITY system**] **> Trunk Groups > Trunk Group Lists**.

Result: Displays Trunk Group List panel.



2 Click **New List**.

Result: Displays the Input window.

3 Type the name for the new list and click **OK**.

Result: That name appears at the top of the pane in the Trunk Group List field and in the list of available trunk group lists when selecting a trunk group to report on.

4 In the list of selectable trunk groups, put a checkmark next to each trunk group you want in the list by clicking on the trunk group name.

- To select all trunk groups, click **Select All**.
- To clear the list, click **Clear All**.

Result: The number of trunk groups selected is automatically updated below the list of trunk groups.

5 Click **Save** to save the settings.

Result: That list can now be used as part of the process of selecting a managed node to report on.

Modify a List To modify or delete a trunk group list, do the following:

1 Click **DEFINITY Systems >** [**specific DEFINITY system**] **> Trunk Groups > Trunk Group Lists**.

Result: Displays Trunk Group List panel.

2 In the Trunk Group list field, scroll through the list and select the name of the list to be modified.

Result: The trunk groups defined for that list displays.

3 Do one of the following:

- To modify the list of trunk groups, select or de-select the trunk groups to be included for the list.
- To delete the entire trunk group list, click **Delete List**.

4 Click **Save** to save the settings.

Specify Report Interval

This procedure describes how to specify the period of time in which to capture data that will be displayed on a Performance report. There are two types of time periods to report on:

- A fixed time period, such as a report that covers a specific period of time for a specific date range
- A moving time period, such as a report that runs every Sunday night and includes data for the preceding week

Procedure

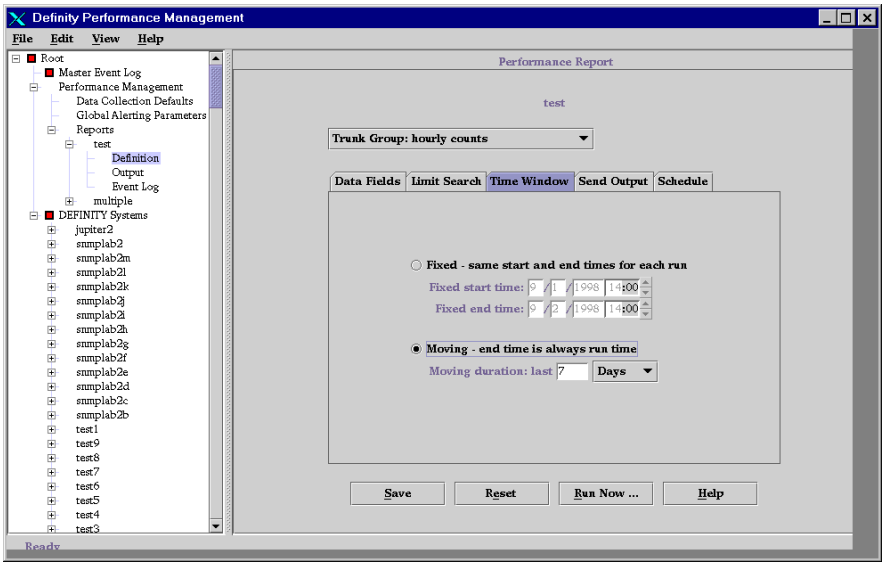
To specify the time span in which to capture data, do the following:

1 Select **Performance Management > Reports >** [**Report name**] **> Definition**.

Result: Displays the Report Definition Pane for that report. The **Data Fields** tab is automatically selected.

2 Click the **Time Window** tab.

Result: Displays the **Time Window** tab.



3 Select one of the following options:

- To run a report one time for a specific period of time for a specific date range, click the **Fixed** button and type the start and end date and time in the respective fields. Type the time in military format.

- To run a report periodically, for example, at the end of every week, click the **Moving** button and type the time span that you want to report on in the time field, or click the arrow button to change the hours.

  You can also change the increments of time from the default of Hours to Days or Weeks as appropriate by clicking the down arrow and selecting the desired increment.

  The end time is the time when the report runs; the start time is the end time minus the number of hours specified in the Hours field.

4 Click the Send Output tab and make sure the output destination is the screen. Click **Run Now** to see how the report looks on the screen.

5 Go to *"Define Destination of Report Output" on page 163*, then *"Schedule a Report" on page 151* for scheduling information.

Example 1

To set up a report that runs once a week on Sunday night at midnight and reports on the system for the preceding week, you would do the following. This example assumes you have defined what data to include on the report:

1 From the Time Window tab, click the **Moving** button.

2 Type 168 in the Hours field.

3 Click **Run Now** to see how the report looks on the screen.

4 If the report does not display on your screen, go to the Send Output tab and make sure **Screen** is selected. Once you are satisfied with the output, select another output destination on the Send Output tab according to the instructions in *"Define Destination of Report Output" on page 163*. Reports scheduled to run at a later time cannot be sent to your screen.

5 Click the **Schedule** tab.

6 Click **Run weekly at** and type **Sun** in the first field and **0:00** in the second field, if not already there. See the directions in *"Schedule a Report" on page 151* for more scheduling information.

7 Click **Save** to save the settings.

Exampel 2 To set up a report that covers an entire day, enter the date for the day to report on in the Fixed start time and enter 00:00 in the time field, then enter same date for the Fixed end time, and enter 23:00 in the time field. The report will cover the entire 24 hours for that day.

Schedule a Report

This procedure describes how to schedule when a report should run at a later time, such as weekly at a specific time.

When to Use

Use this procedure when you want to schedule a report to run at a later time rather than right now. To run a report immediately, see *"Run a Report" on page 167*.

Related Information

To view or change the rest of the report definition parameters, see the following:

- *"Define Data Fields" on page 126*
- *"Select Managed Nodes" on page 139*
- *"Specify Report Interval" on page 147*
- *"Set up Report in Table Format" on page 154*
- *"Set up Report in Chart Format" on page 157*
- *"Define Destination of Report Output" on page 163*

Restriction

You cannot run a report at a later time and send its output to the screen; its output must go to a file or a printer. See *"Define Destination of Report Output" on page 163* for more information.

Procedure

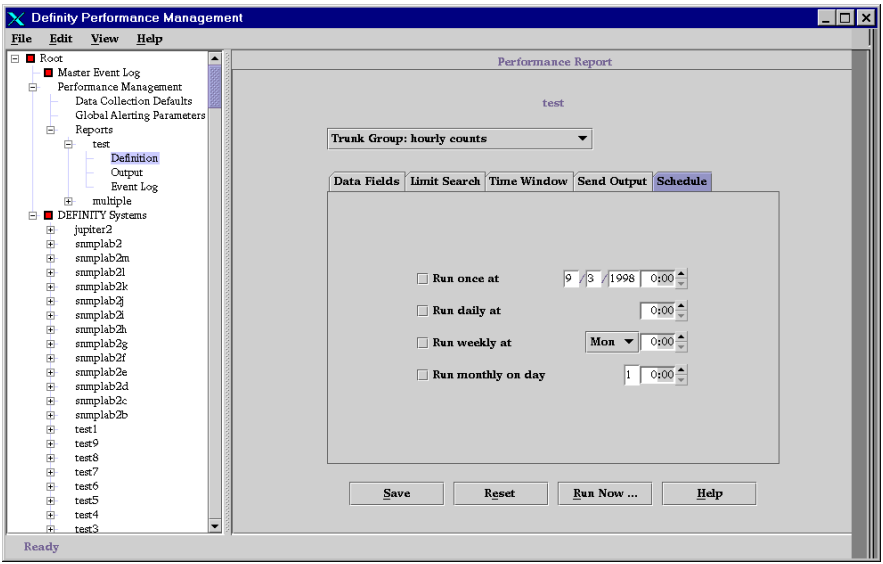
To define when a report should run, do the following:

1 Select **Performance Management > Reports >** [**Report name**] **> Definition**.

Result: Displays the Report Definition Pane for that report. The **Data Fields** tab is automatically selected.

2 Click the **Schedule** tab.

Result: Displays the **Schedule** tab.



3 Select one of the following:

To run a report...	Check this box	And type this in the corresponding fields...
One time at a specific date and time	**Run once at**	The date and hour you want the report to run.
Daily	**Run daily at**	The hour the report should run.
Weekly	**Run weekly at**	The day and hour the report should run.
Monthly	**Run monthly on day**	The day of the month and the hour the report should run.

4 Go to *"Define Destination of Report Output" on page 163*.

Set up Report in Table Format

This procedure describes how to set up a report in a tabular format. You can specify the sort order of up to three fields on a table in ascending or descending order.

Procedure

To set up a table in tabular format, do the following:

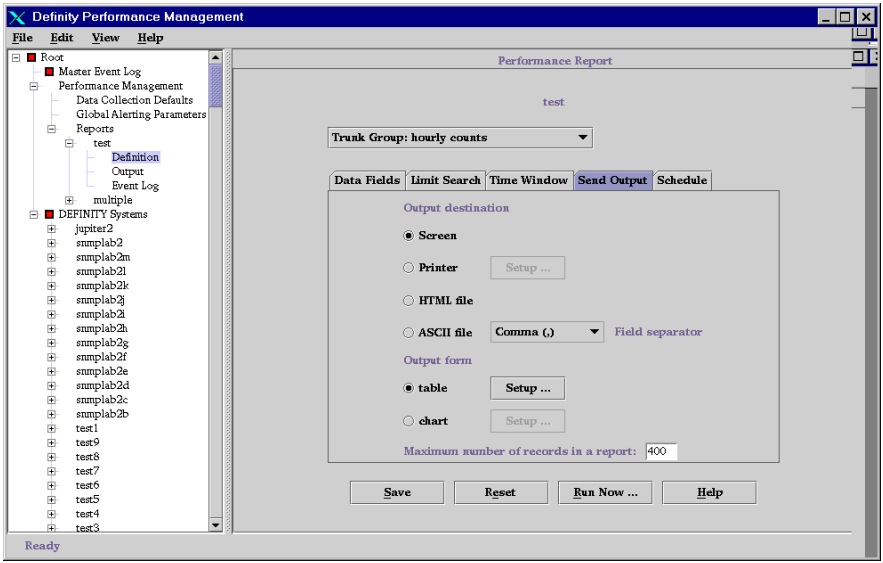
Note: The sort properties defined here stay with the report regardless of its output.

1. Click **Reports >** [**report name**] **> Definition**.

   Result: Displays the Report Definition Pane for that report.

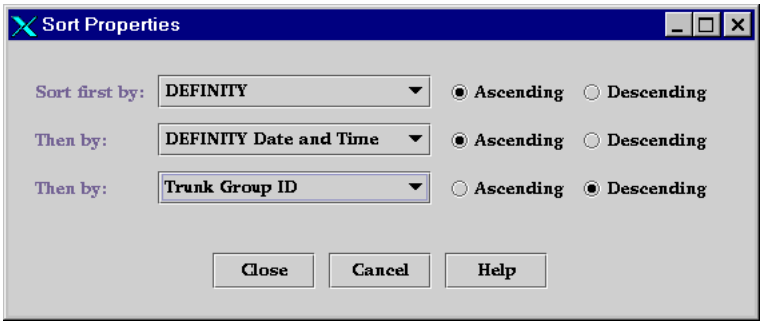
2. Click the **Send Output** tab.

   Result: Displays the **Send Output** tab.



3 Click **table**, then the **Setup** button next to it.

Result: Displays the Sort Properties window, where you can define the order of the rows as they appear on the report.



4 In the three sort fields, select the three fields to sort on, in either ascending or descending order (alphabetical order, from A to Z, or numerical from large to small counts). These are the fields you selected on the **Data Fields** tab for this report.

5 Click **Close**.

Result: The Sort Properties window disappears, and the Report Definition pane is displayed.

6 To run the report, see *"Run a Report" on page 167*.

Set up Report in Chart Format

This procedure describes how to set up a report to display in a chart format. You can specify the type of chart, its contents, and customize its appearance.

Prerequisites

The report must already be created in the Performance Management system. See *"Create a New Report" on page 124* for creating a report. Also, you should be familiar with setting up a chart with an X and Y axis.

Procedure

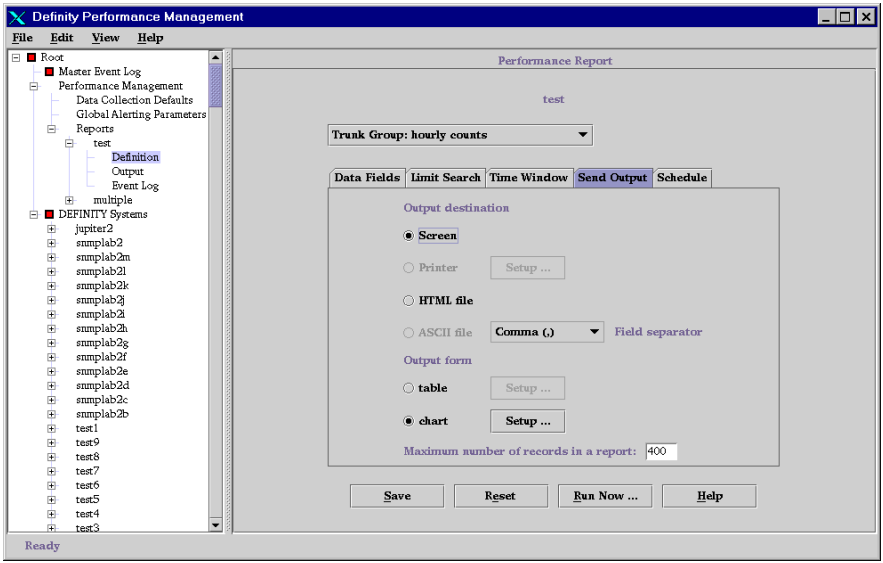
To set up a report in a chart format, do the following:

1. Click **Reports >** [**report name**] **> Definition**.

   Result: Displays the Report Definition Pane for that report.

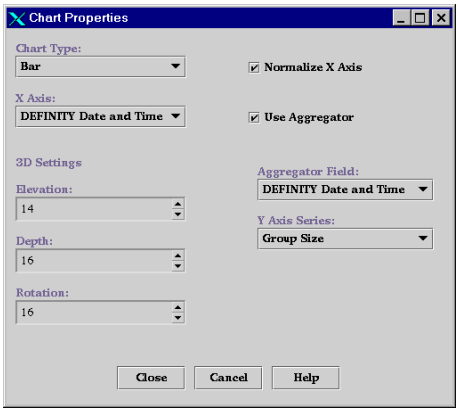
2. Click the **Send Output** tab.

   Result: Displays the **Send Output** tab.



3 Click **chart**, then the **Setup** button next to it.

Result: Displays the Chart Properties window.



4 In the Chart Type field, select the type of chart: line graph, bar chart, stacked bar chart, or pie chart.

5 Click the Normalize X Axis field to eliminate gaps where no data is available for reporting.

For example, if you plot time along the X axis and you collect data only during business hours, there will be gaps on the chart for nights and weekends. Clicking in this field will eliminate the gaps, so that 6 pm Friday is followed immediately by 8 am Monday.

6 Optionally, click the Use Aggregator field to select another key field, also called an aggregator field. If you use an aggregator, you can only choose one field for the Y axis. If you do not use an aggregator, you can choose up to 10 Y-axis series as listed in the Y Axis Series field.

   For example, you could plot the date and time on the X axis of a line graph, and click Use Aggregator for a managed node (DEFINITY switch). The chart would create a Y series for each managed node selected. See the sample following this table.

   - If you click the Use Aggregator field, select an aggregator field from the selection list in the Aggregator field.

7 In the X axis field, select a key field to plot on the horizontal axis. For example, this can be a record identifier, a managed node name, or a trunk group ID. The X axis contains the key fields selected on the **Data Fields** tab on the Report Definition pane.

8 To use 3-dimensional (3D) effects, set the elevation and rotation to determine the apparent position of the viewer:

   - Set the elevation as high as 45 degrees to show a 3D graph as it would appear from above.
   - Set the 3D depth as a percent of the chart width.
   - Set the rotation to show the graph from right or left.

9 Click **Close**.

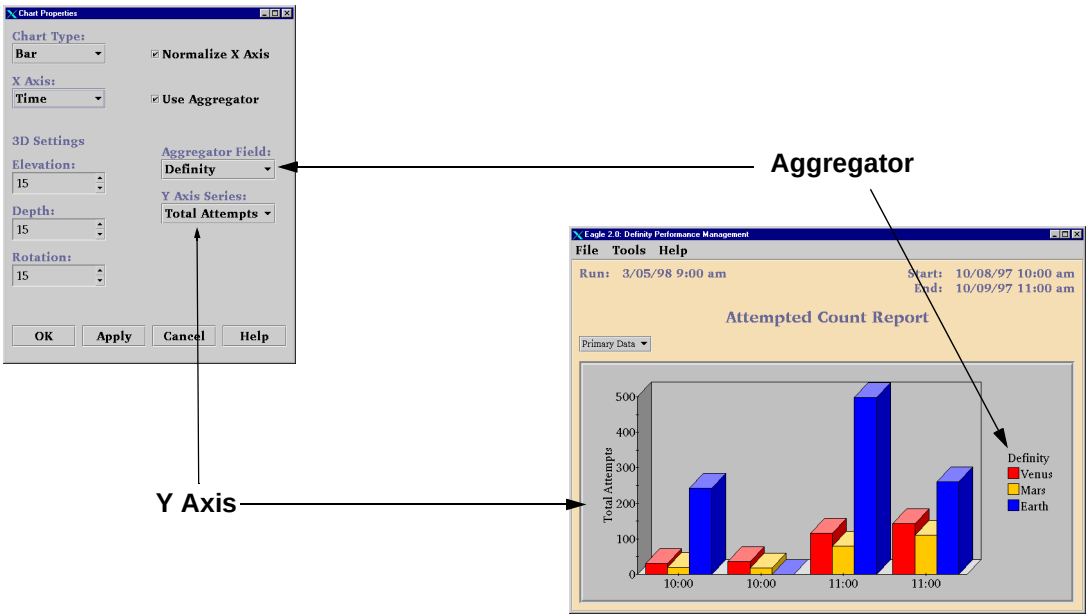
   Result: The Report Definition pane reappears.

10 Click **Save** to save the settings.

11 To run the report, see *"Run a Report" on page 167*.

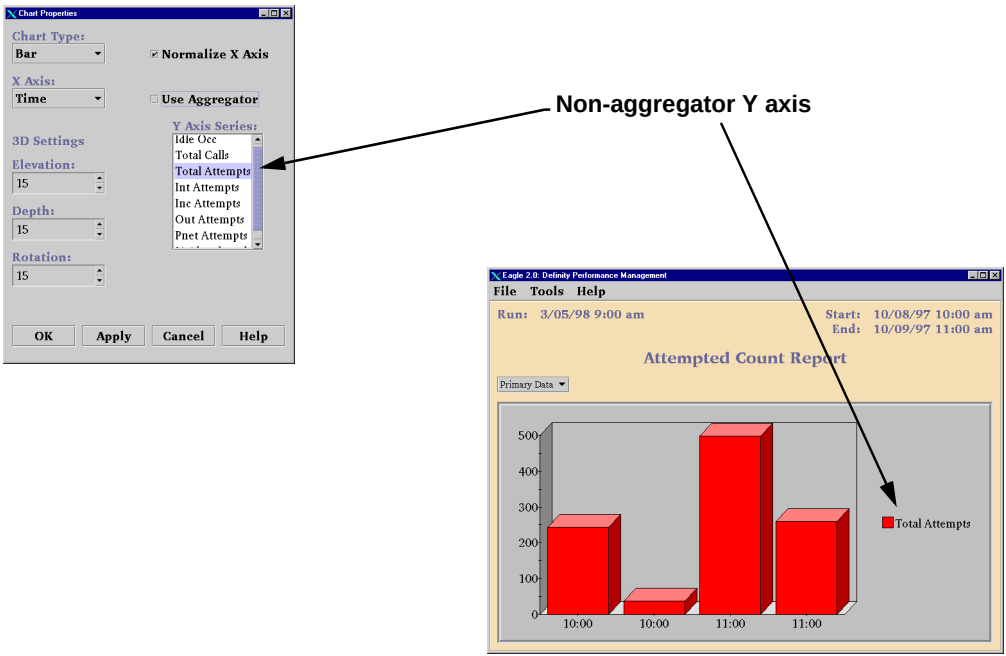
Sample Chart Using Aggregator

The following sample windows show chart properties using an aggregator and the output of those properties:



Sample Chart without Aggregator

The following sample windows show chart properties without an aggregator and the output of those properties:



Define Destination of Report Output

This procedure describes how to define where the output of a report should go. You can send the output to:

- Your screen
- A printer
- An HTML or ASCII file to be viewed or printed later

Suggestions for Type of Output

Send the report to an HTML file when you want to view the report with a browser such as Netscape or Internet Explorer. The report can be printed from the browser. Note that you should use a local browser to view the HTML file.

Note: If you want to view a report in HTML format using a local browser such as Netscape, and you are running on Solaris, you need to click the **Setup** link that displays at the bottom of the the browser window when you try to view the file. This link connects you to a Java plug-in that is necessary for viewing the file. If running in a Windows environment, you will be automatically prompted to select a plug-in.

Send the report to an ASCII file if you want to use the file with another software package, such as in a spreadsheet program.

Procedure

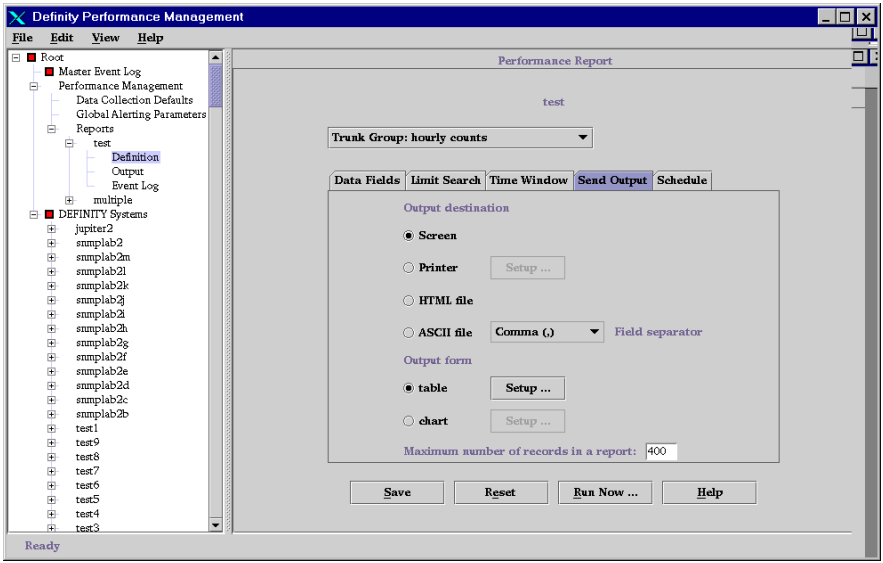
To define the destination of a report, do the following:

1 Click **Reports >** [**report name**] **> Definition**.

Result: Displays the Report Definition Pane for that report.

2 Click the **Send Output** tab.

Result: Displays the **Send Output** tab



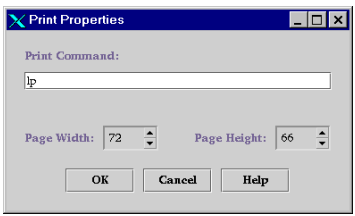
3 Do one of the following:

- To send the output to the screen, that is, display the report on the screen, click **Screen**. The report will display on the screen.

- To send the output to a printer, click **Printer**. The output will go to a printer. To define print properties, click **Setup** to display the Print Properties window. Go to the next step.
- To send the output to an HTML file, click **HTML**. The output will go to an HTML file. The system will automatically assign and display the file name and path when you run the report.
- To send the output to an ASCII file, click **ASCII**. The output will go to an ASCII file. The system will automatically assign and display the file name and path when you run the report.

  You can also select a field separator in the Field separator field. The separator is a single character that separates fields on a table. This is useful for making the table readable in another software package.

4 To define printer detail from the Print Properties window, change the settings as described in the following table and click **Close**. These values are usually set up by your system administrator, but you can customize them here.



Field	Description
Print Command	The print command the system will use to print the report.
Page Width	The width of the report. The default is 72 characters for portrait mode.
Page Height	The height of the report. The default is 66 characters for portrait mode.

5 Click **Save** to save the settings.

6 To change the number or rows in a table from the default of 1000, go to the *Maximum number of records in a report* field at the bottom of the pane and type the new value. This value restricts the size of the reort, thereby ensuring that you are not overburdening your desktop or your printer with too much report output. Note that if there are any secondary records, this number includes the combined total of primary and secondary records.

Run a Report

You can set up a report so that it runs automatically as defined in the **Schedule** tab of the Report Definition pane, or you can run a report manually (on demand) immediately. This procedure describes how to run a report manually.

Procedure

To run a report, do the following:

1. Click **Reports >** [**report name**] **> Definition**.

   Result: Displays the Report Definition pane for the report.

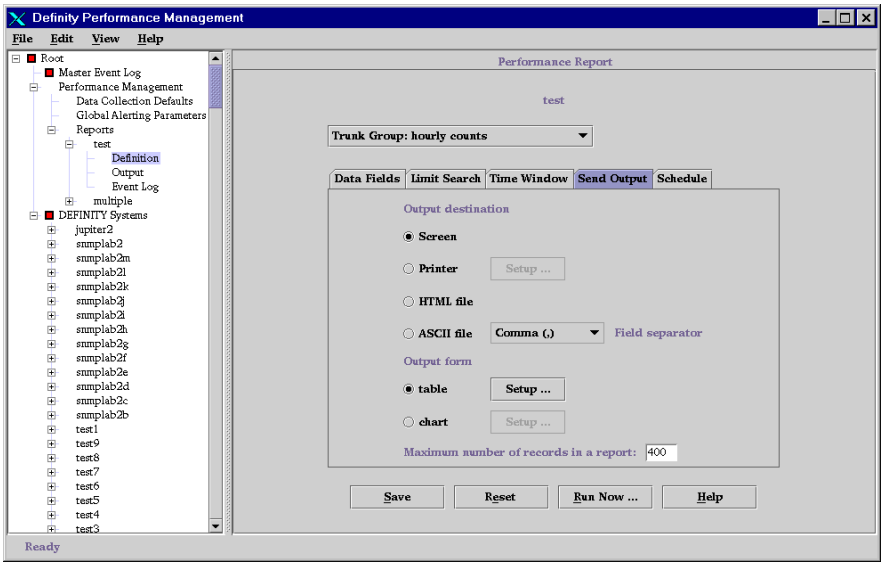
2. Do one of the following:

   - To run the report immediately, click **Run Now**.

   Result: Displays the report on your screen using whatever is defined for the report. To make any changes, go to the next step.

   - To define the report destination before running the report, click the **Send Output** tab.

   Result: Displays the **Send Output** tab.

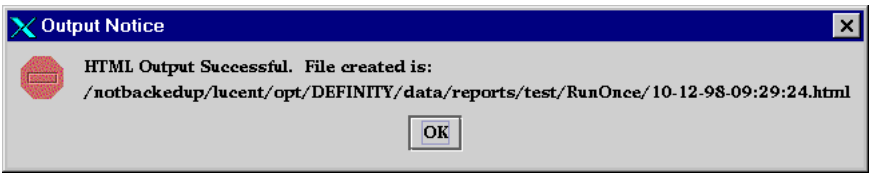


3 To define the destination of the report, go to *"Define Destination of Report Output" on page 163*.

4 To define the format of the report, go to *"Set up Report in Table Format" on page 154* or *"Set up Report in Chart Format" on page 157*.

5 From any of the tabs on the **Report Definition** pane, click **Run Now**.

Result: Report will run in the format and to the destination as specified in the preceding steps. If you send the output to a an HTML or ASCII file, a confirmation window appears, specifying the file name and path of the file. The system automatically appends an .htm (for HTML) or .txt (for ASCII) extension to the file name. See the following output notice sample.



6 If the report output is the *screen*, go to *"Options from a Displayed Report" on page 131* to perform any of the options from a displayed report.

If the report output is a *file*, go to *"Display Report Output" on page 170*.

Display Report Output

This procedure describes how to display the output of a previously-run report that is in an HTML or ASCII file format. The system segregates the list of available reports on a daily, run once, weekly, or monthly basis. For example, if a report has run weekly for several weeks, a list of those weekly report runs will appear when you click on the **Weekly** tab.

Viewing HTML Output

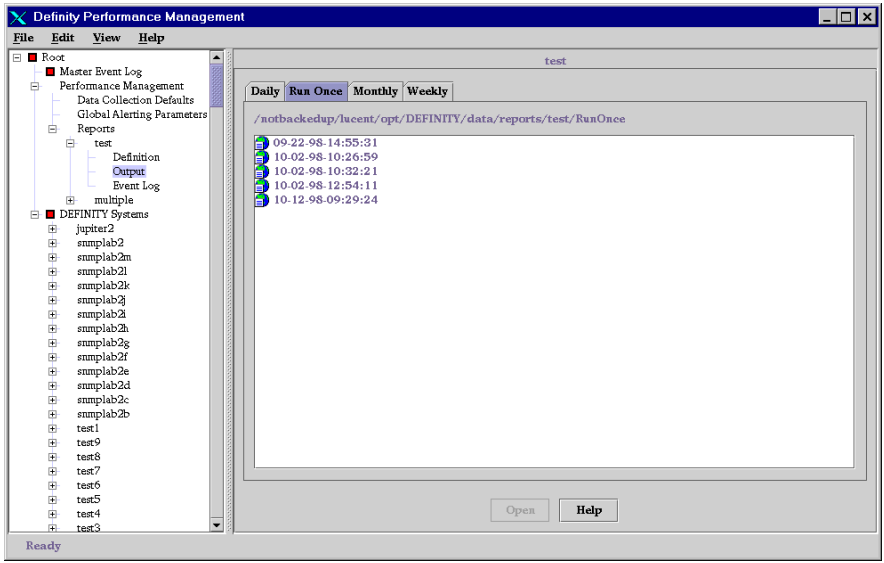
If you want to view a report in HTML format using a local browser such as Netscape,and you are running on Solaris, you need to click the **Setup** link that displays at the bottom of the the browser window when you try to view the file. This link connects you to a Java plug-in that is necessary for viewing the file. If running in a Windows environment, you will be automatically prompted to select a plug-in.

Procedure

To display the output of a report, do the following:

1 Click **Reports >** [**report name**] **> Output**.

Result: Displays the Display Output pane for that report. If any of the reports include primary data, there will be a .p extension after the report file name. Secondary data will have a .s extension.



2 Click on the tab that matches the schedule of the report you want to see. For example, if you have a report that runs on a monthly basis, then click the **Monthly** tab.

Result: Displays a list of generated reports that match that schedule.

3 To view the report, double click on the desired file name, or single click on the file name and click **View**.

Result: Displays the report.

4 To change any of the report definition parameters, such as the format of the report, go to *"Options from a Displayed Report" on page 131*.

View a Report on a Browser

This procedure describes how to view a Performance Management report in an HTML format on a Web browser.

Prerequisites

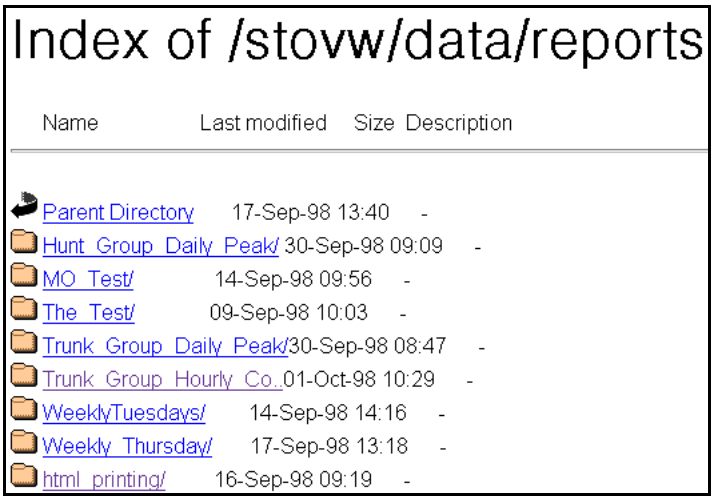
- Make sure you know the World Wide Web location (URL) and the server where the Performance Management files are located. The person that installed Performance Management should know this information.
- Your web browser will need a Java applet (plug-in) so that the html file (which runs the applet) can open a network connection to download data necessary to display the table or chart. You will be given instructions on how to install this plug-in during the following procedure.

Procedure

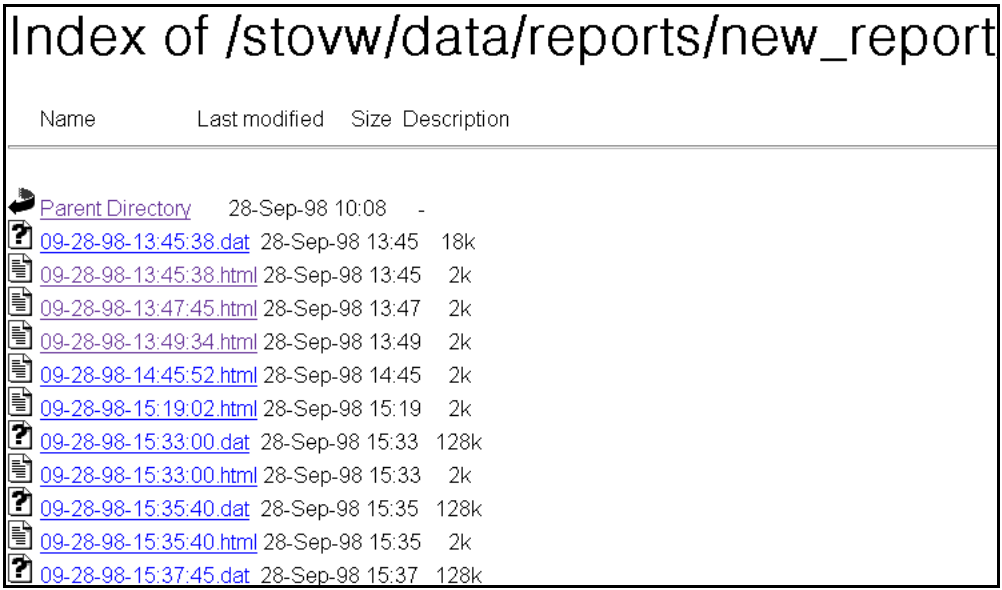
To view a report on a browser, do the following:

Note: You may be prompted to get a Java plug-in for your browser during this process. If necessary, have your system administrator help with getting the plug-in.

1. Run the report and define its output destination as **HTML** as described in *"Run a Report" on page 167* and *"Define Destination of Report Output" on page 163*. Remember the file name of the report.
2. From your browser, enter the web location (URL) on the server where the report files reside. If necessary, see your administrator for this information.
3. From the index of reports (see sample screen below), click on the directory that contains the report you want.



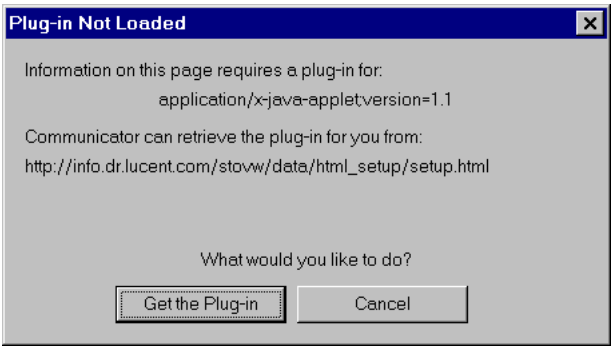
4 Continue to click on the appropriate links until the report you want is listed, as shown in the following sample screen.



5 Click on the file name of the report you want to see.

Result: If your browser has the required plug-in, the report displays. If your browser does not have the required plug-in to display the report, go to the next step.

6 If your browser cannot find the plug-in needed for displaying the file, you will be prompted to get the plug in as shown in the following sample screen. Click on the **Get the Plug-in** button and follow the set up instructions that are provided automatically in order to download and install the plug-in and view the report. Regardless of whether the following sample screen displays of not, you must click on the **Setup** link at the bottom of the browser window in order to get the instructions for downloading the plug-in.



Note: If you are in a UNIX environment, it is helpful to have a working knowledge of UNIX, or else get your UNIX administrator to help you set up the plug-in.

Result: The report displays in the browser window.

8 Event Log

Chapter Contents

Introduction

Purpose of Event Log

By using an event log, you can pinpoint any system problems, assess the severity of the problem, and view the history to the problems. At that point you can close out the event causing the problem, or you can investigate and take care of the problem using the information provided by the event log.

Definition of Event Log

The event log displays a table listing all of the events for either all managed nodes in the DEFINITY system, or events specific to selected parts of a managed node. An event is an occurrence, condition, or problem that the system detects and records in the event log. Conditions that can cause an event to appear in the event log include:

- Data collection failure
- Report not generating
- Managed node not meeting an established threshold
- Trunk group not meeting a threshold service

Types of Event Logs

Performance Management provides several types of event logs. Each event log contains the same fields, but differ on what type of events they contain. The following table lists the different event logs and what they contain.

Type of Event Log	Description
Master	Shows all events for all managed nodes
Data Collection	Shows all data collection events for the selected managed node
Processor Occupancy	Shows all processor occupancy events for the selected managed node
Trunk Group (Grade of Service)	Shows all trunk group grade of service events for the selected managed node
Report	Shows all failures for a particular report

Using the Event Log

Description

The event log displays all of the events for the either all managed nodes, or events specific to selected parts of a managed node. An event is an occurrence or condition that the system detects and is recorded in the event log. Conditions that can cause an event to appear in the event log include:

- Data collection failure
- Report generation failure
- Managed node not meeting the established threshold
- Trunk group not meeting threshold service

Each managed node has its own event log, but the master event log contains all events for all managed nodes.

This procedure describes how to view and interpret the Master Event Log.

Viewing an Event Log

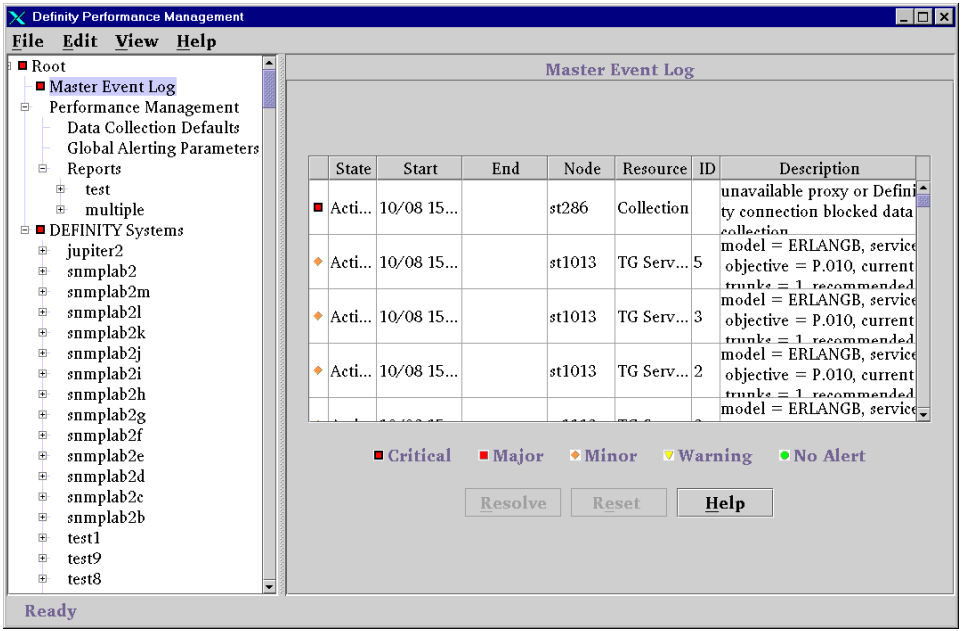
To view any of the various event logs, do the following:

To view this event log...	From the left pane, click...	The system displays...
Master	**Master Event Log**	Master Event Log
Data Collection	**DEFINITY Systems >** [**specific managed node**] **> Data Collection > Event Log**	Data Collection Event Log for the managed node

To view this event log...	From the left pane, click...	The system displays...
Processor Occupancy	**DEFINITY Systems >** [**specific managed node**] **> Processor Occupancy > Event Log**	Processor Occupancy Event Log for the managed node
Trunk Group (Grade of Service)	**DEFINITY Systems >** [**specific managed node**] **> Trunk Groups > Event Log**	Grade of Service Event Log for the managed node
Report Generation	**Performance Management >Reports>** [**specific Report**] **> Event Log**	Report Generation Event log for that report

Sample Event Log

The following screen is a sample event log with corresponding alert indicators.



Event Log description

The fields in the event log are described as follows. Newest active events are displayed at the top, followed by resolved events, with newest resolved events listed first.

Event Column	Description
First column	Icons representing one of five alert levels. The levels, in order of increasing severity, are: Warning, Minor, Major, and Critical. The highest active alert icon will be displayed the left pane for each alertable node. An event generates an alert when it does not have an end time. If no alerts are present, the No Alert icon is displayed. If "None" is specified as the alert level, the event does not generate an alert. The highest level of severity displays for each alertable node.
State	The current status of the event; either active or resolved. An active event does not have an end time. An event is resolved when you or the system ends the event, whereby an end time is added to the event.
Start	The time when the Performance Management system detects the problem and logs the problem as an event. The time is in the local time zone where the Performance Management system is located.

Event Column	Description
End	The time when either the system or a user ends the event. The time is in the local time zone where the Performance Management system is located.
Node	The network component that caused the event to be logged, such as Data Collection.
Resource	The monitored resource at the node that caused the event to be logged. For example, a trunk group service is a resource. Data collection, processor occupancy, and trunk group service events are related to a specific managed node. Report generation events are created by the Performance Management system.
ID	Resource identifier that is set when there are multiple resources of the same type at the given node. For example, trunk group service events can occur for any monitored trunk group for a specific managed node. The trunk group is the resource identifier.
Description	Provides details about the event, such as the parameters used to determine its existence. The details come from the system that detected the problem, which is usually the data collector.

Resolve an Event

Introduction

Active events normally end automatically by the system when new data is obtained about the situation that caused the event to be logged in the event log. For example, a report event ends when an attempt is made to generate the report again. If the report fails again, a new event is recorded in the event log. With Performance Management, you have the option of resolving an event manually, as described below.

Procedure

To manually resolve an event, highlight one or more rows in the event log table and click **Resolve**. The state of the events that are resolved change to “Resolved” and the End time is set to the current time.

Conditions for ending events automatically

The following table lists how events are ended by the system automatically:

This event...	is ended when...
Report	The next attempt is made to generate the report.
Data collection	The next attempt is made to collect data.
Processor occupancy	new processor occupancy data is retrieved for the managed node.
Trunk group	new trunk group data is retrieved from the managed node.

9 Set Alerting Parameters

Chapter Contents

Introduction

Alerts are visual reminders of any problems in the DEFINITY system. Alerting is also used by the NMS to identify problems associated with a specific managed node. You can define what events trigger alerts and at what level of severity. You can then tell at a glance by looking in the left pane of Performance Management where the problems are. For example, you can set your system up so that you are notified by a critical alert if there are any problems collecting data.

This chapter describes alerts, how to determine which events generate alerts, and how to determine the severity level for an event.

About Alert Levels

When setting alerting parameters as described in this chapter, you need to specify the level of severity attached to each condition that causes an alert to occur. The level of security is a visual cue to remind you of the severity of the problem associated with a specific managed node.

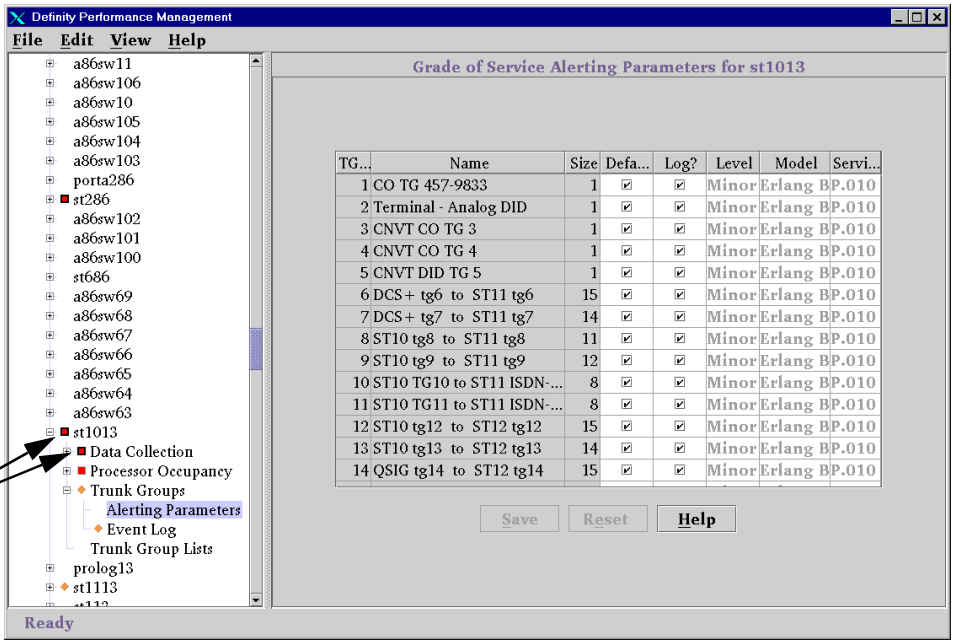
Alert Levels and Icons

The levels of alerts, in order of increasing severity, are shown in the following table:

Alert Level	Alert Icon you see in left window pane
Warning	
Minor	
Major	
Critical	

Escalation of Alert

The highest alert icon will display for each node of that managed node. For example, in the following example, the highest level alert icon, a major alert icon, appears not only next to the event log for that managed node, but also next to the managed node.



Most severe alert escalated to DEFINITY Systems node

Set Global Alerting Parameters

This procedure describes how to set alerting parameters for the Performance Management system. Some of these parameters can be overridden for a specific managed node, as described in the following sections of this chapter:

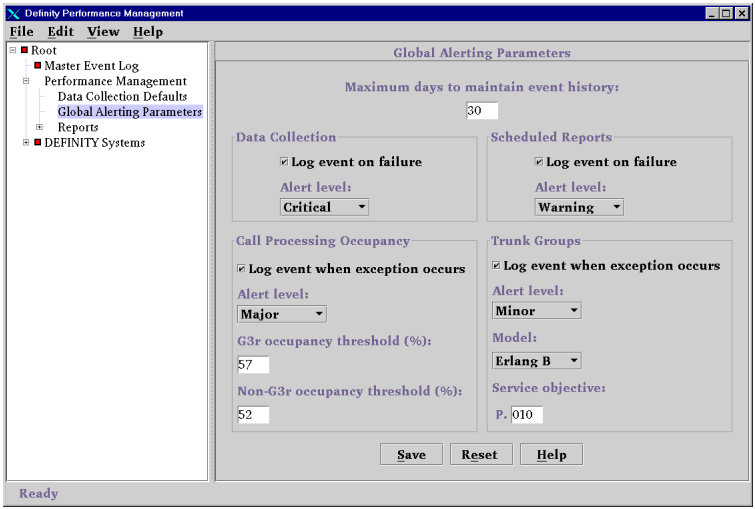
- *"Set Processor Occupancy Alerting Parameters" on page 195*
- *"Set Trunk Group Alerting Parameters" on page 198*

Procedure

To set default alerting parameters that will be used throughout the Performance Management system, do the following:

1 From the left window pane, click **Performance Management > Global Alerting Parameters.**

Result: Displays the Global Alerting Parameters pane.



2 In the Maximum days to maintain event history field, enter the number of days you want to retain event data in the database log. At midnight of each day, old records are purged if their start time is older than the maximum allowed days.

3 In the Data Collection box, do you want the system to record data collection failures in the event log?

- If *yes*, put a check mark in the box next to the Log Event on failure field. Set the alert level for the event by clicking on the arrow in the Alert level pull-down list and selecting one of the options.
- If *no*, leave the box unchecked. The system will not record any data collection errors in the event log, even if data collection parameters have been established.

4 In the Scheduled Reports box, do you want the system to record report generation failures in the event log?

- If *yes*, put a check mark in the box next to “Log Event on failure”. Set the alert level for the event by selecting one of the options listed in the Alert level pull-down list.
- If *no*, leave the box unchecked. The system will not record any report generation failures in the event log.

5 In the Call Processing Occupancy box, do you want the system to record call processing occupancy exceptions in the event log?

- If *yes*, put a check mark in the box next to “Log event when exception occurs” in the Call Processing Occupancy box. Set the alert level for the event by clicking on the arrow in the Alert level pull-down list and selecting one of the options.

- If *no*, leave the box unchecked. The system will not record any call processing occupancy exceptions in the event log.

  The G3r occupancy threshold field reflects the maximum percent of CPU occupancy being used by the call processing software for DEFINITY G3r switches before an event is generated. Enter the threshold percent in this field by typing the percent or by clicking the up or down arrows to obtain the desired percent.

  The Non-Gr3 occupancy threshold field sets the default call processing occupancy threshold for switches other than the DEFINITY Gr3. Fill in this field as described in the G3r field.

6 In the Trunk Groups box, do you want the system to record trunk group grade of service exceptions in the event log?

- If *yes*, put a check mark in the box next to “Log event when exception occurs”. Set the alert level for the event by clicking on the arrow in the Alert level pull-down list and selecting one of the options.
- If *no*, leave the box unchecked. The system will not record any trunk group grade of service exceptions in the event log.

  In the Model field, select the model to use in calculating trunk group grade of service. Choose the model whose assumptions most closely match your situation.

  The Erlang B model assumes that calls that are blocked from accessing the trunk group are cleared from the system.

The Erlang C model assumes that there is an infinite queue for calls trying to access the trunk group to wait in until resources are available. This means that all calls are eventually served.

The Retrial model assumes that some calls are blocked but will retry. The Retrial model is an approximation using the average of the results of the Erlang B and Erlang C models.

Choose one of the following options:

- Erlang B
- Erlang C
- Retrial

In the Service objective field, type a number between .001 and .700 that represents the percent of calls that may be blocked from accessing that trunk group based on the current call activity. Trunk group grade of service events are generated when the computed service objective exceeds the value in this field.

7 Click **Save** to save the settings.

Set Processor Occupancy Alerting Parameters

Introduction

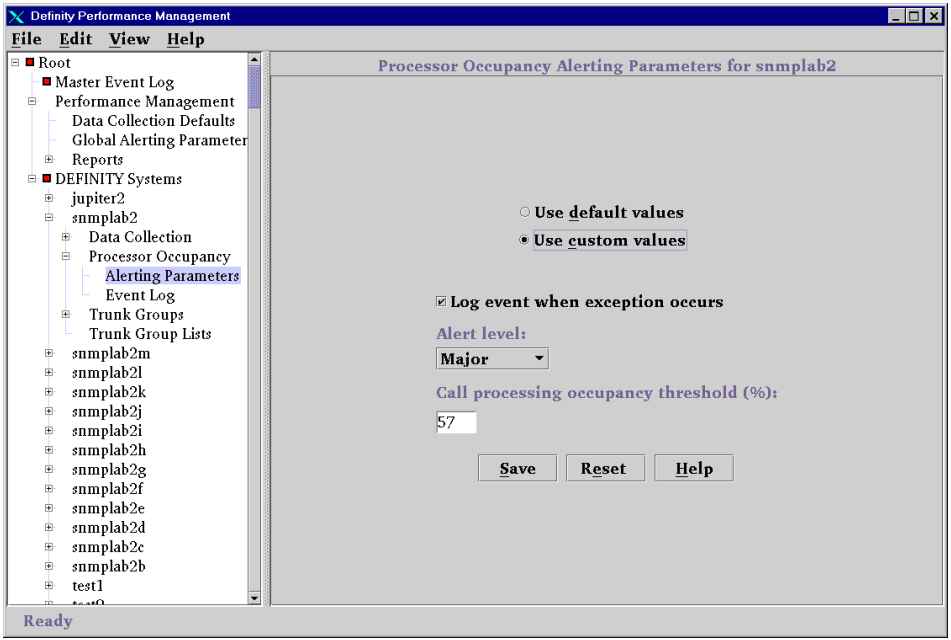
This procedure describes how to override the default processor occupancy alerting parameters for a specific managed node.

Procedure

To set processor occupancy alerting parameters, do the following:

1 From the left window pane, click **DEFINITY Systems >** [**managed node**] **> Processor Occupancy > Alerting Parameters**

Result: Displays the Processor Occupancy Alerting Parameters pane for the managed node you selected.



2 Do one of the following:

- To use the global default processing occupancy parameters, click the **Use default values** button.
- To customize the parameters for this managed node, click the **Use custom values** button.

3 Do you want the system to record call processing occupancy exceptions in the event log?

- If *yes*, put a check mark in the box next to “Log event when exception occurs”.
- If *no*, leave the box unchecked. The system will not record any call processing occupancy exceptions in the event log.

4 Set the alert level for the event by clicking on the arrow in the Alert level pull-down list and selecting one of the options.

5 In the Call processing threshold field, enter the maximum percent of CPU occupancy being used by the call processing software before an event is generated. Type the percent or click the up or down arrows to obtain the desired percent.

6 Click **Save** to save the settings.

Set Trunk Group Alerting Parameters

Introduction

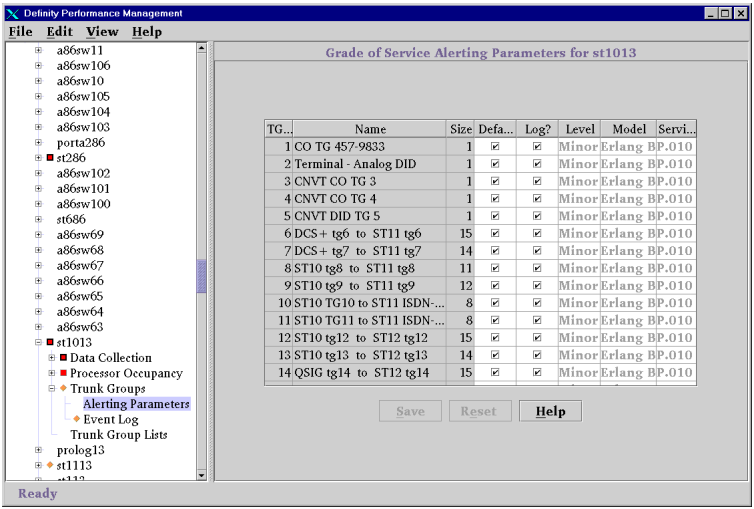
This procedure describes how to override the default trunk group alerting parameters for a specific managed node.

Procedure

To set the trunk group alerting parameters, do the following:

1 From the left window pane, click **DEFINITY Systems >** [**managed node**] **> Trunk Groups > Alerting Parameters.**

Result: Displays the Grade of Service Alerting Parameters pane for that managed node. The columns on the left side of the table identify the trunk group number, name and number of trunks. These columns cannot be changed. The remaining fields can be changed if the Default? box is not checked.



2 Click in the Default column for the trunk group you want to change so that the Default? box is unchecked.

Result: You can now change the parameters in the remaining columns.

Note: If the Default box is checked, the system will use the global default values to determine when to record alerts. The remaining fields will display the default values and cannot be changed.

3 In the Log column, put a checkmark in the box if you want the system to record trunk group grade of service exceptions. If you do not want to record exceptions, leave the box unchecked.

4 In the Level column, set the alert level for the event by clicking on the arrow in the Alert level pull-down list and selecting one of the options.

5 In the Model column, select the model to use in calculating trunk group grade of service. The Retrial calculation is an approximation of the standard Retrial calculation. It is basically the average of Erlang B and Erlang C.

Choose one of the following options:

- Erlang B
- Erlang C
- Retrial

6 In the Service Objective column, type a number between .001 and .700 that represents the percent of calls that will be blocked from accessing that trunk group based on the current call activity. Trunk group grade of service events are generated when the computed service objective exceeds the value in this field.

7 Click **Save** to save the settings.

10 Maintenance and Error Recovery

Chapter Contents

Introduction

This chapter describes various aspects of maintaining Performance Management. It also describes how the system recovers from various errors. Topics included in this chapter are:

- What Performance Management does upon initialization
- Errors and how the system handles them
- Trace file description
- Event type description

Error Recovery

Performance Management handles errors in the following manner:

Type of Error	Description	How System Handles
SNMP errors	Errors returned to the application software from the lowest SNMP software. Usually result in data collection failure.	• Informs user of error by alert in Data Collection node in left pane. • Logs the error in the event log. • Stops requesting data • Attempts to collect data again at the next scheduled collection time.
SNMP failures	SNMP response indicating an error condition at the Proxy Agent or the network.	• Informs user of failure by an alert in the Data Collection node. • Logs the failure in the event log. • Stops requesting SNMP data from the node that provided the failure response. • Continues to collect data from other managed nodes • Attempts to collect data from the affected managed node at the next scheduled collection time.

Type of Error	Description	How System Handles
SNMP No Response	Problem with the network or Proxy Agent.	• Retries the request. If retries fail, displays an alert in the Data Collection node. • Logs the error in the event log. • Posts an alert in the Data Collection node. • Stops requesting data from the failed managed node, but continues to request data from the other managed nodes as scheduled. • Attempts to request data from failed managed node at next scheduled collection time.
Inconsistent Data	For example, a trunk group data with no corresponding configuration data.	• Stores the data normally. • Writes a message to the trace file.

System Notification of Errors

Performance Management provides information for errors that can prevent the system from performing its task. Errors can display in the following ways:

- Pop-up error messages
- Alerts shown in the left pane

Error and Exception Log

All performance exceptions and selected errors are recorded in the database in an event log. You can view the events by viewing the various event log panes, which generate alerts that have an associated severity level based on how the alerting parameters are defined. The alerts appear in the left pane and are associated with the DEFINITY component (managed node or performance report) that generated the event.

SNMP problems generate a data collection failure event. A scheduled report that is not generated also generates an event. Exception events are performance exceptions that are outside threshold limits as defined for the system.

Performance Management periodically checks the event log and deletes records whose start time exceeds the defined time that event records are kept.

Process Trace

Description

Each pprocess writes a message to a common trace file. The message has:

- Time stamp
- Process name
- User name
- Managed node name (or “DPM” if message is not related to a managed node)
- Text description that varies with the message type

About LOG and TRACE

Message types LOG and TRACE are normal application progress messages.

LOG messages are always logged, and correspond to trace level zero.

TRACE messages are logged if you raise the trace level.

TRACE Description

A TRACE message contains trace level, thread name if applicable, class, and method. The system has an indeterminate number of TRACE events, but only a few fixed LOG events.

Event Types Exception and Error

The start and end of an exception or error alert is logged in the trace file. The events are described in the following table:

Exception Event	Description
Processor occupancy	Call processing occupancy, occupancy threshold
Trunk group GOS	Trunk group number, exception criteria, size, recommended size
Scheduled report failure	Report name, error code, error description, if available
Scheduled report truncated	Report name, record limit, and total records, if available
Scheduled report data missing	Report name, data type
SNMP no response	Switch name, timeout interval, number of retries
SNMP failure	Error code and error string, if available
Database storage failure	Error code and error string, if available
Inconsistent data	Switch name, data type

Message Type SWERR

These are internal software errors that do not cause an alert, though they may cause other failures that will cause alerts.

SWERR Event	Description
Internal SNMP errors	Error code and error string, if available
Abnormal process termination	Process name

Delete Managed Node from Database

When a managed node is permanently removed from the Proxy Agent, its data remains in the database. Since the data for the managed node is not necessary, you can delete the data from the database by following this procedure.

Procedure

To remove the data for a managed node from the database, do the following:

1. Shut down background processes by typing the following at the UNIX prompt and pressing **Return**:

   ProcStartup -K

2. Type the following and press **Return**:

   RemoveDEF

   Result: Displays any managed nodes that have been removed from the Proxy Agent.

3. Type the command in step 3 followed by each managed node to be deleted. To delete multiple nodes, separate each managed node by a space. For example:

   RemoveDEF Definity1 Definity2

   Result: The data from the specified managed nodes are removed from the database.

Index

M