

Lucent Technologies
Bell Labs Innovations



DEFINITY[®] Network Management Release 3.0 for Proxy Agent

User Documentation
Installation and Administration

March 2000

Contents

Contents 2

Resources and Notices 12

Introduction 13

DEFINITY Network Management CD-ROMs 14

Lucent Resources 15

Sales and Design Support Center (SDSC) 16

NetCare Professional Services (NPS) 16

Technical Services Center (TSC) 17

References 18

Lucent References 19

Vendor References 21

System Security Notices 23

Network Security 23

Toll Fraud Security 24

Year 2000 Compliance Notice 25

1 Proxy Agent Overview 26

Introduction 27

Overview of the Proxy Agent 29

Management Information Base (MIB) 33

Alarm-to-Trap Conversion 36

Alarm Forwarding 37

SNMP Access 39

Enhanced Cut-Through 41

System Security 42

Login Security 42

SNMP Authentication 43

Proxy Agent Security 43

PA001 Request Form 44

New Features 45

Supported Systems 48

System Requirements 49

Hardware Certification 49

Software Requirements 50

| | |
|------------------------------------|----|
| Overview of the User Documentation | 51 |
| Target Audiences | 51 |
| Customer Pre-Installation Tasks | 52 |
| Proxy Agent Installation | 52 |
| Help Screens and Commands | 53 |
| Access Procedures | 53 |
| Network Managers Administration | 53 |
| Default Location Administration | 54 |
| Alarm Path Administration | 54 |
| Filter-Set Administration | 54 |
| Default Login Administration | 55 |
| Managed Nodes Administration | 55 |
| Communication Application | 55 |
| Emulation Application | 56 |
| Configuration Application | 56 |
| I/O Setup Application | 57 |
| Maintenance and Troubleshooting | 57 |

2 Customer Pre-Installation Tasks 58

- Introduction 59
- Plan the Connectivity 60
 - Connectivity Overview 60
 - Data Communication Hardware 64
 - Cables for Communication Devices 67
- Complete the PA001 Form 72
- Install the UnixWare Operating System 73
 - UnixWare Upgrade Patches 73
 - UnixWare Installation Tasks 74
- Administer the Communication Devices 76
- Administer Security Options 78
- Change the Dip Switch Settings 81
 - Settings for AT&T 2224CEO Modems 81
 - Settings for 7400B/B+ Data Modules 82
 - Settings for PDMs 83
 - Settings for MPDMs 85
- Set the Interface for 7400A Modules 86
- Execute the Platform Acceptance Test 87

3 Proxy Agent Installation 90

Introduction 91

Installation Checklists 93

Installation Tasks Checklist 94

Technical Verification Checklist 96

Customer Acceptance Checklist 97

Installation Prompts 98

Directory Prompt 98

RAM Megabytes Prompt 99

SNMP Polling Prompt 99

SNMP Traps Prompt 99

SNMP Set Capability Prompt 100

Password Prompts 100

Function Prompt 100

Device Type Prompt 102

Reboot Prompt 103

Serial I/O Subsystem 104

Install the New Proxy Agent 106

Upgrade from Proxy Agent 2.0 and Later 116

Upgrade from Proxy Agent 1.4 and Earlier 126

Remove the Proxy Agent 128

4 Help Screens and Commands 130

Introduction 131

Functions Window 132

Commands and Hotkeys 133

Format Conventions 137

5 Access Procedures 141

Introduction 142

Log in to the Proxy Agent 143

 Log in from the UNIX Shell 143

 Log in from the Desktop 145

Access the User Documentation 150

Access the IO_Setup Folder 153

Review of the Main Menu 156

Review of the Proxy Admin Menu 160

Start the Proxy Agent 164

Display of the Status Screen 165

 Review of the Status Screen Fields 167

 Display the Status Screen 170

Stop the Proxy Agent 171

6 Network Managers Administration 172

Introduction 173

Review the Network Managers Screen 174

Administer the Network Managers 179

7 Default Location Administration 182

Introduction 183

Review of the Default Location Screen 185

Administer the Default Location 191

8 Alarm Path Administration 193

Introduction 194

Review of the Alarm Path Screen 196

Administer the Alarm Path 199

9 Filter Set Administration 201

Introduction 202

Examples of Filter Sets 206

Review of Filter Set 1 207

Review of Filter Set 2 209

Review of the Filter Set Screen 211

| | |
|-------------------------------|-----|
| Administer the Filter Sets | 219 |
| Add a New Filter Set | 220 |
| Change an Existing Filter Set | 223 |
| Display the Filter Set Screen | 226 |
| Remove a Filter Set | 227 |

10 Default Login Administration 230

| | |
|------------------------------------|-----|
| Introduction | 231 |
| Review of the Default Login Screen | 232 |
| Administer the Default Login | 235 |

11 Managed Nodes Administration 237

| | |
|---------------------------------------|-----|
| Introduction | 238 |
| Review of the Managed Nodes Screen | 241 |
| Review of the Fields on Page A | 242 |
| Review of the Fields on Page B | 250 |
| Review of the Fields on Page C | 254 |
| Review of the Fields on Pages D and E | 257 |
| Review of the Fields on Page F | 262 |
| Administer the Managed Nodes | 265 |

12 Communication Application 274

Introduction 275

Review of the Communication Manager Screen 278

Connect to Managed Nodes 281

Connect to DEFINITY Systems with ASG 287

Disconnect from Managed Nodes 296

13 Emulation Application 297

Introduction 298

Review the Emulation Screen 299

Conduct an Emulation Session 300

 Connect to One Managed Node 301

 Connect to Two Managed Nodes 303

14 Configuration Application 306

Introduction 307

Administer the Change Hardware Screen 309

 Review the Change Hardware Screen 310

 Administer the Change Hardware Options 314

Administer the Change User-Interface Screen 316

 Review the Change User-Interface Screen 317

 Administer the Change User-Interface Options 322

15 I/O Setup Application 324

Introduction 325

Devices File 326

Edit the Devices File 327

Dialers File 328

Devices and Dial Strings 328

Edit the Dialers File 332

16 Maintenance and Troubleshooting 334

Introduction 335

Add New Devices 336

Change Settings for SNMP Access 337

View Alarm and Error Logs 338

Use Alarm Testing Tools 339

Index 344

Resources and Notices

Chapter Contents

- [Introduction](#) [13](#)
- [DEFINITY Network Management CD-ROMs](#) [14](#)
- [Lucent Resources](#) [15](#)
 - [Sales and Design Support Center \(SDSC\)](#) [16](#)
 - [NetCare Professional Services \(NPS\)](#) [16](#)
 - [Technical Services Center \(TSC\)](#) [17](#)
- [References](#) [18](#)
 - [Lucent References](#) [19](#)
 - [Vendor References](#) [21](#)
- [System Security Notices](#) [23](#)
 - [Network Security](#) [23](#)
 - [Toll Fraud Security](#) [24](#)
- [Year 2000 Compliance Notice](#) [25](#)

Introduction

This chapter contains resources and notices that are pertinent to the **DEFINITY Network Management (DNM)** products.

The **DEFINITY Network Management CD-ROMs** section lists the contents of the product CD-ROMs that are delivered to customers.

The **Lucent Resources** section describes the services that are available from the Sales and Design Support Center (SDSC), NetCare[®] Professional Services (NPS), and Technical Services Center (TSC).

The **References** section contains Lucent contact information, including web sites, phone numbers, and email addresses. The section also contains contact information for third-party vendors.

The **System Security** section defines the precautions that customers must take to maintain the security of their networks and systems. The section also contains information on toll fraud security.

The **Year 2000 Compliance** section contains the Lucent policy to meet the year 2000 requirements for the manufacture and sales of its products after September 26, 1996.

DEFINITY Network Management CD-ROMs

Lucent Technologies delivers the DEFINITY[®] Network Management (DNM) products **and** the user documentation to customers on two separate CD-ROMs, which are entitled:

- DEFINITY Network Management for UNIX[®] **or** Windows[®] NT
- DEFINITY Network Management Proxy Agent

The contents of each of the CD-ROMs are listed below:

DEFINITY Network Management Release 3.0 UNIX Version

- Product software and Versant database
- DNM Online Help System integrated in the product software
- DNM User Documentation for UNIX Version, Installation and Getting Started
- PA001 Administration Request form

DEFINITY Network Management Release 3.0 Windows NT Version

- Product software and Versant database
- DNM Online Help System integrated in the product software
- DNM User Documentation for NT Version, Installation and Getting Started
- PA001 Administration Request form

DEFINITY Network Management Proxy Agent Release 3.0

- Proxy Agent software
- Proxy Agent User Documentation for Installation and Administration
- PA001 Administration Request form

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.

Note: The DEFINITY Network Management products are a **software-only** offer. Therefore, **customers** are solely responsible for the purchase and maintenance of all third-party hardware and software that are required to run the DEFINITY Network Management products.

The DEFINITY Solutions web site contains the system requirements and other provisioning and connectivity information for the DNM products. Refer to ["Lucent References" on page 19](#) for the web address.

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

Sales and Design Support Center (SDSC)

The Sales and Design Support Center (SDSC) works with customers and account teams to develop detailed solutions for connectivity to the DEFINITY and other supported systems. The SDSC also designs network configurations to support the DEFINITY Network Management products.

NetCare Professional Services (NPS)

NetCare[®] Professional Services (NPS) is available to work with customers to design and build a **turn-key** network management system.

NetCare offers the consulting services listed below:

- Plan and design a custom network system
- Purchase and configure SCO-certified hardware and external devices for the Proxy Agent computer and the Network Management System (NMS) platforms
- Install and set up the UnixWare Operating System
- Connect and administer all devices, ports, and cards
- Install and integrate the DEFINITY Network Management products on the NMS platform
- Train users on the operation and management of the products

Technical Services Center (TSC)

The Technical Services Center (TSC) provides support for the DEFINITY Network Management products to account teams, field technicians, and customers.

The TSC works with the customer and the Lucent field technicians to perform the tasks below and to ensure that the products are properly installed and working:

- Platform Acceptance Test from the Proxy Agent computer
- Installation support for the DEFINITY Network Management products
- Technician Verification checklist
- Customer Acceptance checklist

Time and materials charges

The Technical Services Center (TSC) will **bill** customers for support on a time and materials basis if the following conditions exist:

- Customers do not have a current maintenance agreement
- Customers do not procure and install the required systems and software as defined in the Project Provisioning Package
- Customers request support that is outside the purchase agreement

The Technical Services Center (TSC) does **not** support hardware or software that customers purchase from third-party vendors.

References

This section contains references to web sites, phone numbers, and email addresses for Lucent Technologies and third-party vendors.

The contact information is listed in the sections below:

- ["Lucent References" on page 19](#)
- ["Vendor References" on page 21](#)

Customers can access web sites that are **outside** the Lucent fire wall.



CAUTION:

The owners of the web sites may change the universal resource location (URL) for a specific web site address **without** notice. The reference information will be updated with each new release of the DEFINITY Network Management products.

Lucent References

The table below contains Lucent web sites, phone numbers, and email addresses for various sources. Some of the web sites are inside the fire wall and are *not* accessible to customers.

Table 1. Lucent web sites

| Source | Web Sites |
|--|---|
| DEFINITY Solutions | Systems Management site: http://www.bcs.lucent.com/salesmarket/definity/sysmgmt |
| Documentation and Training Information Development | DNM 3.0 project web site: http://pubnet.lucent.com/project/dnm3_0.htm |
| IntraWorks Catalog | DEFINITY Network Management User Document Set: http://www.lucent.com/enterprise/documentation |
| NetCare Professional services (NPS) | Email: dnmconsulting@lucent.com Consulting offer: http://www.netcaredata.com/solutions/consult.shtml |
| Project Development Team R&D Bell Labs | DEFINITY Network Management (DNM) internal web site: http://info.dr.lucent.com/defnm |
| | <i>1 of 2</i> |

Table 1. Lucent web sites

| Source | Web Sites |
|--|---|
| DEFINITY Enterprise Management Support | DNM Proxy Agent internal web site: http://dfmpa1.dr.lucent.com |
| Project Provisioning Package | http://dfmpa1.dr.lucent.com/docs/snmpppp30.doc |
| Sales and Design Support Center (SDSC) | Phone: 1-888-297-4700, prompt 6 Main site (requires a password): http://www.bcs.lucent.com/tech_info/sdsc |
| Technical Services Center (TSC) | Technical Support: 1-800-242-2121, ext. 8-6767 Fax for PA001 form: 1-303-804-3367 Connectivity Guide: http://www.dc.tsc.bcs.lucent.com/html/table1/htm |
| Tier IV Support Registry | International Customers only: Fax for PA001 form: (U.S. code) 303-538-5506 |
| Toll Fraud Intervention | 1-800-643-2353 |
| | <i>2 of 2</i> |

Vendor References

The table below contains the web sites for third-party vendors.

Table 2. Vendor web sites

| Vendor | Web Sites |
|----------------------------------|--|
| AIX | AIX patches: http://service.software.ibm.com/support/rs6000 |
| Computone I/O cards | Main site: http://www.computone.com |
| Equinox | Main site: http://www.equinox.com |
| Hewlett Packard | Main site: http://www.hp.com OpenView site: http://www.openview.hp.com |
| IBM | Main site: http://www.ibm.com |
| Remedy ARS | Main site: http://www.remedy.com |
| Santa Cruz Operation, Inc. (SCO) | Main site: http://www.sco.com UnixWare certified hardware: http://wdb1.sco.com/chwp/owa/hch_search/form Upgrade patch: ftp://ftp.sco.com/UW21 |
| Sun Microsystems, Inc. | Main site: http://www.sun.com Solutions site: http://sunsolve.sun.com |
| | <i>1 of 2</i> |

Table 2. Vendor web sites

| Vendor | Web Sites |
|------------------|---|
| Microport | Purchasing and support for Unixware Main site: http://www.mport.com |
| Telamon TelAlert | Main site: http://www.telamon.com |
| Tivoli | Main site: http://www.tivoli.com |
| | <i>2 of 2</i> |

System Security Notices

Customers are **solely** responsible for the security of their system, network, and access to hardware and software.

The sections below define the precautions that all customers should take to maintain the security of their systems.

Network Security

The DEFINITY Network Management products use the standard security features on the UNIX and NT operating systems.

Lucent **strongly** recommends that customers use passwords to prohibit access to their systems and to routinely change those passwords to maintain security.

Lucent also **strongly** recommends that customers assign the “browse” login to managed systems and disable the “password-aging” feature. SNMP set enabled on the proxy agent requires Maintenance and Administrator permissions when SNMP is used to set system time and/or to do bus-out/release.



SECURITY ALERT:

Customers should always change passwords immediately after external vendors have completed installation, maintenance, troubleshooting, or other tasks on their system.

Toll Fraud Security

Although the DEFINITY Network Management products are generally not at risk for toll fraud, **customers** are solely responsible for the security of their entire telecommunications systems.

Toll Fraud is the unauthorized use of a company's telecommunications system by unauthorized parties. Unauthorized parties are persons other than the company's employees, agents, subcontractors, or persons working behalf of on the company.

Note: Toll fraud can result in substantial additional charges for the company's telecommunications services.

The company's system manager is responsible for the security of the company's system, which includes programming and configuring the equipment to prevent unauthorized use.

Lucent Disclaimer

Lucent Technologies does **not** warrant that this product is immune from or will prevent unauthorized use of common-carrier telecommunications services or facilities accessed through or connected to it. Lucent Technologies will **not** be responsible for any charges that result from such unauthorized use. .

Lucent Fraud Intervention

If customers suspect that they are a victims of toll fraud and need technical assistance, customers should refer to the ["Lucent References" on page 19](#) for the Toll Fraud Intervention phone number.

Year 2000 Compliance Notice

The Business Communication System (BCS) 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 BCS 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 Proxy Agent Overview

Chapter Contents

- [Introduction](#) [27](#)
- [Overview of the Proxy Agent](#) [29](#)
 - [Management Information Base \(MIB\)](#) [33](#)
 - [Alarm-to-Trap Conversion](#) [36](#)
 - [Alarm Forwarding](#) [37](#)
 - [Enhanced Cut-Through](#) [41](#)
 - [SNMP Access](#) [39](#)
- [System Security](#) [42](#)
- [PA001 Request Form](#) [44](#)
- [New Features](#) [45](#)
- [Supported Systems](#) [48](#)
- [System Requirements](#) [49](#)
 - [Hardware Certification](#) [49](#)
 - [Software Requirements](#) [50](#)
- [Overview of the User Documentation](#) [51](#)

Introduction

This chapter contains an overview of the primary features in the Proxy Agent product and pertinent information on the topics listed below:

- System security
- PA001 Administration Request form
- New features
- Supported Systems
- System requirements for hardware and software

In addition, this chapter describes the target audiences for *Proxy Agent User Documentation* and outlines the organization of this book.

Software-only offer

The DEFINITY Network Management and Proxy Agent products are **software-only** offers. **Lucent Technologies** is *solely* responsible for the support and maintenance of the product software.

Customers are *solely* responsible for the purchase, support, and maintenance of third-party hardware and software products that are *required* for this offer.

**Product
CD-ROMs**

The DEFINITY Network Management (DNM) product and the DNM Proxy Agent product are delivered to customers on two CD-ROMs.

The DNM Proxy Agent CD-ROM contains the software **and** the user documentation listed below:

- Proxy Agent software
- Proxy Agent User Documentation for Installation and Administration
- PA001 Administration Request form

Users should print the documentation and PA001 forms directly from the CD-ROM **before** they install the Proxy Agent software.

The DEFINITY Network Management product, for either the UNIX or NT version, also contain the product software and user documentation for respective version.

Overview of the Proxy Agent

The DEFINITY Network Management (DNM) product and the DNM Proxy Agent provide a complete solution to manage network resources from a central point of entry.

These products provide users with a snapshot of the health and performance of their network systems. The DEFINITY Network Management and Proxy Agent products work together as an integrated application.

Proxy Agent product

The DEFINITY Network Management Proxy Agent is a protocol conversion resource. The Proxy Agent software resides on a stand-alone personal computer and operates on the SCO UnixWare Operating System.

The Proxy Agent uses serial ports to collect configuration and management data from supported systems. The Proxy Agent converts the data into the Simple Network Management Protocol (SNMP).

In addition, the Proxy Agent generates SNMP traps when supported systems generate alarms and system errors.

The Proxy Agent then transmits the SNMP data to the DEFINITY Network Management (DNM) product that resides on the Network Management System (NMS) network server. The NMS network server can be either a UNIX system or a Windows NT system.

DNM product

The DEFINITY Network Management (DNM) product provides users with graphical and tabular tools to monitor the status and performance of a network of supported systems and external devices.

The DNM product collects configuration, fault, and performance data from the Proxy Agent via Simple Network Management Protocol (SNMP) and displays the data in text, tables, and graphic formats.

The primary features of the DEFINITY Network Management product include:

- **Graphical User Interface (GUI)** -- The DNM main window contains a navigation tree that lists all the supported system and displays a colored alert symbol that indicates highest exception level. Users can expand the list to view all of the configuration components and specific alert symbols for each component.
- **Configuration** -- Users can view the configuration and administered properties of all supported systems (managed nodes) in both a graphic view and a table view.
- **Administration** -- Users define the system-wide parameters for the features below:
 - **Data collection** -- Users define the parameters for the data to be collect from each system, including the type of data, the schedule for collecting data, and the length of time to store the data.
 - **Exception logging** -- Users define the conditions to log exceptions for performance thresholds, faults, and system errors.

- **Exception alerting** -- Users specify the alert levels for exceptions from each supported system. Alerts levels may include exceptions that are critical, major, minor, or warning. The alert level and location of the exception display in the main window as long as the exception exists.
- **Report Manager** -- Users can define the parameters for individual reports for all or selected systems. The report options include:
 - Performance
 - Configuration
 - Exceptions
 - Trunk group

Users can immediately view the reports on screen in both the table and chart formats or direct the output of reports to a printer or an HTML file.

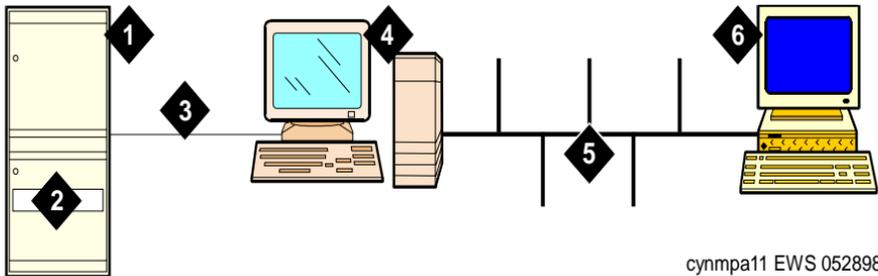
- **Scheduled Reports** -- Users can schedule reports to run on a daily, weekly, or monthly basis and edit and delete schedules as needed.

The DEFINITY Network Management product runs on the network server platforms below that are required for the current release:

- HP OpenView that runs on Sun Solaris or HP-UX
- Tivoli TME 10 NetView that runs on AIX
- Windows NT platform

*Overview of the Proxy Agent***Network configuration**

The figure below shows an **example** of the network configuration between a DEFINITY system, the Proxy Agent computer, and an NMS network server.



cynmpa11 EWS 052898

- 1 *DEFINITY system*
- 2 *Netcon channel or system access ports on the DEFINITY system*
- 3 *Dial-up connection between DEFINITY system and the Proxy Agent modem*
- 4 *Proxy Agent stand-alone computer and Proxy Agent product*
- 5 *Internet TCP/IP connection (LAN or WAN) between the Proxy Agent and the NMS server*
- 6 *Network server (UNIX or NT) where the DEFINITY Network Management (DNM) product resides. The server can be one of the platforms listed below*
 - *OpenView that runs on Sun Solaris or HP-UX;*
 - *NetView that runs on AIX*
 - *Windows NT system*

Figure 1. Network configuration

Management Information Base (MIB)

The Management Information Base (MIB) allows the Proxy Agent to access management data from the supported systems through the Simple Network Management Protocol (SNMP).

The MIB view consists of three groups:

- MIB-II group contains the standard SNMP MIB
- DEFINITY G3-MIB defines the management data that the Proxy Agent collects and converts from the Operations Support System Interface (OSSI) protocol to the SNMP
- Conversant, Audix, Intuity, Intuity Interchange, and CMS MIB

The Proxy Agent places the data extracted from the system into the appropriate MIB group. Then, the Proxy Agent communicates the MIB group through the SNMP to the appropriate DEFINITY Network Management applications on the NMS server (UNIX or NT system) through the network manager.

Cache mechanism

The primary purpose behind the cache mechanism is to speed up data access to management information. Due to the nature of the interface to the system data, the Proxy Agent cannot directly extract the data for each SNMP *GetRequest* or *GetNext Request* message. Therefore, the Proxy Agent places the system data in a cache file and uses the cache data to respond to requests from the network manager for MIB data.

For example, the Proxy Agent will cache data from a system form that contains a table. A series of *GetNextRequests* that are used to parse the table will initiate a single request for that form. The Proxy Agent provides the cached data in a set of **objects** for each cached group. This allows the network manager to make use of the cached data in the DNM applications.

Cache objects

The Proxy Agent creates the cache file when the user establishes the first connection to the supported system. In addition, the Proxy Agent will retrieve any missing cache data when re-connections are established.

The Proxy Agent automatically refreshes cache data. Users can manually execute the “refresh” command from the DNM product.

The Proxy Agent adds the **objects** listed below to the cache files for each group that uses caching:

- A read-only object that specifies the time since the data in the cache was extracted from the system.
- A read-write object that specifies the time interval for which cached data is considered valid. The Proxy Agent uses this value and the age value to determine if the system data needs to be refreshed.
- A read-only object that contains the amount of time that the Proxy Agent used to extract the system data.
- A read-write object that indicates the cache contains refreshed data.
- A read-only object that identifies the groups that contain table data and indicates the number entries in the table.

If the Proxy Agent encounters system command errors during the refresh process, then the cache file will contain **null** data. The empty cache file will still exist, but it will only contain the objects for all the system releases. However, if an attempt to refresh a cached object fails because of command contention on the system, then the existing cache will not be disturbed.

Alarm-to-Trap Conversion

The Proxy Agent receives alarm notification for each supported system that is administered on the MANAGED NODES screen on the Proxy Agent.

To receive alarm notification, users must also administer the *alarm source* fields on the Alarm Path screen in the Proxy Agent. Users must also administer the supported systems to send their alarm notifications to the Proxy Agent's alarm receiver modem or modem pool.

The Proxy Agent also supports the receipt of alarm dispatch and close notifications from the Initialization and Administration System (INADS).

Enterprise traps The Proxy Agent encapsulates the information contained in the alarm in an Enterprise-specific trap and sends the trap to the set of administered network managers. The format of the created traps match the trap definitions in the MIB files for each of the supported systems. These ASN.1 MIB files are included with the Proxy Agent and reside in the **appl_files/agent** directory.

When sending DEFINITY alarm traps, the Proxy Agent refreshes health, alarm, error, and restart data. This refresh process allows the data to be current when the NMS requests the alarm traps.

User-defined script The Proxy Agent also calls a user-defined script that is based on the supported systems. The arguments that are passed to the script also match the arguments that are currently sent to corresponding scripts on the NMS. The scripts that are included in the Proxy Agent are **not** set up. Users must modify the scripts to meet their needs.

Alarm Forwarding

Users can administer the Alarm Path screen on the Proxy Agent to forward alarms to INADS. When the supported system generates an alarm, the Proxy Agent adds an additional field that contains a sequence number to the end of the alarm stream. The Proxy Agent stores the sequence number in the alarm logs.

The Proxy Agent uses the sequence number for tracking purposes. The Proxy Agent forwards the alarms and the sequence number to INADS and includes the number as part of the alarm traps and alarm script arguments.

The Technical Services Center (TSC) uses the sequence number to trace alarms and verify that the alarms received by the Proxy Agent are successfully delivered to the TSC, INADS, and the NMS.

Administration

Users must activate the alarm forwarding feature on a **system-wide** basis, otherwise the feature will not work. To activate alarm forwarding, users must administer both the *alarm source* and *alarm destination* fields on the ALARM PATH screen. If the users do not administer the *destination fields* on the ALARM PATH screen, then alarm forwarding is not active for any managed node.

Users must also administer the supported systems as **managed nodes** on the MANAGED NODES screen. The screen also allows users to administer alarm forwarding on a node-by-node basis.

Alarm filtering The Proxy Agent also provides a new alarm filtering feature that allows users to block the forwarding of certain alarms to INADS. Users can create sets of filtering criteria on the FILTER SET screen and then apply the filter sets to all or individual systems on the MANAGED NODES screen.

When a managed node generates an alarm, the Proxy Agent checks the filter set and compares each set of criteria for a **match** against the alarm. If the Proxy Agent finds a match for any criteria, then the Proxy Agent does **not** forward the alarm to INADS. If no match is found, the Proxy Agent forwards the alarm to INADS.

Reports The Proxy Agent reports any problems when trying to forward alarms to INADS. Alarm forwarding includes SNMP traps and the execution of the user-defined alarm scripts.

The Proxy Agent creates two types of problem reports:

- Receipt of a negative acknowledgement (NAK) from INADS. This usually means that the product ID for the managed node has not been administered in INADS.
- Receipt of an invalid acknowledgment from INADS. This usually occurs if INADS drops the connection too soon, and the Proxy Agent only receives part of the acknowledgement (ACK) needed to complete the “handshake” between the two systems.

SNMP Access

During the installation of the Proxy Agent, installers have the option to enable or disable the SNMP access to DEFINITY management data. For the Proxy Agent to work properly with the DNM applications, installers should enable SNMP polling.

However, installers can select other options to meet their specific business requirements. The installation script contains three prompts to enable or disable SNMP Polling, SNMP Traps, and SNMP Set Capabilities. These options are explained in the sections below:

To change settings for SNMP access **after** the Proxy Agent is installed, installers must reinstall the Proxy Agent and select the appropriate options for SNMP access at the installation prompts.

SNMP Polling

For the Proxy Agent to poll the supported systems and create Enterprise-specific traps, installers should **enable** SNMP Polling. The installation script automatically enables SNMP Traps, since both options are required for SNMP polling.

Installers can choose to **disable** SNMP polling if the Proxy Agent is used only as an alarm notification device **and** the DEFINITY Network Management product is **not** used.

SNMP Traps

If SNMP Polling is disabled, then the installation script displays the prompt to enable or disable SNMP Traps.

Installers should **enable** SNMP Traps if they want to receive traps from a large number of supported systems. In this release, if SNMP Polling is disabled and SNMP Traps are enabled, then the Proxy Agent allows installers to administer up to **600** managed nodes for each Proxy Agent. This option reduces the load on the Proxy Agent and requires a less powerful computer to manage a larger number of supported systems.

Installers also have the option to **disable** SNMP Traps if the SNMP Proxy Agent is only used for alarming.

SNMP Set Capability

During the Proxy Agent installation, installers can also enable or disable the SNMP Set Capability.

This feature allows users on the NMS server to managed the tasks listed below from the DEFINITY Network Management product:

- Busy Out and release boards, ports, trunk groups and trunks
- Set system date and time

**SECURITY ALERT:**

Due to security limitations in the SNMP, installers should only *enable* the SNMP Set Capability *if* the Proxy Agent is behind a fire wall.

Enhanced Cut-Through

The Proxy Agent provides enhanced cut-through features to the user interface to the DEFINITY G3 and ECS systems. The enhancements include color screen displays and pop-up windows that display help and error messages.

The user at a Network Management System (NMS) has the ability to access the DEFINITY administration and management screens. From the NMS, the user telnets to the Proxy Agent computer, logs in, and initiates the emulation application to cut-through to the DEFINITY system.

In addition, users can manually connect to one or two managed nodes to conduct an emulation session from the Proxy Agent using the Communication Manager.

System Security

The Proxy Agent supports both DEFINITY login sessions and the Access Security Gateway (ASG) interface.

For non-DEFINITY managed nodes, the Proxy Agent provides a simple terminal emulation interface to access these systems.

Login Security

To safeguard access to the supported systems, Lucent **strongly** recommends that system administrators only grant the minimal permissions that the Proxy Agent needs to collect management data.

During installation, users should only enable SNMP Set Capability if the Proxy Agent is behind a **secure** fire wall.

Default Login screen

The DEFAULT LOGIN screen allows users to enter a system-wide **default** login and password or Access Security Gateway (ASG) key for DEFINITY systems. The system automatically displays the login and allows the user to modify the password on page F of the MANAGED NODES screen. Refer to [Chapter 10, "Default Login Administration"](#).

This feature reduces the time required to administer large numbers of new DEFINITYs on the Proxy Agent. With this feature, users do **not** have to manually connect to each DEFINITY system and save the login data.

ASG login

For DEFINITY systems that are protected by the Access Security Gateway (ASG) system, the Proxy Agent automatically generates a *response to a challenge* if the login and ASG key have already been administered when users administer new DEFINITYs on the Proxy Agent.

The procedure to ["Connect to DEFINITY Systems with ASG" on page 287](#) contain the steps to **manually** enter the response and challenge to login to an ASG-protected DEFINITY system.

SNMP Authentication

The Proxy Agent provides minimal SNMP authentication through the community strings and node names that users administer on the NETWORK MANAGERS screen and the MANAGED NODES screen.

The SNMP provides minimal authentication based on a valid community string in the SNMP messages. The SNMP uses the same mechanism to authorize NMS access to the MIB.

Proxy Agent Security

The Proxy Agent uses the standard SCO UnixWare login controls and permissions to authorize user login to the Proxy Agent applications.

PA001 Request Form

The CD-ROM for the DEFINITY Network Management Proxy Agent Release 3.0 contains the PA001 Administration Request form, entitled:

- PA001 Administration Request form

The Technical Services Center (TSC) require customers to complete the PA001 form in order to register their systems with these organizations.

Customers should also submit an updated PA001 form whenever they add new managed nodes to the Proxy Agent or make changes to their hardware, software, and network systems.

Customers can print the PA001 forms directly from the Proxy Agent CD-ROM.

New Features

This section contains a brief description of the new features, improvements, and changes to the Proxy Agent for release 3.0.

- Support for the SNMP traps and alarm traps from the systems listed below:
 - DEFINITY releases 7.1, 8.0, and 8.1, including Survivable Remote Processors (SRPs)
 - Multipoint Conferencing Unit (MCU) release 6.0
- Support for alarm traps from the systems listed below:
 - DEFINITY Audix release 4.0
 - INTUITY Audix releases 4.4 and 5.0
 - INTUITY Interchange releases 5.2 and 5.3
 - Call Management System (CMS) R3V8
 - Conversant release 7.0
- Added the user documentation listed below to the Proxy Agent CD-ROM:
 - Proxy Agent User Documentation for Installation and Administration
 - PA001 Administration Request forms
- Changed access to documentation on the UnixWare Desktop. The installation script now installs the documentation.
- Support for Access Security Gateway (ASG) to the DEFINITY systems and new login procedures for ASG-protected systems.

- Added new DEFAULT LOGIN screen to allow users to administer a system-wide **default** for login data for new DEFINITY systems. This feature reduces the time to administer large numbers of new DEFINITYs on the Proxy Agent.
- Added page F to the MANAGED NODES screen that displays the login data. The screen shows the login ID for DEFINITY systems and periods in the password/ASG Key fields. This allows for a specific login ID on a per managed node basis.
- When adding New DEFINITY systems to the Managed Nodes screen, Page F will display the login data from the default login screen.
- Support for the new Filter Set application to block alarm forwarding to INADS, including:
 - New commands on the PROXY ADMIN menu: add filter-set; change filter-set; display filter-set; and remove filter-set
 - New FILTER-SET screen
 - New Filter Set Name field on the revised MANAGED NODES screen
- Changes to the ALARM PATH screen and function. Removed the support to receive alarms from Trouble Trackers
- Support to enable or disable SNMP polling and SNMP traps during the installation process.

- Support for up to **600** managed nodes **only** if the Proxy Agent is used for alarming and the DEFINITY Network Management (DNM) product is **not** used. During installation, users must disable SNMP polling. Users can either enable or disable SNMP traps depending on their business requirements.
- Revised PA001 Administration Request forms (Rev. 12/99) to reflect the data that users enter at the installation prompts. For security reasons, the PA001 forms do **not** contain login and passwords data.

Supported Systems

The DNM Proxy Agent Release 3.0 product supports **both** SNMP communication and SNMP alarm traps for the systems listed below:

- DEFINITY G3 PBX release 4.0 and DEFINITY ECS releases 5.0 through 8.1
- Survivable Remote Processors (SRPs)
- MultiPoint Conferencing Unit (MCU) release 5.0 through 6.0.

The Proxy Agent treats SRPs and MCUs as DEFINITY systems.

The DNM Proxy Agent Release 3.0 supports **only** SNMP alarm traps from the systems listed below:

- DEFINITY Audix releases 3.1 through 4.0
- INTUITY Audix release 4.3 through 5.0 (with or without the remote maintenance board)
- INTUITY Interchange release 5.1 through 5.3
- Call Management System (CMS) R3V6 through R3V8
- Conversant release 7.0

System Requirements

The sections below outline the hardware and software products that are required for the DNM Proxy Agent Release 3.0 product.

Customers should work with their Lucent account team to determine the hardware requirements that meet their business and performance specifications. The Lucent account team uses the DOSS Configurator to configure the hardware requirements for the Proxy Agent stand-alone computer.

Hardware Certification

Lucent Technologies **requires** that the Proxy Agent hardware must be certified by The Santa Cruz Operation, Inc. (SCO).

The SCO maintains web sites where customers can find general information, SCO-certified hardware, and patches to upgrade the UnixWare.

See also Refer to ["Vendor References" on page 21.](#)

CAUTION:

Customers are solely responsible for the purchase, support, and maintenance of third-party hardware and software products that are required for this offer

The DEFINITY Solutions web site contains a list of recommended communications devices and I/O serial cards that are known to work with the Proxy Agent.

See also Refer to ["Lucent References" on page 19.](#)

Software Requirements

The Proxy Agent Release 3.0 operates on the UnixWare Operating System Release 2.1.3 (5-user version).

The DEFINITY Proxy Agent Release 3.0 product supports the DEFINITY Network Management (DNM) Release 3.0 products for UNIX systems and Windows NT systems.

Note: Earlier releases of the DNM products must be upgraded to release 3.0 in order to work with release 3.0 of the Proxy Agent.

Only the products listed below should reside on the Proxy Agent stand-alone computer:

- SCO UnixWare Operating System Release 2.1.3 (5-user version)
- DEFINITY Network Management Proxy Agent Release 3.0

Note: The SCO no longer supports the UnixWare Operating System release 2.1.3. Customers must obtain support and maintenance services from authorized third-party vendors. Microport is the authorized provider for Unixware 3.1.3. Refer to the SCO main web site listed in the ["Vendor References" on page 21](#) for more information.

Customers must remove all other software products from the Proxy Agent computer. Other products may interfere with the Proxy Agent's operation and communication devices.

Ensure you run DEFINITY Network Management Release 3.0 UNIX or NT Version.

Overview of the User Documentation

The sections below briefly outline the chapter contents in Proxy Agent User Documentation (this book).

The individual chapters provide the essential information to install, administer, and maintain the Proxy Agent. The chapters contain screen layouts, field descriptions, and step-by-step procedures.

Target Audiences

The target audiences for the Proxy Agent User Documentation include both technical users and general users at all levels.

- System administrators
- Network managers
- Technical Services Center engineers
- Lucent field technicians and installers
- Lucent consulting groups, NetCare, SDSC, and others
- Lucent account executives and project teams
- Global Services Organization and local support vendors for international customers

All users need to have working knowledge of the hardware and software listed below:

- UNIX systems
- SCO UnixWare Operating System

- Network Management Systems (NMS) platforms, OpenView and NetView
- Windows NT platform
- Hardware connectivity
- Software installation and integration

In addition, the User Documentation is an essential resource for users who are unfamiliar with the purpose and operation of the Proxy Agent.

Customer Pre-Installation Tasks

The information in [Chapter 2, "Customer Pre-Installation Tasks"](#) outlines the tasks that customers must complete prior to the installation of the Proxy Agent.

The pre-installation tasks also include two important requirements:

- Completion of the PA001 Administration Request form and
- Execution of the Platform Acceptance Test

Proxy Agent Installation

The information in [Chapter 3, "Proxy Agent Installation"](#) contain the essential checklists to install and administer the Proxy Agent and post installation checklists to ensure the system is functioning properly.

The chapter also contains the procedures to install a new Proxy Agent and to upgrade earlier releases of the Proxy Agent.

Help Screens and Commands

The information in [Chapter 4, "Help Screens and Commands"](#) primarily targets **new** users who are unfamiliar with the Proxy Agent.

This chapter contains descriptions of the help screens, commands, and hotkeys (keyboard shortcuts) that are available from Proxy Agent menus and application screens.

The Format Conventions are used in the procedure steps to help users input the correct information to execute specific tasks.

Access Procedures

The information in [Chapter 5, "Access Procedures"](#) also targets **new** users.

This chapter contains the basic procedures to log in to the Proxy Agent and to access the Proxy Agent applications.

The chapter also contains the procedures to **start** and **stop** the Proxy Agent and to view the STATUS screen.

Network Managers Administration

The purpose of the NETWORK MANAGERS screen is to provide the Network Management System (NMS) with access to the SNMP data collected from the managed nodes. Refer to [Chapter 6, "Network Managers Administration"](#).

The NMS applications use the SNMP data to populate the tables and graphical displays in the appropriate DEFINITY Network Management (DNM) screens.

Default Location Administration

The purpose of the DEFAULT LOCATION screen is to administer the system-wide, default location submaps for supported systems. Refer to [Chapter 7, "Default Location Administration"](#).

Users can override the default location map for individual managed nodes from the MANAGED NODES screen on the Proxy Agent and from the NMS network server.

Alarm Path Administration

The purpose of the ALARM PATH screen is to administer the system-wide, default settings for the communication devices that receive alarms and forward alarms.

To activate alarm forwarding, users must administer the alarm source fields and the alarm destination fields on the ALARM PATH screen. Refer to [Chapter 8, "Alarm Path Administration"](#).

Users can turn on or turn off the alarm forwarding option for individual managed nodes on the MANAGED NODES screen.

Filter-Set Administration

The Proxy Agent provides a new alarm filtering feature that allows users to block the forwarding of certain alarms. Refer to [Chapter 9, "Filter Set Administration"](#).

Users can create sets of filtering criteria on the FILTER SET screen and then apply the filter set to all or individual systems on the MANAGED NODES screen.

Default Login Administration

The DEFAULT LOGIN screen allows users to enter a system-wide **default** login and password or Access Security Gateway (ASG) key for DEFINITY systems. The system automatically displays the login and allows the user to modify the password on page F of the MANAGED NODES screen. Refer to [Chapter 10, "Default Login Administration"](#).

This feature reduces the time to administer large numbers of new DEFINITYs on the Proxy Agent. With this feature, users do **not** have to manually connect to the system on the COMMUNICATION MANAGER screen and save the login data.

Managed Nodes Administration

The MANAGED NODES screens contain the individual settings and options for each supported system that users administer on the Proxy Agent. Refer to [Chapter 11, "Managed Nodes Administration"](#).

Generally, users administer all management tasks from the MANAGED NODES screen.

Communication Application

The purpose of the Communication application is to manually connect the Proxy Agent to managed nodes to troubleshoot connection problems.

Refer to [Chapter 12, "Communication Application"](#) for the procedures to manually connect and disconnect the Proxy Agent to and from the managed nodes. The procedures contain the login prompts to access managed nodes and DEFINITY systems that are protected by the Access Security Gateway (ASG) software.

Emulation Application

The purpose of the Emulation application is to provide communication access to a managed node for real-time administration.

Refer to [Chapter 13, "Emulation Application"](#) for the procedures to establish an emulation session from the Proxy Agent with one or two managed nodes.

Configuration Application

The purpose of the Configuration application is to administer the system-wide, default parameters for the communication devices and configuration options for the monitor and screen elements.

[Chapter 14, "Configuration Application"](#) contains screen descriptions and procedures to administer the two configuration screens listed below:

- The CHANGE HARDWARE screen contains the software versions for UnixWare and Proxy Agent and the system-wide default parameters for the serial ports.
- The CHANGE USER-INTERFACE screen contains the configuration options for the monitor and screen elements.

I/O Setup Application

The I/O Setup application allows system administrators (root users) to edit the Devices file and the Dialers file.

[Chapter 15. "I/O Setup Application"](#) contains the default dial strings and the procedures to edit the Devices and the Dialers files.

Maintenance and Troubleshooting

The information in [Chapter 16. "Maintenance and Troubleshooting"](#) contains utilities and logs to allow the system administrator to maintain the Proxy Agent and troubleshoot problems with alarms, traps, and system errors.

The chapter also contains an example of a Test Trap script to test an event configuration on the Network Management System (NMS).

2 Customer Pre-Installation Tasks

Chapter Contents

- [Introduction](#) [59](#)
- [Plan the Connectivity](#) [60](#)
- [Complete the PA001 Form](#) [72](#)
- [Install the UnixWare Operating System](#) [73](#)
- [Administer the Communication Devices](#) [76](#)
- [Administer Security Options](#) [78](#)
- [Change the Dip Switch Settings](#) [81](#)
 - [Settings for AT&T 2224CEO Modems](#) [81](#)
 - [Settings for 7400B/B+ Data Modules](#) [82](#)
 - [Settings for PDMs](#) [83](#)
 - [Settings for MPDMs](#) [85](#)
- [Set the Interface for 7400A Modules](#) [86](#)
- [Execute the Platform Acceptance Test](#) [87](#)

Introduction

Customers are **solely** responsible for completing the pre-installation tasks described in the sections below:

- 1 Plan the Proxy Agent connectivity, with help from the Design Specification
- 2 Complete the PA001 Administration Request form, with help from the Design Specification
- 3 Install or upgrade the UnixWare Operating System
- 4 Connect the communication devices
- 5 Execute the Platform Acceptance Test, with support from the Technical Services Center (TSC)

Customers must complete all of the pre-installation tasks **prior** to the installation of the Proxy Agent product.



CAUTION:

This is a **software-only** offer. **Lucent Technologies** is **solely** responsible for the support and maintenance of the product software. **Customers** are **solely** responsible for the purchase, support, and maintenance of third-party hardware and software products that are *required* for this offer.

Plan the Connectivity

The customer and the project team work together to plan the Proxy Agent connectivity between the DEFINITY system and the Network Management System (NMS).

The figures in this section show the basic configurations designs and required hardware:

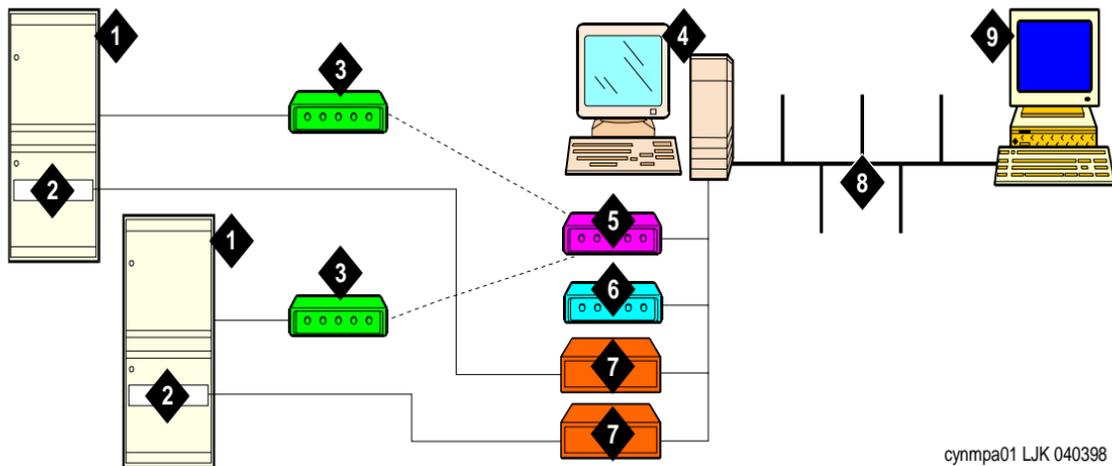
- ["Connectivity overview" on page 61](#)
- ["Hardware for communication devices" on page 66](#)
- ["Cable connections for local analog modems" on page 68](#)
- ["Cable connections for remote analog modems" on page 69](#)
- ["Cable connections for digital data modules" on page 70](#)
- ["Cable connections for an ADU with a moss adaptor" on page 71](#)

See also For more detailed configurations, visit the web site for the Sales and Design Support Center (SDSC). Refer to ["Lucent References" on page 19](#).

Connectivity Overview

The figure below shows a high-level view of the Proxy Agent connectivity between DEFINITY systems and the Network Management System (NMS):

Connectivity Overview



cynmpa01 LJK 040398

- 1 DEFINITY systems
- 2 Netcon channels or system ports
- 3 External or internal INADS modem connected to the DEFINITY systems
- 4 Proxy Agent computer
- 5 Proxy Agent alarm **receiver** modem
- 6 Proxy Agent **sender** modem to forward alarms to INADS
- 7 Static or Dynamic dial-up device to poll the system. The device can be an analog modem, digital data module, ADU, **or** a direct connection
- 8 Local Area Network (LAN)
- 9 Network management station (NMS) where the DEFINITY Network Management products reside

Figure 2. Connectivity overview

Connectivity Overview

Alarm stream In figure 1, the alarm stream between the DEFINITY system and the Proxy Agent contains two dedicated analog modems:

- The INADS modem on the DEFINITY system (callout 3) is usually an internal modem that is integrated on a circuit pack. The Prologix system requires an external INADS modem.
- The Proxy Agent modem that **receives** the alarm from the DEFINITY system (callout 5)

The alarm stream can also contain a Proxy Agent modem that **sends** alarms to the INADS or a Trouble Tracker modem. This option is not shown in Figure 1.

Dial-up connections Figure 1 only shows a permanent dial-up connection between the DEFINITY system and the Proxy Agent (callout 7). You can also add a temporary dial-up connection to cut-through from the Network Management Station (NMS) to the Proxy Agent computer in order to administer the DEFINITY system.

Dial-up connections may use the public network to connect the Proxy Agent computer to the DEFINITY system.

Analog dial-up connections Analog dial-up connections to the DEFINITY system require modem pooling on the system.

Multiple dial-up connections Multiple dial-up connections allow simultaneous connections to the DEFINITY system for administration. Administration terminals can be the Proxy Agent computer or any other type of administration terminals.

- The **DEFINITY G3r** systems allow up to 8 simultaneous administration logins on the system. However, only 5 administration commands can be used at one time.
- The **DEFINITY G3i V4** systems allow up to 3 simultaneous administration logins.
- The **DEFINITY G3i V5** systems allow up to 5 simultaneous administration logins. However, only 1 administrative command can be used at a time.

See also Refer to the DEFINITY product documentation for more information about multiple dial-up connections and administration of the system.

Data Communication Hardware

It is essential that customers use only communication hardware that is **certified** by Lucent Technologies. Equally important is that customers follow the Lucent certified diagrams to configure the hardware connections.

Circuit Packs

The table below matches the communication device and the line type to appropriate the circuit pack.

Note: The TN numbers for the circuit packs are for use in the U.S.A. International users must check the **DEFINITY Application Notes** for the correct circuit pack.

Table 3. Circuit pack selection

| Communicate Device | Line Type | Circuit Pack |
|-------------------------------|-----------|------------------|
| Any supported modem | Analog | TN746 and TN742 |
| Data modules 7400B and 7400B+ | Digital | TN754 |
| Data module 8400B+ | Digital | TN2181 or TN2224 |
| ADU | Data | TN726B |
| | | |

Hardware requirements

The connections between the DEFINITY system and the Proxy Agent computer requires various types of hardware that are described below:

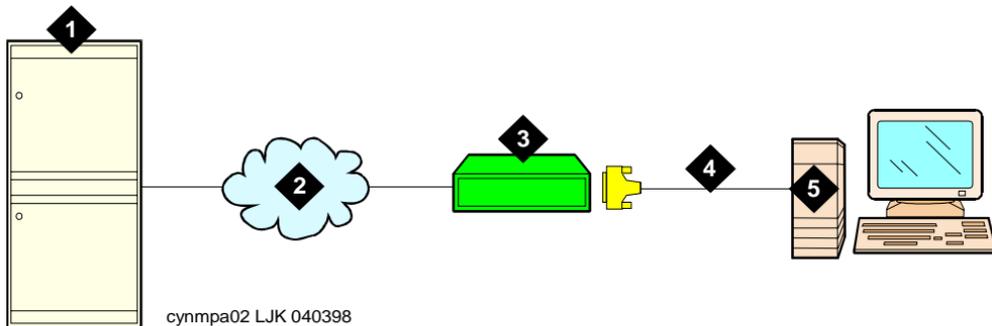
- Communication devices including:
 - Analog modems
 - Digital data modules (7400A, 7400B, 7400B+, or 8400B+),
 - Asynchronous Data Units (ADUs)
 - Direct connections
- House wiring and cables for the Local Area Network (LAN)
- Gender changers between the connections

The table below lists hardware requirements for a public or private network.

Table 4. Hardware requirements for network connections

| Network Type | Communication Device | Distance from DEFINITY system | Hardware Requirements |
|--------------|----------------------|-------------------------------|---|
| Public | Any supported modem | Unlimited | Modem pooling on the DEFINITY system |
| Private | Digital data module | Within 5000 feet | A port on a digital board (TN754 in the U.S.A.) |
| | ADU | Within 2000 feet | A port on a dataline board (TN726E in the U.S.A.) |
| | | | |

Figure The figure below shows hardware for communication devices.



- 1 DFINITY system with circuit packs: TN754C, TN2181, and TN2224
- 2 Site-specific network connection
- 3 Communication device that is either an analog modem, a digital data module, **or** an ADU with a moss adapter
- 4 Serial I/O modular adapter and cable that connects the device to a serial port on the Proxy Agent computer
- 5 Proxy Agent computer

Figure 3. Hardware for communication devices

Cables for Communication Devices

The figures in this section illustrate the cable connections for the various communication devices, including:

- ["Cable connections for local analog modems" on page 68](#)
- ["Cable connections for remote analog modems" on page 69](#)
- ["Cable connections for digital data modules" on page 70](#)
- ["Cable connections for an ADU with a moss adaptor" on page 71](#)

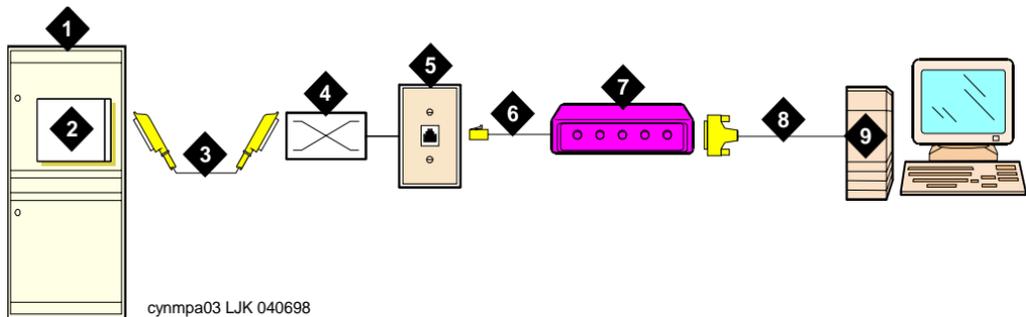
The type of DEFINITY system does **NOT** affect the cabling for communication devices.

See also

Refer to the documentation from the vender to:

- Install the correct cables to connect a modem to the computer
- Install the port card hardware and software on the computer

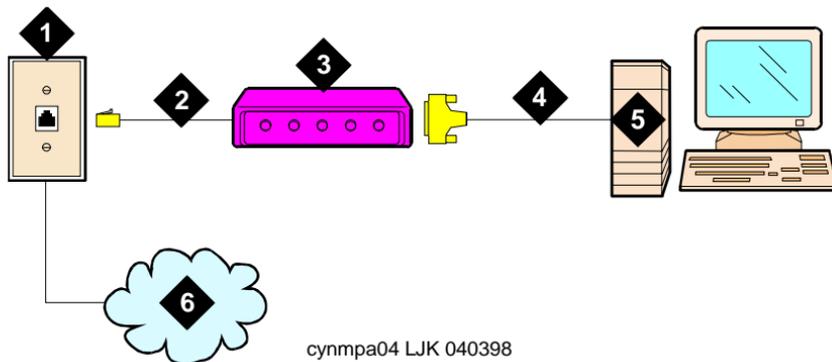
Figure The figure below shows the cable connections for **local** analog modems:



- 1 DEFINITY system with modem pooling
- 2 Analog line circuit pack on the DEFINITY system
- 3 B25A cable with connectors
- 4 Cross-connection at main distribution frame
- 5 103A or wall jack
- 6 RJ11 cable to the analog modem
- 7 Analog modem
- 8 Serial I/O modular adapter and cable that connects the device to a serial port on the Proxy Agent computer
- 9 Proxy Agent computer

Figure 4. Cable connections for local analog modems

Figure The figure below shows the cable connections for **remote** analog modems:



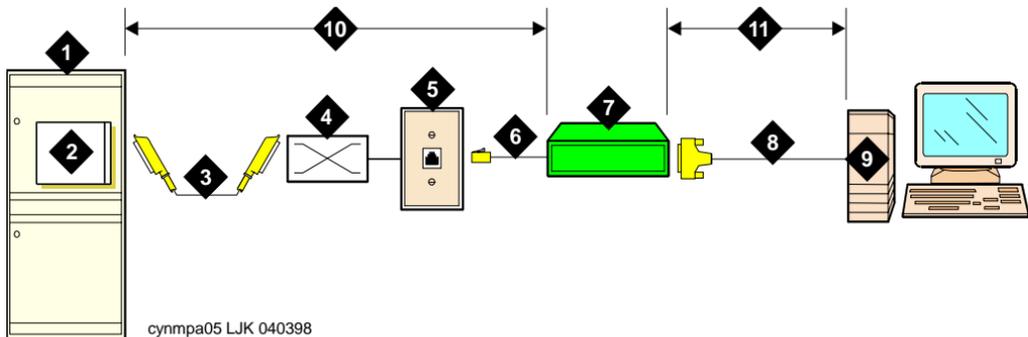
- | | |
|---------------------------|---|
| 1 103A or wall jack | 4 Serial I/O modular adapter and cable that connect the device to a serial port on the Proxy Agent computer |
| 2 RJ11 cable to the modem | 5 Proxy Agent computer |
| 3 Analog modem | 6 Analog public or private network |

Figure 5. Cable connections for remote analog modems

2 Customer Pre-Installation Tasks

Cables for Communication Devices

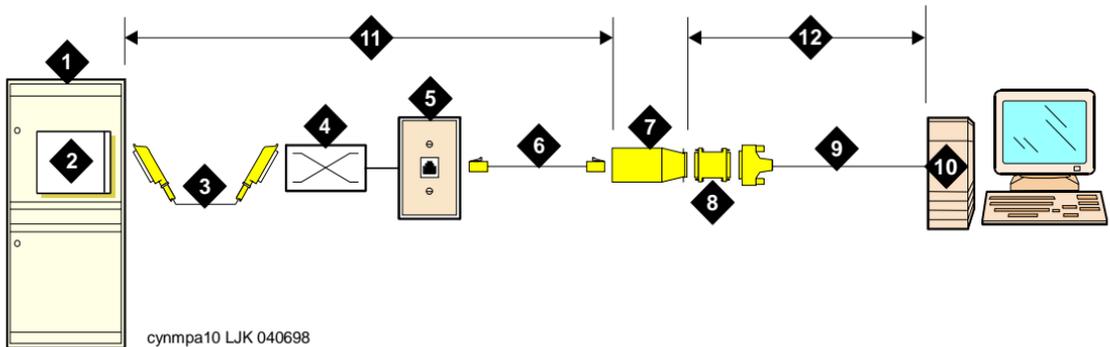
Figure The figure below shows the cable connections for digital data modules and maximum distance between systems:



- | | |
|---|--|
| <p>1 DEFINTY system</p> <p>2 Digital line circuit pack on the DEFINTY system</p> <p>3 B25A cable with connectors</p> <p>4 Cross-connection at main distribution frame</p> <p>5 103A or wall jack</p> <p>6 D82-87 cable to the digital data module</p> | <p>7 Digital data module</p> <p>8 Serial I/O modular adapter and cable that connects the device to a serial port on the Proxy Agent computer</p> <p>9 Proxy Agent computer</p> <p>10 Maximum of 5000 feet between the DEFINTY system and the data module</p> <p>11 Maximum of 50 feet between the data module and the Proxy Agent computer</p> |
|---|--|

Figure 6. Cable connections for digital data modules

Figure The figure below shows the cable connections for an ADU with moss adaptor and maximum distance between systems:



- | | |
|---|---|
| <p>1 DEFINITY system</p> <p>2 Digital line circuit pack on the DEFINITY</p> <p>3 B25A cable with connectors</p> <p>4 Cross-connection at main distribution frame</p> <p>5 103A or wall jack</p> <p>6 D82-87 cable to the digital data module</p> <p>7 ADU</p> | <p>8 Moss adaptor</p> <p>9 Serial I/O modular adapter and cable that connects the device to a serial port on the Proxy Agent computer</p> <p>10 Proxy Agent computer</p> <p>11 Maximum of 2000 feet between the DEFINITY system and the data module</p> <p>12 Maximum of 50 feet between the data module and the Proxy Agent computer</p> |
|---|---|

Figure 7. Cable connections for an ADU with a moss adaptor

Complete the PA001 Form

The Technical Services Center (TSC) **requires** all U.S.A. and Canadian customers to register their systems with the TSC. Customers must complete the **PA001 Administration Request** and fax the form to the TSC.

International customers

International customers must work with their local service organizations to plan and install their systems and software.

International customers must complete the **PA001 Administration Request** and fax the form to the Tier IV Registry. Instructions are on the Fax Cover Sheet.

The local service organization should also fax the completed PA001 form to ITAC.

Updates to the PA001 form

Customers only need to complete the portions of the form that pertain to the upgrades or changes to their systems and fax those pages to the TSC.

Customers must update the PA001 form whenever they:

- Upgrade the system hardware and software
- Change or upgrade the network and Network Management System (NMS) platform
- Add, delete, or change data for the managed nodes or communication devices

Customers can print the **current** version of the PA001 form directly from the Proxy Agent CD-ROM for this release.

Install the UnixWare Operating System

Customers are **solely** responsible for the requirements listed below:

- Procure and set up the SCO-certified hardware for the Proxy Agent computer
- Install and configure the UnixWare operating system.



CAUTION:

Lucent Technologies does **not** install, support, or maintain the SCO UnixWare operating system or other vendor hardware and software products.

UnixWare Upgrade Patches

The SCO web site contains patches to upgrade to the UnixWare Operating System Release 2.1.3. Users can only use the upgrade patches if UnixWare 2.1.0 or later is installed on the Proxy Agent computer. Refer to ["Vendor References" on page 21](#) for the web address.

Users must verify which release of UnixWare is installed on the Proxy Agent computer. Refer to CHANGE HARDWARE screen.

Then execute **one** of the options below:

- If UnixWare 2.1.0 or later is installed, then install the UnixWare 2.1.3 upgrade patch from the SCO web site.
- If a release of UnixWare prior to release 2.1.0 is currently installed, then you must complete a Destructive installation of the UnixWare 2.1.3 operating system. Non-destructive upgrades of the UnixWare 2.0.x and earlier versions, have been error-prone.

UnixWare Installation Tasks

Customers must complete the tasks below to install the UnixWare operating system:

- 1 **Set up** the SCO-certified Proxy Agent computer hardware:
 - Install the network interface card
 - Install the host bus adapter
 - Install the serial I/O port cards
- 2 **Install** the UnixWare Release release 2.1.3 on the Proxy Agent computer.
- 3 **Add** the packages below to UnixWare:
 - **bsdcompat** -- BSD compatibility
 - **bkrs** -- Extended backup and restore
 - **ccs** -- Optimizing C compilation system
 - **cmds** -- Advanced commands
 - **oam** -- Operations, administration & maintenance
 - **terminf** -- Terminfo utilities
 - **manpages** -- Traditional manual pages
- 4 **Delete** the packages below from UnixWare:
 - **nwnet** -- NetWare Networking
 - **nuc** -- NetWare UNIX Client
 - **nwsup** -- NetWare Integration Kit

5 *Disable* the plug-n-play cards for all add-on interface cards installed on the Proxy Agent computer. Unixware 2.1.3 does **not** support plug and play hardware. Some plug-n-play cards use interrupts or I/O addresses that have been previously assigned to other hardware devices and drivers. Unless you disable the plug-n-play, you may experience installation difficulties.

UNIX backup

Lucent strongly recommends that users backup the UNIX system at least twice a month.

- For tape drive backups, perform a full system backup and then reboot the UNIX system.
- For backups on floppy diskettes, backup the **/usr/g3-ma** directory and then reboot the UNIX system.

Administer the Communication Devices

Customers must complete the tasks below to connect the communication devices:

- 1 Administer the TCP/IP connections:
 - Configure the Ethernet/Token Ring interface
 - Set up the IP address in the **Hosts** file
 - Test the TCP/IP connection
- 2 Verify that the routing table contains the default router command
- 3 Configure Dial-In access to the DEFINITY system for system management access. This may entail Data Modules, Modem Pools, and/or System Port/Netcon Channels and Hunt Groups.
 - On DEFINITY G3r systems, the **system port** is an administered resource and requires a *data board* and *pdata board*. You execute the commands below to administer the system port:
 - Execute the ***add data-module*** command to assign the system port to an extension.
 - Execute the ***add hunt-group*** command to add the system port extension as a member of a hunt group.
 - On DEFINITY G3i systems, the **netcon port** is an internal channel that you can assign as a port. You execute the commands below to administer the netcon port:
 - Execute the ***add data-module*** command to assign the netcon port to an extension.
 - Execute the ***add hunt-group*** command to add the netcon port extension as a member of a hunt group.

- 4 Execute the **add station** command to administer the devices below:
 - Analog line
 - Digital voice and data module
 - Digital data-only module (may require modem pooling)
 - ADU
- 5 To forward alarms to INADS or to the Proxy Agent for DEFINITY G3 systems, execute the command, **change system-parameters maintenance** and enter the phone number in the *OSS Telephone Number* field 1 or 2.
- 6 The DEFINITY ECS systems are set up to forward alarms to INADS. To also set up the Proxy Agent to receive and forward alarms, then
 - Enter the phone numbers for both the INADS and Proxy Agent on the form entitled, **Maintenance-Related System Parameters**.
 - Execute the command **change system-parameters maintenance**, then enter the telephone number for the Proxy Agent in one of the *OSS Telephone Number* fields.
- 7 To set up the Proxy Agent to receive alarms from other types of supported system, enter the phone number for the Proxy Agent alarm receiver devices on the systems.

Administer Security Options

Customers must complete the tasks below to administer the security options:

- 1 For DEFINITY systems, execute the commands below:
 - ***add login*** [*name*]
 - ***change permissions*** [*login name*], then
 - Enter **Y** in the fields entitled: *Display Admin and Maint Data* and *System Measurements*.
 - Set the permissions to “**browse only**” or “**non-superuser read-only**”

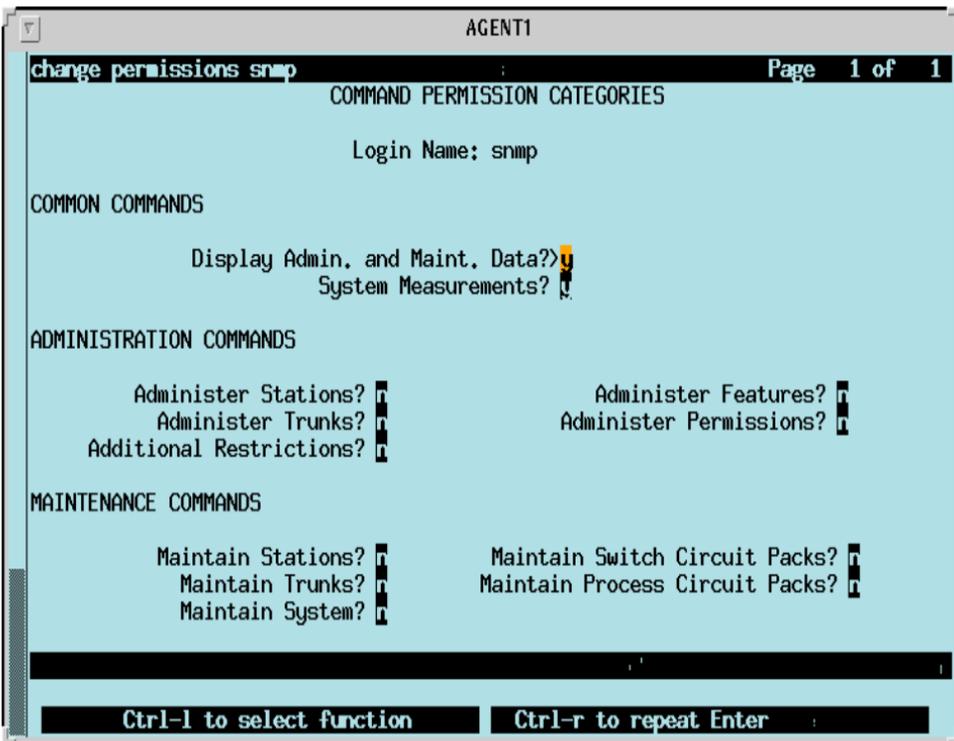


Figure 8. Browser Change Permissions SNMP

2 Customer Pre-Installation Tasks

Administer Security Options

- Disable the “**password-aging**” feature
 - All other fields on the form should be set to **No**
 - Fields for basic DPA use no SNMP Sets:
 - Display Admin and Maintenance Data = y
 - System Measurements = y
 - Busy/Release use of DPA w/snmp sets and above plus:
 - Maintain Stations = y
 - Maintain Trunks = y
 - Maintain System = y
 - Maintain Switch Circuit packs = y
 - Maintain Process circuit packs = y
- 2 For other types of supported systems, access the appropriate forms and administer the security options below:
- Set the permissions to “**browse only**,” unless the users wants to be able to do bus-outs/releases and set DEFINITY time via SNMP. SNMP sets requires Maintenance and Administrator permissions.
 - Disable the “**password-aging**” feature

Change the Dip Switch Settings

Customers may need to change the dip switch settings for each communication device that is connected to the Proxy Agent.

The tables in this section contain the dip switch settings for the data communications devices listed below:

- AT&T 2224CEO analog modem
- 7400B/B+ data module
- Port data module (PDM)
- MPDM

Settings for AT&T 2224CEO Modems

For the AT&T 2224 CEO analog modem, change the dip switches on the front panel of the modem:

- 1 Set dip switch **#1** to the **up** position
- 2 Set dip switch **#6** to the **up** position
- 3 All other dip switches must be in the **down** position.

Note: The AT&T 2224CEO modem is **not** certified for Proxy Agent modems that **send alarms** to INADS or a Trouble Tracker.

Settings for 7400B/B+ Data Modules

For 7400B/B+ data modules, change the dip switches to match the settings in the table below.

Table 5. Dip switch settings for 7400B/B+ modules

| Data Module | Dip Switch Setting |
|--|--|
| Stand alone, data-only: <ul style="list-style-type: none">• 7400B• 7400B+ | <ul style="list-style-type: none">• Change the SW1 dip switch to the on position• All other dip switches should be in the off position |
| Voice-and-data: <ul style="list-style-type: none">• 7400B• 7400B+ | All dip switches should be in the off position. This module requires a connection to a digital phone and is rarely used with the Proxy Agent. |
| | |

Settings for PDMs

For PDMs, change the dip switches to match the settings in the table below.

Note: For **9600** baud, the dip switch must be set to the **ON** position.

Table 6. Dip switch settings for PDMs

| Dip Switch | Setting | Dip Switch | Setting |
|------------|---------|------------|---------------|
| LOW | OFF | PRTY | OFF |
| 300 | OFF | I/OD | OFF |
| 1200 | OFF | DMLL | OFF |
| 2400 | OFF | MKBY | OFF |
| 4800 | OFF | SPARE | (none) |
| 9600 | ON | SIGLS | ON |
| 19.2 | OFF | AANS | ON |
| SPARE | (none) | DL-HI | OFF |
| SPARE | (none) | CN25 | OFF |
| SPARE | (none) | CN18 | OFF |
| HDX | OFF | RL21 | OFF |
| SYNC | OFF | CI12 | OFF |
| | | | <i>1 of 2</i> |

Table 6. Dip switch settings for PDMs

| Dip Switch | Setting | Dip Switch | Setting |
|------------|---------|------------|---------------|
| INT | OFF | PRTY | OFF |
| DISC | OFF | I/OD | OFF |
| KYBD | ON | DMLL | OFF |
| | | | <i>2 of 2</i> |

Settings for MPDMs

For MPDMs, change the dip switches to match the settings in the table below.

Note: For **9600** baud, the dip switch must be set to the **ON** position.

Table 7. Dip switch settings for MPDMs

| Dip Switch | Setting | Dip Switch | Setting |
|------------|---------|------------|---------|
| LOW | OFF | SYNC | ASYN |
| 300 | OFF | INT | EXT |
| 1200 | OFF | DISC | OFF |
| 2400 | OFF | KYBD | OFF |
| 4800 | OFF | PRTY | OFF |
| 9600 | ON | I/OD | OEN |
| 19.2 | OFF | DMLL | OFF |
| 56K | OFF | MKBY | OFF |
| 64K | OFF | SPARE | (none) |
| TRDK | OFF | SIGLS | OFF |
| HDX | FDX | AANS | OFF |
| LOW | OFF | SYNC | ASYN |
| | | | |

Set the Interface for 7400A Modules

For the 7400A data modules, customers must set the interface on the device before you connect the device to the Proxy Agent computer.

- 1 On the front panel of the module, set the interface control:
 - Press **Next/No** until the system displays the prompt: `SET INTERFACE?`
 - Press **Enter/Yes**

If the `SET INTERFACE?` prompt does **NOT** display, then

- Continuously press **Next/Yes** until the system displays the `SET INTERFACE?` prompt
- Press **Enter/Yes**

Result: The system displays the prompt: `INT = AT COMM?`

- 2 Press **Enter/Yes** to exit.

Result: The data module resets the interface and performs a self test.

Execute the Platform Acceptance Test

Both the customer and a TSC engineer work together to execute the Platform Acceptance Test.

The purpose of the Platform Acceptance Test to:

- Verify that the Network Management Station (NMS) is functioning
- Verify that the correct version of the UnixWare operating system is installed
- Verify that the modem connection is functioning

Required materials

Customers need the materials and information listed below:

- Root login and password
- PA001 form

Procedure

Complete the procedure below to execute the Platform Acceptance Test.

- 1 The user calls the TSC to set up the test. For the TSC Technical Support phone number, refer to ["Lucent References" on page 19](#).
- 2 To begin the test, ping the NMS from the Proxy Agent computer.

At the UNIX prompt:

- Type `/usr/sbin/ping [nms_name]`
- Press **ENTER**

Result: The system displays the message: `[nms_name] is alive`

Execute the Platform Acceptance Test

- 3 Verify the release number for the UnixWare software.

At the UNIX prompt:

- Type **uname -v**
- Press **ENTER**

Result: The system displays the UnixWare release number: 2.1.3

- 4 Hook-up a modem to a serial card port on the Proxy Agent. For the UNIX device name, refer to the **Devices** section on the PA001 form.

At the UNIX prompt, connect the device:

- Type **cu -s 9600 -l /dev/[device name]**
- Press **ENTER**

Result: The system displays the message: `Connected`

- 5 At the UNIX prompt, verify the connection:

- Type **at&f**
- Press **ENTER**

Result: The system displays the message: `OK`

- 6 At the UNIX prompt, disconnect the modem:

- Type **~.**
- Press **ENTER**

Example: Type: tilde (~) period (.) with **no** space between them.

Result: The system displays the message: `Disconnected`

- 7 At the completion of the test, go to the **Proxy Agent** section of the PA001 form and complete the field listed below:
Platform Acceptance Test completed by:
 - In the *Name* field, enter the name customer's employee who completed the test with the TSC
 - In the *Date* field, enter the date of the test
- 8 Complete the fields on the Fax Cover Sheet. Then, fax the completed PA001 form to TSC at the telephone number on cover sheet.

3 Proxy Agent Installation

Chapter Contents

- [Introduction](#) [91](#)
- [Installation Checklists](#) [93](#)
- [Installation Prompts](#) [98](#)
- [Serial I/O Subsystem](#) [104](#)
- [Install the New Proxy Agent](#) [106](#)
- [Upgrade from Proxy Agent 2.0 and Later](#) [116](#)
- [Upgrade from Proxy Agent 1.4 and Earlier](#) [126](#)
- [Remove the Proxy Agent](#) [128](#)

Introduction

This chapter contains the procedures to install the **DEFINITY Proxy Agent Release 3.0** product as a new or upgrade installation.

Pre-installation tasks

Customers must complete all of the pre-installation tasks **before** they install the new Proxy Agent product or upgrade the current Proxy Agent product. Refer to chapter 2, "[Customer Pre-Installation Tasks](#)" on page 58.

Installation checklists

The section entitled "[Installation Checklists](#)" on page 93 contain the lists below:

- The installer completes the Installation Tasks Checklist during the installation.
- The installer and the TSC complete the Technical Verification Checklist after the installation.
- The TSC and the customer complete the Customer Acceptance Checklist after the installation.

Installation procedures

The installation procedures are divided into separate sections for either a new installation or an upgrade to the current release:

- For a **new** installation of the Proxy Agent, refer to "[Install the New Proxy Agent](#)" on page 106.
- For an **upgrade** of an existing Proxy Agent, refer one of the sections below that matches the release number of the product currently installed:
 - "[Upgrade from Proxy Agent 2.0 and Later](#)" on page 116
 - "[Upgrade from Proxy Agent 1.4 and Earlier](#)" on page 126

Post installation options The system administrator (root user) can execute the maintenance options listed below **after** the Proxy Agent has been installed:

- ["Add New Devices" on page 336](#)
- ["Change Settings for SNMP Access" on page 337](#)

User documentation The installation script for this release automatically copies the Proxy Agent User Documentation to the **lucntdoc** directory.

Users can access the documentation only from the UnixWare Desktop. Refer to the procedure to ["Access the User Documentation" on page 150.](#)

Installation Checklists

The installation checklists contain the tasks that installation technicians must complete to install the new Proxy Agent 3.0 or upgrade to the Proxy Agent 3.0.

The ["Installation Tasks Checklist" on page 94](#) contains the tasks that installers must execute **during** the installation process.

The ["Technical Verification Checklist" on page 96](#) contains the **post installation** tasks that the installation technician and the engineer at the Technical Services Center (TSC) must complete to insure that the Proxy Agent is properly administered and functioning.

The ["Customer Acceptance Checklist" on page 97](#) contains the **post installation** tasks that the engineer at the TSC and the customer must complete to insure that the customer can operate the Proxy Agent and accepts the installation as complete.

The checklists only contain references to procedures. If installers are unfamiliar with the Proxy Agent applications, then they should read the introduction and the screen description sections that precede the procedure section.

Installation Tasks Checklist

Installers must execute the installation tasks listed below in the order presented.

- 1 Verify that all tasks in [Chapter 2, "Customer Pre-Installation Tasks"](#) have been completed.
- 2 Call the Technical Services Center (TSC) to verify that the procedure to ["Execute the Platform Acceptance Test" on page 87](#) has been completed.
- 3 Assemble the required materials and information, including:
 - Root name and password
 - Default **login ID** and **password** or **ASG secret key** for new DEFINITY systems
 - New password for the **g3maadm** login
 - Completed PA001 form
 - CD-ROMs DEFINITY Network Management Proxy Agent Release 3.0
 - Printed copy of the DNM 3.0 Proxy Agent User Documentation for Installation and Administration (this book)
 - Technical Services Center (TSC) number: **1-800-242-2121**, ext. **8-6767**
- 4 Execute **one** of the installation procedures (a, b, or c) listed below:
 - a ["Install the New Proxy Agent" on page 106.](#)
 - b ["Upgrade from Proxy Agent 2.0 and Later" on page 116](#)
 - c ["Upgrade from Proxy Agent 1.4 and Earlier" on page 126](#)
- 5 Complete the procedure to ["Administer the Network Managers" on page 179.](#)
- 6 Complete the procedure to ["Administer the Default Location" on page 191.](#)

Installation Tasks Checklist

- 7 Complete the procedure to ["Administer the Alarm Path" on page 199.](#)
- 8 Complete the procedure to ["Administer the Filter Sets" on page 219.](#)
- 9 Complete the procedure to ["Administer the Default Login" on page 235](#)
- 10 Complete the procedure to ["Administer the Managed Nodes" on page 265](#)
- 11 Complete the tasks on the ["Technical Verification Checklist" on page 96.](#)
- 12 Complete the tasks on the ["Customer Acceptance Checklist" on page 97.](#)

Technical Verification Checklist

The Technical Verification Checklists contains the **post installation** tasks. The engineer at the Technical Services Center (TSC) validates the completion of the tasks below:

- 1 Verify that the **customer** completed and faxed **PA001** form to the TSC.
- 2 Verify that the **TSC** has updated the System Management database with the current data from the PA001 form.
- 3 Verify that all of the tasks on the ["Installation Tasks Checklist" on page 94](#) have been completed.
- 4 Verify that the Proxy Agent is connected to each managed node.
- 5 If "alarm forwarding" is active, then check the ALARM PATH screen to verify that both the source and destination fields are properly administered. Refer to ["Administer the Alarm Path" on page 199](#). Then validate that "alarm forwarding" is properly functioning:
 - Verify that the Proxy Agent can **receive** alarms from each managed node and **forward** alarms to INADS
 - Verify that INADS **received** each alarm that was sent to them
 - Verify that INADS **created** a TSC-SS ticket for each alarm
- 6 If "alarm forwarding" is administered for DEFINITY ECSs, then verify that both INADS and the Proxy Agent can **receive** alarms. If INADS cannot receive the alarms, then execute a **test inads-line** command for each ECS.
- 7 Verify that the TSC login and password for **root2** and **ncsc** have been administered. Lucent uses these logins to conduct maintenance tasks.

Customer Acceptance Checklist

The engineer at the Technical Services Center (TSC) works with the customer to validate the **post installation** tasks on the **Customer Acceptance** checklist below.

- 1 Verify that the customer can log in to the Proxy Agent from both the UNIX shell or the UnixWare Desktop. Refer to the procedures below:
 - ["Log in from the UNIX Shell" on page 143](#)
 - ["Log in from the Desktop" on page 145](#)
- 2 Verify that the customer can view the Proxy Agent User Documentation from the UnixWare Desktop. Refer to ["Access the User Documentation" on page 150](#).
- 3 Verify that the customer can start the Proxy Agent, display the STATUS screen, and stop the Proxy Agent. Refer to the procedures below:
 - ["Start the Proxy Agent" on page 164](#)
 - ["Display of the Status Screen" on page 165](#)
 - ["Stop the Proxy Agent" on page 171](#)
- 4 Review the Proxy Agent application screens with the customer. Refer to chapters 4 through 14.
- 5 Verify that the customer has changed the **root** and **g3maadm** logins.

Installation Prompts

The installation script for this release has been **revised** in order to simplify the process and to make the installation of the Proxy Agent more automatic.

PA001 form

The completed **PA001 Administration Request** form contains most of the information that is specific to the customer's system. Installers must refer to the various sections on PA001 form in order to enter the information that is requested at the installation prompts.

Default options

The sections below describe the prompts in the order presented in the installation script. Lucent **strongly** recommends that installers select the default options where appropriate. The default options allow users to maintain consistency when upgrading to new releases. The installation script overwrites previous settings during the installation process.

Directory Prompt

The directory prompt requests the installer to define the directory where the Proxy Agent software will reside on the system.

Installers can enter **one** of the options below:

- a Accept the default **/usr/g3-ma** directory (recommended)
- b Enter a different directory path (not recommended)

RAM Megabytes Prompt

The RAM megabytes prompt requests the installer to enter the megabytes of RAM on the Proxy Agent stand-alone computer. If the number is more than 128 megabytes, the installation script makes modifications to the kernel boot file.

The PA001 form contains the system information in the Proxy Agent section.

SNMP Polling Prompt

For the Proxy Agent to poll the supported systems and create Enterprise-specific traps installers should **enable** SNMP Polling. The installation script automatically enables SNMP Traps, since both options are required for SNMP polling.

Installers can choose to **disable** SNMP polling if the Proxy Agent is used only as an alarm notification device **and** the DEFINITY Network Management product is **not** used.

SNMP Traps Prompt

If SNMP Polling is disabled, then the installation script displays the prompt to enable or disable SNMP Traps.

Installers should **enable** SNMP Traps if they want to receive SNMP traps only. In this release, if SNMP Polling is disabled and SNMP Traps are enabled, then the Proxy Agent allows installers to administer up to **600** managed nodes for each Proxy Agent. This option reduces the load on the Proxy Agent and requires a less powerful computer to manage a larger number of supported systems.

Installers also have the option to **disable** SNMP Traps if the Proxy Agent is only used for alarm processing.

SNMP Set Capability Prompt

During the Proxy Agent installation, installers can also enable or disable the SNMP Set Capability.

This feature allows users on the NMS server to managed the tasks listed below from the DEFINITY Network Management product:

- Busy Out/Release boards, ports, trunk groups, and trunks
- Set DEFINITY system date and time



SECURITY ALERT:

Due to security limitations in the SNMP, installers should only *enable* the SNMP Set Capability *if* the Proxy Agent is behind a fire wall.

Password Prompts

For new installations only, the password prompts require the installer to enter the **g3maadm** login password to allow access to the Proxy Agent user interface.

Function Prompt

The customer may administer four types of communication devices on the *serial I/O subsystem* to perform the four functions required by the Proxy Agent:

- Remote maintenance access
- Product access
- Receive alarms
- Send alarms

Refer to the ["Serial I/O Subsystem" on page 104](#) for examples of naming formats for the different types of the subsystems.

If the customer administers additional devices, then the PA001 form also should contain the information for those devices.

The installation script runs the Modem Setup program and displays the UNIX device name (/dev/ttyxxx) for all devices administered on the serial I/O subsystem and displays the prompt to select the function for that device.

The following is an example of the device name (/dev/ttysa1) and function prompt:

```
UNIX device name: /dev/ttysa1:
```

```
Select the function for this device:
```

```
[M] Maintenance Remote Access (TSC/ITAC)
```

```
[P] Product Access (default)
```

```
[R] Receive Alarms
```

```
[S] Send Alarms
```

```
Or, select one of the options below:
```

```
[N] Next Device (skip this one)
```

```
[X] Exit Modem Setup and continue the installation
```

```
Enter the device function or another option [default=P]:
```

Installers must execute the appropriate option for each device detected by the installation script. Installers can exit the Modem Setup program only from the function prompt.

Device Type Prompt

The installation script then displays the second prompt for the *device type* of the device name (`/dev/ttysa1`) shown in the previous prompt. The device type prompt refers to the make and model of the device.

The installation script displays different lists in the device type prompt that are based on the **function** that the installer selected for this device.

The following is an example of the *device type* prompt for the **remote maintenance** function:

```
UNIX device name: /dev/ttysa1:
Select the device type for the maintenance remote access
function:
[1] 3710 AT&T Dataport
[2] 3715 AT&T Dataport Express
[3] US Robotics Sportster 33.6 Kbps
[4] Other (manually)
Or select the option below:
[N] Next Device (skip this one)
```

```
Enter the device type or another option[default=1]:
```

Installers must execute the appropriate option for each device assigned to the Proxy Agent.

Reboot Prompt

If the device type is **not** on the list, then the installer should enter the number for **Other** (4) at the prompt. The system administrator must manually administer a different type of modem in the *Devices* file **after** the installation is complete.

The installation script continues to display the next device name and function prompt for all devices on the serial I/O subsystem. When all the devices on the PA001 form have been administered, then the installer exits the Modem Setup program from the function prompt.

Reboot Prompt

The reboot prompt is the last prompt in the installation script. Installations must enter the *shutdown* command to reboot the system **before** they execute the procedures to administer the Proxy Agent.

Serial I/O Subsystem

Generally, the devices are connected to serial input/output (I/O) subsystems, such as the ones listed below:

- Equinox XP
- Equinox SST
- Computone RackPort 3
- Specialix SIO
- Standard COM Ports `/dev/tty00` - `/dev/tty03`

The UNIX device name (`/dev/ttyxxx`) is based on the different numbering formats used by each subsystem (`ttyxxx`) as described below.

Subsystem numbering format

A subsystem usually consists of several “bricks” linked together through a plug-in module. Each port on the brick has a different port number (`ttyxxx`). In addition, each type of subsystem has a different numbering format for the ports on each brick.

The table below shows the numbering format for the serial I/O subsystems listed above. The number of “bricks” supported by each subsystem will vary.

Table 8. Serial I/O Subsystems

| Brick Number | Port Number | Equinox XP | Equinox SST | Computone RackPort 3 | Specialix SIO |
|----------------|-------------|------------|-------------|----------------------|---------------|
| Brick 1 | Port1 | ttysa1 | tty1a1 | ttyS01 | ttyA1 |
| | Port2 | ttysa2 | tty1a2 | ttyS02 | ttyA2 |
| | Port[n] * | ttysa[n] | tty1a[n] | ttyS0[n] | ttyA[n] |
| Brick 2 | Port1 | ttysb1 | tty1b1 | ttyS016 | ttyB1 |
| | Port2 | ttysb2 | tty1b2 | ttyS017 | ttyB2 |
| | Port[n] | ttysb[n] | tty1b[n] | ttyS0[n] | ttyB[n] |
| Brick 3 | Port1 | ttysc1 | tty1c1 | ttyS031 | ttyC1 |
| | Port2 | ttysc2 | tty1c2 | ttyS032 | ttyC2 |
| | Port[n] | ttysc[n] | tty1c[n] | ttyS0[n] | ttyC[n] |
| Brick 4 | Port1 | n/a | tty1d1 | ttyS046 | ttyD1 |
| | Port2 | n/a | tty1d2 | ttyS047 | ttyD2 |
| | Port[n] | n/a | tty1d[n] | ttyS0[n] | ttyD[n] |

* [n] represents the **next** port number on the brick

Install the New Proxy Agent

This section contains the procedures to install the **new** DNM Proxy Agent Release 3.0 product on the Proxy Agent stand-alone computer.

Before installers begin the installation procedures, verify the completion of the tasks listed below:

- Verify that all tasks in [Chapter 2, "Customer Pre-Installation Tasks"](#) have been completed.
- Review the ["Installation Tasks Checklist" on page 94](#) and complete the tasks in the order listed in the checklist.
- Read the entire section entitled, ["Installation Prompts" on page 98](#). This section explains how to respond to the prompts in the installation script.

Required materials

Installers need the materials and information listed below:

- Root login and password
- New password for the **g3maadm** login
- Completed PA001 Administration Request form
- CD-ROM entitled, DEFINITY Network Management Proxy Agent Release 3.0

3 Proxy Agent Installation

Install the New Proxy Agent

New installation procedure Complete the procedure below to install the **new** DEFINITY Network Management Proxy Agent Release 3.0.

1 Execute the tasks below:

- Request all users to log off the system.
- Close all open windows and applications.

2 At the UNIX *login* prompt, login as the root user:

- Type [root login]
- Press **ENTER**

3 At the *Password* prompt,

- Type [root password]
- Press **ENTER**

4 At the *Display Desktop? y/n* prompt,

- Type **N** (no)
- Press **ENTER**

Result: The system displays the UNIX prompt.

5 At the UNIX prompt (#), start the installation process:

- Type **pkgadd -d cdrom1 DG3PA**
- Press **ENTER**

Result: The system displays the name of the package and the prompt:

```
Insert CD into SCSI CD-Rom Drive. Type [go] when
ready or [q] to quit (default=go):
```

- 6 Insert the CD-ROM entitled, **DEFINITY Network Management Proxy Agent Release 3.0**, into the CD-ROM drive.

At the UNIX prompt,

- Type **go**
- Press **ENTER**

Result: The system displays the prompt: Strike ENTER when ready or ESC to stop.

- 7 At the UNIX prompt, press **ENTER**

Result: The system installs the program, which takes a few moments.

- 8 **RAM Megabytes Prompt.** The system displays the prompt:

How much RAM does the Proxy Agent serve have in it? If it is more than 128 Megabytes, then a modifications must be made to the kernel boot file.

How many megabytes of RAM?

On the PA001 form, go to the *Proxy Agent* section, then refer to the *Random Access Memory (RAM)* field for the number of megabytes of RAM (MB).

At the UNIX prompt,

- Type the [number] of megabytes of RAM
- Press **ENTER**

Result: The system modifies the kernel boot file.

- 9 SNMP Polling Prompt.** The system displays an explanation of the reasons to enable (default) or disable SNMP Polling. Then, the system displays the current setting and the prompt:

```
The current setting is SNMP polling ENABLED.
```

```
Should SNMP Polling be DISABLED? [n] y:
```

At the prompt, execute **one** of the options (a or b) below:

- a** To **enable** SNMP polling (default),

- Press **ENTER**.

- Go to step [11](#)

- b** To **disable** SNMP polling,

- Type **Y** (yes)

- Press **ENTER**

- Go to step [10](#)

- 10 SNMP Traps Prompt.** If users **disabled** SNMP polling in step [9](#), then the system displays an explanation of the reasons to enable (default) or disable SNMP traps. This prompt will **not** display if users **enabled** the SNMP Polling because SNMP Traps are required for SNMP Polling.

Then, the system displays the current setting and the prompt:

```
The current setting is SNMP Traps are ENABLED.
```

```
Should SNMP Traps be DISABLED? [n] y:
```

At the prompt, execute **one** of the options (a or b) below:

a To **enable** SNMP traps (default),

– Press **ENTER**

– Go to step [11](#)

b To **disable** SNMP traps,

– Type **Y** (yes)

– Press **ENTER**

– Go to step [12](#)

11 SNMP Set Capability Prompt. If users **enabled** SNMP Polling in step [9](#), then the system displays an explanation of the reasons to disable (default) or enable SNMP Set Capability. The SNMP Set Capability allows network managers on the NMS to execute the tasks below from the DEFINITY Network Management product.

- Busy-out and release alarms
- Set the system date and time

Then the system displays a warning and the prompt:

```
WARNING: If you are not behind a secure firewall,  
it is strongly suggested that this option be  
disabled!
```

```
The current setting is SNMP Set Capability is  
DISABLED.
```

```
Should SNMP Set Capability be ENABLED? [n]/y:
```

3 Proxy Agent Installation

Install the New Proxy Agent

At the prompt, execute **one** of the options (a or b) below:

- a To **disable** SNMP set capability (default), if the Proxy Agent is **not** behind a secure fire wall,
 - Press **ENTER**
 - Go to step [12](#)
- b To **enable** SNMP set capability, if the Proxy Agent is behind a secure fire wall,
 - Type **Y** (yes)
 - Press **ENTER**
 - Go to step [12](#)

Result: The system updates the SNMP access files.

- 12 Password Prompt.** Then the system displays the password fields for the *g3maadm* login. Type a new **g3maadm** password in the fields below. Press **ENTER** after each entry:

New password: **xxxxxx**

Re-enter new password: **xxxxxx**

Result: The system administers the *g3maadm* login and the TSC Maintenance accounts, then displays the message:

TSC Maintenance accounts successfully administered.

- 13 Function Prompt.** After this message, the installation script executes the *Modem Setup* program. The Modem Setup program displays **all** devices detected on the serial I/O subsystem. Refer to the *Devices* section of the PA001 form and **skip** all devices that are not listed on the form.

The system displays the first **device name** from the serial I/O subsystem and the **device function prompt** for that device:

```
UNIX device name: /dev/ttyxxx:
```

```
Select the function for this device:
```

```
[M] Maintenance Remote Access (TSC/ITAC)
```

```
[P] Product Access (default)
```

```
[R] Receive Alarms
```

```
[S] Send Alarms
```

```
Or, select one of the options below:
```

```
[N] Next Device (skip this one)
```

```
[X] Exit Modem Setup and continue the installation
```

```
Enter the letter for the device function or another  
option [default=P]:
```

Refer to the *Devices* section on the PA001 form and check the fields, *Device Name* and *Device Function*, for this device.

At the prompt, execute **one** of the options (a or b) below:

- a If the device name is on the PA001 form, then
 - Type the **[letter]** that matches the *function* for this device
 - Press **ENTER**
 - Go to step [14](#)

- b If the device name is **not** on the PA001 form, then skip this device,
 - Type **N** (Next)
 - Press **ENTER**
 - The system displays the device name and function prompt for the next device in the I/O subsystem. Repeat this step to skip every device that is **not** on the PA001 form.

14 Device Type Prompt. The system displays the **device type** prompt. The prompt below is an **example** of the maintenance function. The list varies by the function selected in the previous prompt.

```
UNIX device name: /dev/ttyxxx:
```

```
Select the device type for the maintenance remote  
access function:
```

```
[1] 3710 AT&T Dataport
```

```
[2] 3715 AT&T Dataport Express
```

```
[3] US Robotics Sportster 33.6 Kbps
```

```
[4] Other (manually)
```

```
Or select the option below:
```

```
[N] Next Device (skip this one)
```

```
Enter the number for the device type or another  
option[default=1]:
```

Refer to the *Devices* section on the PA001 form and check the *Device Type* field for this device. At the prompt, execute **one** of the options (a or b) below:

- a If the device name is on the PA001 form, then
 - Type the **[number]** that matches the *device type*
 - Press **ENTER**
- b If the device name is not listed in the prompt, then skip the prompt,
 - Type **N** (Next)
 - Press **ENTER**

Result: The system displays the *device name* and the *device function prompt* for the next device in the I/O subsystem.

Note: Repeat steps [13](#) and [14](#) to set up **all** of the of the devices on the PA001 form. Then go to step [15](#) to exit the Modem Setup program.

15 Exit Modem Setup. To exit the *Modem Setup* program at a *device function* prompt,

- Type **X** (Exit)
- Press **ENTER**

Result: The system exits the *Modem Setup* program and displays the message:

Done setting up Devices.

Result: Next, the system continues the installation, lists a series of messages, which takes several minutes. Then, the system displays another message:

```
Installation of Lucent Technologies DEFINITY Proxy
Agent (DG3PA) was successful.
```

16 Reboot Prompt. Finally, the system displays the reboot prompt:

```
Reboot the machine by executing 'cd /; shutdown -i6
-g0 -y'
```

At the UNIX prompt,

- Type the shutdown command: **cd /; shutdown -i6 -g0 -y**
- Press **ENTER**

Result: The system reboots the computer, which takes several minutes. Then, the system displays the UNIX *login* prompt.

17 Refer to the ["Installation Checklists" on page 93](#) and complete each procedure in the order listed on the checklist.

Upgrade from Proxy Agent 2.0 and Later

This section contains the procedures to **upgrade** from Proxy Agent releases, 2.0.1 and 2.0.2 **to** the Proxy Agent Release 3.0.

UnixWare upgrade patches

To download the latest patch for the UnixWare Operating System release 2.1.3, refer to the "[Vendor References](#)" on [page 21](#) for the SCO web address.

The customer **must** ensure that the UnixWare Operating System is release 2.1.3.



CAUTION:

The customer is **solely** responsible for the installation and maintenance of third-party products. For technical support of these products, the customer must call the vendor. Lucent Technologies does **not** provide support for third-party hardware or software products.

Installation script

The *Devices* section of the PA001 form should contain all of the device names that are assigned to the Proxy Agent.

For upgrades, the installation script only searches for devices that are **not** currently detected on the *I/O subsystem*. If the script detects any undefined devices, then the script displays the prompts for those devices.

Please read the entire section entitled, "[Installation Prompts](#)" on [page 98](#). This section explains how to respond to the prompts in the installation script.

Required materials

Installers need the following materials and information:

- Root login and password
- Completed PA001 form
- CD-ROM entitled, DEFINITY Network Management Proxy Agent Release 3.0

Upgrade procedure

Complete the procedure below to **upgrade** from Proxy Agent releases , 2.0.1, and 2.0.2 **to** the DEFINITY Proxy Agent Release 3.0.

1 Execute the tasks below:

- Request all users to log off the system, if necessary.
- Close all open windows and applications.
- Stop the Proxy Agent if running. Refer to ["Stop the Proxy Agent" on page 171](#)
- Log off the system.

2 At the UNIX *login* prompt, login to the root (/) directory:

- Type **[root login]**
- Press **ENTER**

3 At the *Password* prompt,

- Type **[root password]**
- Press **ENTER**

4 At the *Display Desktop? y/n* prompt,

- Type **N** (no)
- Press **ENTER**

Result: The system displays the UNIX prompt.

5 At the UNIX prompt (#), start the installation process:

- Type **pkgadd -d cdrom1 DG3PA**
- Press **ENTER**

Result: The system displays the name of the package and the prompt:

```
Insert CD into SCSI CD-Rom Drive. Type [go] when
ready or [q] to quit (default=go):
```

6 Insert the CD-ROM entitled, **DEFINITY Network Management Proxy Agent Release 3.0**, into the CD-ROM drive.

At the UNIX prompt,

- Type **go**
- Press **ENTER**

Result: The system displays the prompt: Strike **ENTER** when ready or **ESC** to stop.

7 At the UNIX prompt, press **ENTER**

Result: The system installs the program, which takes a few moments.

8 **RAM Megabytes Prompt.** The system displays the prompt:

```
How much RAM does the Proxy Agent serve have in it?
If it is more than 128 Megabytes, then a
modifications must be made to the kernel boot file.

How many megabytes of RAM?
```

On the PA001 form, go to the *Proxy Agent* section, then refer to the *Random Access Memory (RAM)* field for the number of megabytes of RAM (MB).

At the UNIX prompt,

- Type the **[number]** of RAM megabytes
- Press **ENTER**

Result: The system modifies the kernel boot file.

- 9 SNMP Polling Prompt.** The system displays an explanation of the reasons to enable (default) or disable SNMP polling. Then, the system displays the current setting and the prompt:

```
The current setting is SNMP polling ENABLED.
```

```
Should SNMP Polling be DISABLED? [n] y:
```

At the prompt, execute **one** of the options (a or b) below:

- a** To **enable** SNMP polling (default),
 - Press **ENTER**.
 - Go to step 11
- b** To **disable** SNMP polling,
 - Type **Y** (yes)
 - Press **ENTER**
 - Go to step 10

- 10 SNMP Traps Prompt.** If users **disabled** SNMP polling in step [9](#), then the system displays an explanation of the reasons to enable (default) or disable SNMP traps. This prompt will **not** display if users **enabled** the SNMP Polling because SNMP Traps are required for SNMP Polling.

Then, the system displays the current setting and the prompt:

```
The current setting is SNMP Traps are ENABLED.  
Should SNMP Traps be DISABLED? [n] y:
```

At the prompt, execute **one** of the options (a or b) below:

a To **enable** SNMP traps (default),

- Press **ENTER**
- Go to step [11](#)

b To **disable** SNMP traps,

- Type **Y** (yes)
- Press **ENTER**
- Go to step [12](#)

11 SNMP Set Capability Prompt. If users **enabled** SNMP Polling in step [9](#), then the system displays an explanation of the reasons to disable (default) or enable SNMP Set Capability. The SNMP Set Capability allows network managers on the NMS to execute the tasks below from the DEFINITY Network Management product.

- Busy Out/Release boards, ports, trunk groups and trunks
- Set the DEFINITY system date and time

Then the system displays a warning and the prompt:

```
WARNING: If you are not behind a secure firewall,  
it is strongly suggested that this option be  
disabled!
```

```
The current setting is SNMP Set Capability is
DISABLED.
```

```
Should SNMP Set Capability be ENABLED? [n]/y:
```

At the prompt, execute **one** of the options (a or b) below:

- a To **disable** SNMP set capability (default), if the Proxy Agent is **not** behind a secure fire wall,
 - Press **ENTER**
 - Go to step [12](#)
- b To **enable** SNMP set capability, if the Proxy Agent is behind a secure fire wall,
 - Type **Y** (yes)
 - Press **ENTER**
 - Go to step [12](#)

Result: The system updates the SNMP access files and executes the *Modem Setup* program.

12 Function Prompt. The Modem Setup program displays a list of **all** devices on the serial I/O subsystem that were defined during a previous installation. The function prompt contains the information listed below:

- Name of the I/O subsystem
- A list of previously defined devices
- The function prompt for the first device name on the I/O subsystem that has not been defined

The system displays the first function prompt as show in the example below:

```
Equinox SST Device Driver Detected
Device /dev/ttyla1 previously defined
Device /dev/ttyla2 previously defined
Device /dev/ttyla3 previously defined
```

```
UNIX device name: /dev/ttyla4:
```

```
Select the function for this device:
```

```
[M] Maintenance Remote Access (TSC/ITAC)
```

```
[P] Product Access (default)
```

```
[R] Receive Alarms
```

```
[S] Send Alarms
```

```
Or, select one of the options below:
```

```
[N] Next Device (skip this one)
```

```
[X] Exit Modem Setup and continue the installation
```

```
Enter the letter for the device function or another
option [default=P]:
```

Compare the list of previously defined devices on the screen to the device names and functions in the *Devices* section of the PA001 form.

At the prompt, execute **one** of the options (a, b, or c) below:

- a If the list of previously defined devices on the screen contains the device names on the PA001 form, then exit the Modem Setup program. Go to step [14](#).
- b To define new devices from the PA001 form,
 - Type the **[letter]** that matches the *function* for this device
 - Press **ENTER**
 - Go to step [13](#)
- c To skip device names that are **not** on the PA001 form,
 - Type **N** (Next) to skip this device
 - Press **ENTER**
 - The system displays the device name and function prompt for the next device in the I/O subsystem. Repeat this step to skip every device that is **not** on the PA001 form.

13 Device Type Prompt. The system displays the **device type** prompt. The prompt below is an **example** of the maintenance function. The list varies by the function selected in the previous prompt.

```
UNIX device name: /dev/ttyla4:
Select the device type for the maintenance remote
access function:
[1] 3710 AT&T Dataport
[2] 3715 AT&T Dataport Express
[3] US Robotics Sportster 33.6 Kbps
[4] Other (manually)
```

Or select the option below:

[N] Next Device (skip this one)

Enter the number for the device type or another option[default=1]:

Refer to the *Devices* section on the PA001 form and check the *Device Type* field for this device.

At the prompt, execute **one** of the options (a or b) below:

- a If the device name is on the PA001 form, then
 - Type the [number] that matches the device type
 - Press **ENTER**
- b If the device name is not listed in the prompt, then skip the prompt,
 - Type **N** (Next)
 - Press **ENTER**

Result: The system displays the next *device name* and the *device function prompt* for the next device.

Note: Repeat steps 12 and 13 to set up **all** of the of the devices on the PA001 form. Then go to step 18 to exit the Modem Setup program.

14 Exit Modem Setup. To exit the *Modem Setup* program at a *device function* prompt,

- Type **X** (Exit)
- Press **ENTER**

Result: The system exits the *Modem Setup* program and displays the message:

```
Done setting up Devices.
```

Result: Next, the system continues the installation, lists a series of messages, which takes several minutes. Then, the system displays another message:

```
Installation of Lucent Technologies DEFINITY Proxy Agent (DG3PA) was successful.
```

15 Reboot Prompt. Finally, the system displays the reboot prompt:

```
Reboot the machine by executing 'cd /; shutdown -i6 -g0 -y'
```

At the UNIX prompt,

- Type the shutdown command: **cd /; shutdown -i6 -g0 -y**
- Press **ENTER**

Result: The system reboots the computer, which takes several minutes. Then, the system displays the UNIX *login* prompt.

16 Refer to the ["Installation Checklists" on page 93](#) and complete each procedure in the order listed on the checklist.

Upgrade from Proxy Agent 1.4 and Earlier

Only the **system administrator** should upgrade from Proxy Agent releases 2.0 and earlier **to** the DEFINITY Network Management Proxy Agent release 3.0.

Proxy Agent releases 1.4 and earlier require an upgrade to the UnixWare Operating System release 2.1.3.

UnixWare upgrade patches

The SCO web site contains patches to upgrade from the UnixWare Operating System releases 2.1.0 through 2.1.2 **to** release 2.1.3. Refer to "[Vendor References](#)" on page 21 for the web address.

If customers are upgrading from Proxy Agent release **1.4**, then they can use these patches to upgrade the UnixWare Operating System to release 2.1.3.

If customers are upgrading from Proxy Agent release **1.3** and earlier, then they must execute a destructive installation of the UnixWare releases 2.1.3 operating system.



CAUTION:

The customer is **solely** responsible for the installation and maintenance of third-party products. For technical support of these products, the customer must call the vendor. Lucent Technologies does **not** provide support for third-party hardware or software.

Installation tasks

The system administrator must execute the installation tasks listed below to upgrade UnixWare 2.1.3 and Proxy Agent 3.0.

- 1 Upgrade or install UnixWare release 2.1.3. Execute the appropriate option below:
 - If UnixWare 2.1.0 through 2.1.2 are currently installed, then install the UnixWare upgrade patch for release 2.1.3.
 - If UnixWare 2.0 and earlier are currently installed, then execute a destructive installation of UnixWare. Install UnixWare 2.1.3 as a new product.

For UnixWare installation procedures, refer to *SCO UnixWare Enterprise Computing Products Installation Handbook*

- 2 Complete the Customer Pre-Installation Tasks to ["Install the UnixWare Operating System" on page 73](#) in this book.
- 3 Remove the Proxy Agent releases 1.4 and earlier. Refer to ["Remove the Proxy Agent" on page 128](#).
- 4 Install the DEFINITY Proxy Agent 3.0 as a new product. Refer to ["Install the New Proxy Agent" on page 106](#).

Remove the Proxy Agent

This section contains the procedure to remove the Proxy Agent. Only the **system administrator** should execute the removal procedure as required for upgrading an earlier version of the Proxy Agent or for other business reasons.

The removal procedure only contains the basis steps. For more information on the UNIX package removal (pkgrm) command, refer to the UNIX system documentation.

Procedure

Complete the procedure below to remove the Proxy Agent from the stand-alone computer.

1 Execute the tasks below:

- Request all users to log off the system, if necessary.
- Stop the Proxy Agent if running. Refer to ["Stop the Proxy Agent" on page 171](#)
- Close all open windows and applications.
- Log off the system.

2 At the UNIX *login* prompt, login as the root user:

- Type **[root login]**
- Press **ENTER**

3 At the *Password* prompt,

- Type **[root password]**
- Press **ENTER**

4 At the *Display Desktop?* y/n prompt,

- Type **N** (no)
- Press **ENTER**

Result: The system displays the UNIX prompt.

5 At the UNIX prompt,

- Type the remove command: **# pkgrm DG3PA**
- Press **ENTER**

Result: The system confirms that the package is currently installed. Then, the system displays the prompt:

```
Do you want to remove this package? [yes, no, ?,  
quit] y
```

6 To select “yes” to remove the package, press **ENTER**.

The system executes the remove command, which may take several minutes. Then, the system displays the reboot prompt:

```
Reboot the machine by executing 'cd /; shutdown -i6  
-g0 -y'
```

At the UNIX prompt,

- Type the shutdown command: **cd /; shutdown -i6 -g0 -y**
- Press **ENTER**

Result: The system reboots the computer, which takes several minutes. Then, the system displays the UNIX *login* prompt.

4 Help Screens and Commands

Chapter Contents

- [Introduction](#) [131](#)
- [Functions Window](#) [132](#)
- [Commands and Hotkeys](#) [133](#)
- [Format Conventions](#) [137](#)

Introduction

The information in this chapter primarily targets **new** users who are unfamiliar with the Proxy Agent software.

The Proxy Agent application contains two types of help windows that users can access from any menu or application screen. The commands to access the help windows include the following:

- The **list** command (**Ctrl-L**) displays a **Functions** window that contains the available commands for the current Proxy Agent menu or application screen.
- The **help** command (**Ctrl-Y**) displays a **help** window for the current Proxy Agent menu or individual field on an application screen. Help windows can be lists of valid options for a specific field or instructions that explain the type of information to input in a field.

Note: Users need only type enough of each command to make it unique. For example: at the proxy main menu, instead of typing “proxy-admin”, you can type just “p”.

The Format Conventions section contains a table that describes the conventions used in this guide.

Functions Window

The figure below is an example of a Functions window with associated hotkeys.

Users can access the Functions window (**Ctrl-L**) from any menu or application screen in the Proxy Agent.

Most commands have **hotkeys**, which are keyboard short cuts. Hotkeys allow users to execute a command without accessing the Functions window.

| Functions | |
|--------------|---------|
| Cancel | ctrl-x |
| Clear Field | ctrl-kf |
| Help | ctrl-y |
| Online Guide | ctrl-gg |
| Page Down | ctrl-d |
| Page Left | ctrl-p |
| Page Right | ctrl-n |
| Page Select | |
| Page Up | ctrl-u |
| Refresh | |
| Submit | ctrl-e |

sdnmist LJK 040898

Figure 9. Functions window

Commands and Hotkeys

The table below contains the description for the commands and the hotkeys that are available on the Proxy Agent.

Table 9. Commands and Hotkeys

| Command | Description |
|-------------------------------|--|
| List command Ctrl-L | <p>Displays the Functions window that contains all of the available commands and associated hotkeys for the current screen.</p> <p>To select an option from the Functions window,</p> <ul style="list-style-type: none">• Press Ctrl-L to display the Functions window:• Use the arrow keys or the TAB key to move the cursor to an option on the screen.• Press ENTER to execute the command. |

Table 9. Commands and Hotkeys

| Command | Description |
|-------------------------|--|
| Help Ctrl-Y | <p>Displays a help window for a field or a menu, as described below:</p> <ul style="list-style-type: none">• Field help window contains a list of options for the field.• Main Menu help window contains explanations of the applications on the menu.• Submenu help window contains available commands. <p>To access a help list for a specific field,</p> <ul style="list-style-type: none">• Move the cursor to the field• Press Ctrl-Y to display the help window• Move the cursor to an option on the list• Press ENTER to execute the option <p>To exit a help window without selecting an option, press ESC.</p> |
| Submit Ctrl-E | <p>Saves changes made in the fields on an application screen and exits the screen.</p> |
| Cancel Ctrl-X | <p>Exits a screen without saving changes.</p> |
| | <i>2 of 4</i> |

Table 9. Commands and Hotkeys

| Command | Description |
|---------------------------------|---|
| Clear Field Ctrl-K F | Deletes the data in the field where the cursor is located. Users can also delete data in a field by pressing the SPACE BAR . |
| Online Guide Ctrl-G G | Displays a message with directions to access the Proxy Agent Installation Guide and User Guide from the Documentation folder on the UnixWare Desktop. The Online Guide has been removed from the Proxy Agent. |
| Page Down Ctrl-D | Displays the next numbered page in a multiple-page application. Example: The MANAGED NODES application contains 10 pages. Press Ctrl-D to page down to the next page (2, 3, 4, etc.). |
| Page Up Ctrl-U | Displays the previous numbered page in a multiple-page application. Example: In the MANAGED NODES application, press Ctrl-U to page up to the previous page (4, 3, 2, 1). |
| | <i>3 of 4</i> |

Table 9. Commands and Hotkeys

| Command | Description |
|-----------------------------|--|
| Page Right Ctrl-N | <p>Displays the next subpage that is to the right of the current page.</p> <p>Example: The MANAGED NODES application is similar to a spreadsheet with columns and rows on 5 subpages (a through e) for each numbered page.</p> <p>Press Ctrl-N to access the next subpage (b, c, d, e) within a spreadsheet application.</p> |
| Page Left Ctrl-P | <p>Displays the previous subpage that is to the left of the current page.</p> <p>Press Ctrl-P to access the previous subpage (d, c, b, a) within a spreadsheet application.</p> |
| Page Select (no hotkey) | <p>Displays a window that contains all available page options within a multiple-page application.</p> <p>The options may include any or all of the page commands listed above.</p> |
| Refresh (no hotkey) | <p>Updates the screen with the current information.</p> |
| | <i>4 of 4</i> |

Format Conventions

The format conventions used in the *Proxy Agent User Documentation* are visual cues to help users identify the type of actions they should execute in the procedures.

UNIX systems have very specific rules for entering data at the UNIX prompt. The procedures in the guides show the text to be entered in **9 point bold font**.

Users should type the text **exactly** as shown in the step. The steps include the conventions below:

- UPPER and lower case, symbols (periods, slashes, hyphens, underscores, etc.), and spaces within the command or path.
- If a *command line wraps* to the next line, this indicates that users should press the **SPACE BAR** before they type the data on the next line.
- If a *web address* (URL) **wraps** to the next line, do NOT insert a space.
- The procedures in the guides contain some data that are enclosed in brackets [password]. The brackets indicate that users should type the requested data **without** the brackets.



CAUTION:

Always check the typed data **before** pressing the **ENTER** or **RETURN** key. Notice the difference between the capital letter “**O**” and the number zero “**0**”. The only error message the UNIX system may display is: `not found`.

The format conventions described in the table below appear in the procedures and in the **Result** paragraph that follow most steps.

Table 10. Format Conventions

| Convention | Description |
|--------------------------------|--|
| Bold text | Indicates that users should type the bold text exactly as shown. Example: Type display status |
| [Bold text in brackets] | <p>Indicates that users should type data that is <i>specific</i> to their system, <i>without</i> the brackets.</p> <p>Text enclosed within brackets contain either the data that may be different on your system or instructions to enter specific data for your system:</p> <ul style="list-style-type: none">• Drive name [d:] which may be different on each system. Example: Type [d:] install• System data from the PA001 form. Example: Type the [IP address] as shown on the PA001 form• Options from a Help list. Example: Select the [managed node name] from the Help list• Description of requested data. Example: Type the [device name] in the field as shown on the PA001 form: /dev/ttyxxx |
| | <i>1 of 3</i> |

Table 10. Format Conventions

| Convention | Description |
|---|---|
| Result paragraph | <p>Describes the result of an action taken in a step, as described in the following example:</p> <p>Result: The system displays the MAIN MENU.</p> <p>A Result paragraph may also contain a message or a prompt that is displayed in the <code>constant width</code> font.</p> <p>A prompt sets up the action to be taken in the next step.</p> <p>Result: The system displays the command window that contains the prompt: <code>Do you wish to continue? y/n</code></p> |
| Series of Menu Options File > Save | <p>The greater than (>) symbol indicates that users should select an option from a series of menus.</p> <p>For example, Click File > Save means that users should:</p> <ul style="list-style-type: none"> • Click on the option on the menu bar (File). • Then click on the second option (Save) from the drop-down menu. <p>The term select is used in place of click if:</p> <ul style="list-style-type: none"> • A program does not accept mouse commands or • Users need to choose an option from a Help list. |
| | <i>2 of 3</i> |

Table 10. Format Conventions

| Convention | Description |
|--|---|
| Execution keys | Appear in bold capital letters and indicate that users should press that key on the keyboard to execute a specific action. Examples: Press ENTER (also refers to the RETURN key) |
| Combination keys Ctrl-L Ctrl-K F | The hyphen (-) between a function key (Ctrl, Alt, Shift) and a letter indicates that users should execute the actions described in the examples below: Example: Press Ctrl-L (list command) <ul style="list-style-type: none">• Press and hold the Ctrl (Control) key• Press the letter (L) key• Then release both keys Example: Press Ctrl-K F (clear field command) <ul style="list-style-type: none">• Press and hold the Ctrl (Control) key• Press the first letter (K) key• Release both keys• Then press the second letter (F) key |
| Repeated keys | Indicates that users should press the same key twice . Example: Press ESC (closes a Help window) |
| | 3 of 3 |

5 Access Procedures

Chapter Contents

- [Introduction](#) [142](#)
- [Log in to the Proxy Agent](#) [143](#)
 - [Log in from the UNIX Shell](#) [143](#)
 - [Log in from the UNIX Shell](#) [143](#)
- [Access the User Documentation](#) [150](#)
- [Access the IO Setup Folder](#) [153](#)
- [Review of the Main Menu](#) [156](#)
- [Review of the Proxy Admin Menu](#) [160](#)
- [Start the Proxy Agent](#) [164](#)
- [Display of the Status Screen](#) [165](#)
 - [Review of the Status Screen Fields](#) [167](#)
 - [Display the Status Screen](#) [170](#)
- [Stop the Proxy Agent](#) [171](#)

Introduction

This chapter contains screen descriptions and procedures to log in to the Proxy Agent from the UnixWare Desktop and UNIX prompt and procedures to access the various Proxy Agent menus and application screens.

This chapter also contains the procedures to:

- ["Start the Proxy Agent" on page 164](#)
- ["Display of the Status Screen" on page 165](#)
- ["Stop the Proxy Agent" on page 171](#)

The information in this chapter primarily targets **new** users who are unfamiliar with the Proxy Agent software.

Log in to the Proxy Agent

Users can log in to the Proxy Agent from either the UNIX or the UnixWare Desktop. This section contains both procedures.

Users must use the Desktop procedures to access the Proxy Agent User Documentation. Refer to "[Access the User Documentation](#)" on page 150.

Log in from the UNIX Shell

When logging from the UNIX shell, users can access all applications from the Proxy Agent MAIN MENU, **except** the Proxy Agent User Documentation.

Procedure

Complete the procedure below to log in to the Proxy Agent MAIN MENU from the UNIX shell.

- 1 At the UNIX *login* prompt,
 - Type the [g3maadm login]
 - Press **ENTER**

Result: The system displays the *Password* prompt.

- 2 At the *Password* prompt,
 - Type the g3maadm [password]
 - Press **ENTER**

Result: The system displays the prompt: Display Desktop? y/n

5 Access Procedures

Log in from the UNIX Shell

3 At the prompt,

- Type **N** (no)
- Press **ENTER**

Result: The system displays the UNIX prompt.

4 At the UNIX prompt,

- Type **proxy**
- Press **ENTER**

Result: The system displays the Proxy Agent MAIN MENU.

```
(PROXY AGENT)
MAIN MENU

Please select one of the following Proxy Agent applications:

communication      exit      proxy-admin
configuration      online-guide  unix-shell
emulation

To access documentation, type 'online-guide'. To exit Proxy Agent, type 'exit'.
Throughout Proxy Agent, to select functions, press Ctrl-L.

enter application name:>
```

5 At the command line, enter an application name. For example:

- Type **proxy-admin**
- Press **ENTER**

Result: The system displays the selected application screen.

Log in from the Desktop

When logging in to the UnixWare Desktop, the system displays the two screens listed below before it displays the Proxy Agent MAIN MENU:

- The UnixWare Desktop contains the DEFINITY_Proxy icon that opens the DEFINITY_Proxy folder.
- The DEFINITY_Proxy folder contains the executable icons or folders described below:
 - **Proxy_Agent** icon opens the MAIN MENU that lists the commands to access the Proxy Agent applications.
 - **Documentation** icon opens a PDF menu to access the Proxy Agent User Documentation and PA001 forms.
 - **IO_Setup** folder contains the icons to access the Dialers file and the Devices file. Users need root password to edit these files.

Users execute most of the daily operation tasks the PROXY ADMIN menu. Chapters 4 through 8 contain field definitions and procedures to execute various tasks on the administration screens.

Procedure Complete the procedure below to log in to the UnixWare Desktop and access the Proxy Agent MAIN MENU.

Note: Accessing the UnixWare Desktop can only be done from the Proxy Agent Console.

- 1 At the UNIX *login* prompt,
 - Type the [g3maadm login]
 - Press **ENTER**

Result: The system displays the *Password* prompt.

- 2 At the *Password* prompt,
 - Type your [password]
 - Press **ENTER**

Result: The system displays the prompt: Display Desktop? y/n

- 3 At the prompt,
 - Type **Y** (yes)
 - Press **ENTER**

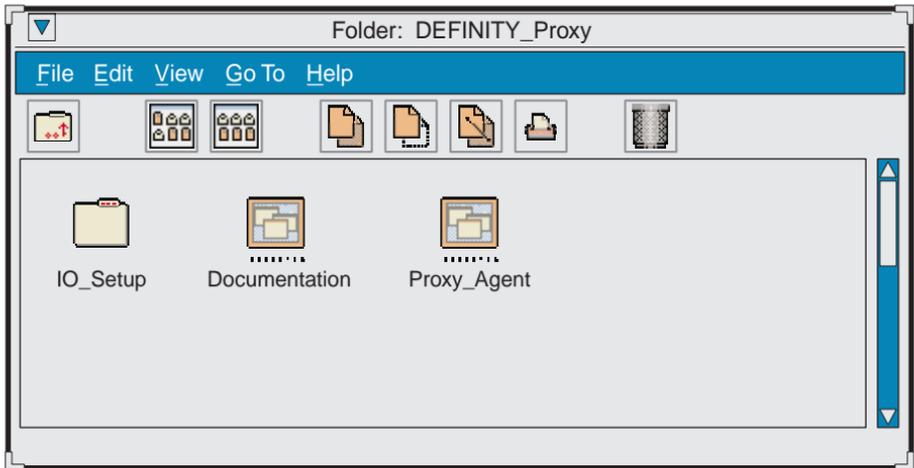
Result: The system displays the UnixWare *Desktop*.



sdnmdtop KLC 03

- 4 Double-click the **DEFINITY_Proxy** icon to open the folder.

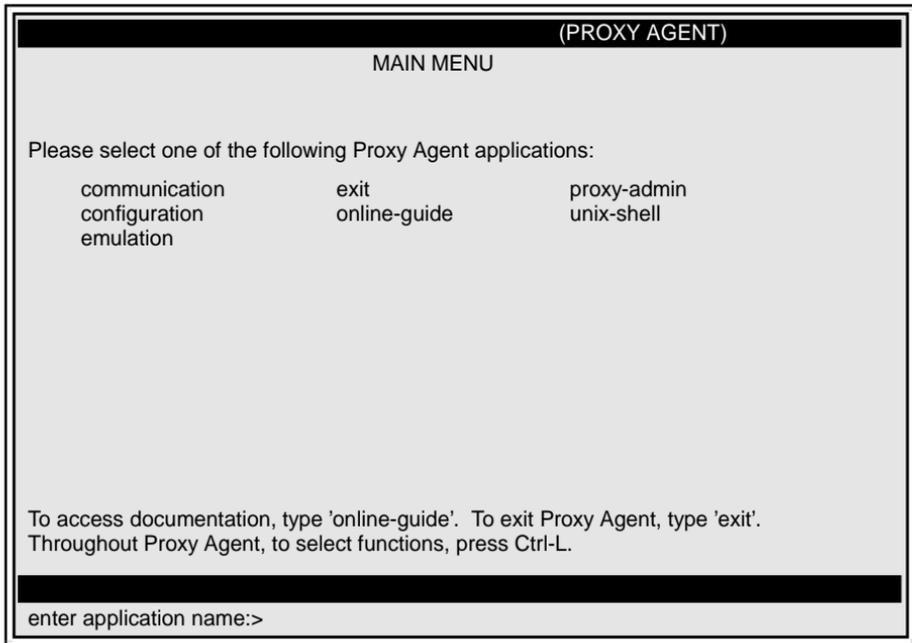
Result: The system displays the contents of the *DEFINITY_Proxy* folder.

5 Access Procedures*Log in from the Desktop*

sdnmprox LJK 092299

5 Double-click the **Proxy_Agent** icon to access the Proxy Agent MAIN MENU.

Result: The system displays the Proxy Agent MAIN MENU.



sdnmain LJK 040798

6 At the command line, enter an application name. For example:

- Type **proxy-admin**
- Press **ENTER**

Result: The system displays the selected application screen.

Access the User Documentation

In this release, the Proxy Agent User Documentation for Installation and Administration is delivered on the product CD-ROM entitled: DEFINITY Network Management Proxy Agent Release 3.0.

During the installation of the Proxy Agent, the installation script copies the User Documentation and PA001 forms to the **lucentdoc** directory. Users can only access the User Documentation from the UnixWare Desktop.

Users also have the option of printing the guides directly from the DEFINITY Network Management Proxy Agent CD-ROM.

PDF viewer

The Proxy Agent User Documentation are PDF files. Users can access any chapter in the book by using the built-in links in the table of contents, index, and chapters. Users can also use the search feature to find specific information.

The PDF viewer is public domain software. Users can learn more about the PDF viewer from the UNIX manual page entitled: XPDF. To access the manual page, enter the **man xpdf** command at a UNIX prompt.

Online_guide command

The Proxy Agent User Documentation replaces the Online Guide. The **online_guide** command is still visible on the Proxy Agent MAIN MENU and Functions screen.

If users execute the command, the system displays a window with instructions for viewing the documentation on the UnixWare Desktop.

Procedure

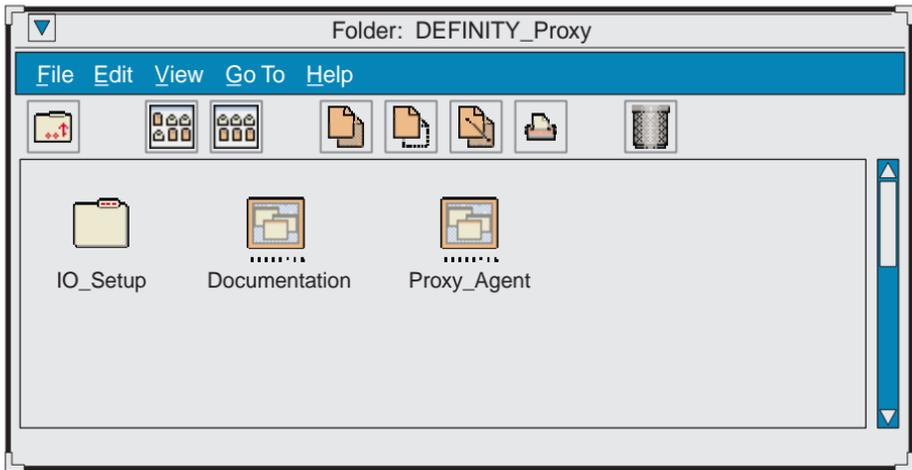
Complete the procedure below to access the Proxy Agent Installation Guide and the User Guide from the Documentation folder on the Desktop.

- 1 Log in as ***g3maadm*** and access the UnixWare Desktop.

Result: The system displays the *Desktop*.

- 2 Click the **DEFINITY_Proxy** icon.

Result: The system displays the *DEFINITY_Proxy* folder.



3 Click the **Documentation** icon.

Result: The system displays the main menu for the PDF viewer.

4 Select an option from the main menu to access the documentation.

5 To exit the PDF viewer from the Menu Bar, select **File > Exit**.

Result: The system displays the DEFINITY_Proxy folder.

Access the IO_Setup Folder

System administrators and root users can edit the **Devices** file and the **Dialers** file from the **IO_Setup folder** on the UnixWare Desktop.

Root users can also edit these files from the UNIX shell. Refer to [Chapter 15, "I/O Setup Application"](#) for special instruction to edit these files.

Procedure

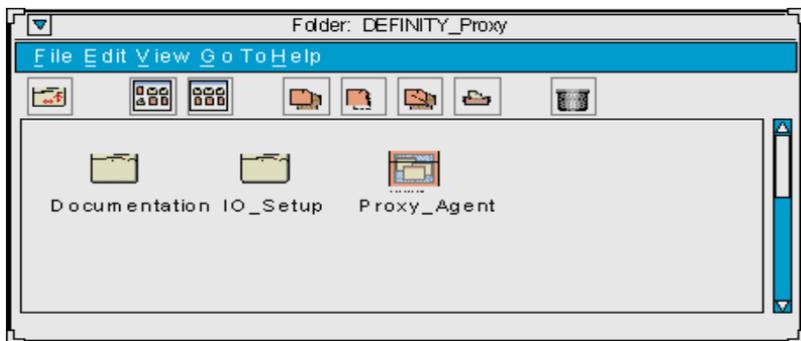
Complete the procedure below to access IO_Setup folder on the Desktop.

- 1 Log in as a **root** user and access the UnixWare Desktop.

Result: The system displays the *Desktop*.

- 2 Click the **DEFINITY_Proxy** icon.

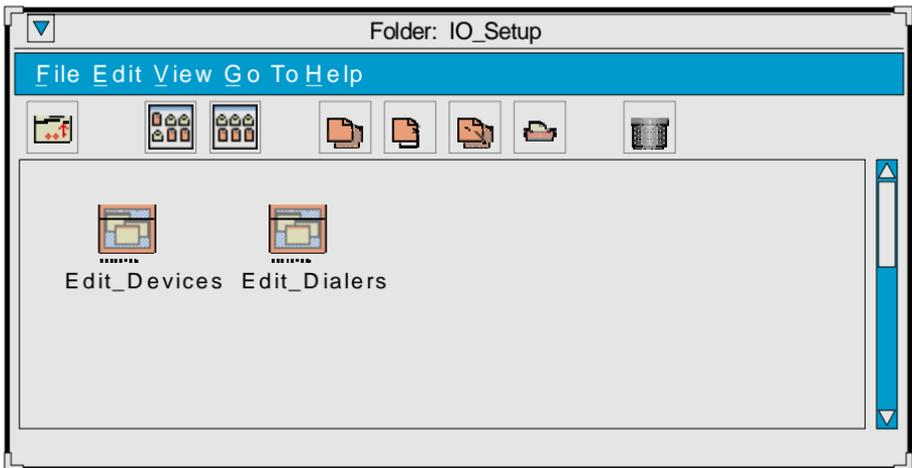
Result: The system displays the *DEFINITY_Proxy* folder.



Access the IO_Setup Folder

- 3 Click the **IO_Setup** icon.

Result: The system IO_Setup folder below:



4 Double-click either the **Edit_Devices** icon or the **Edit_Dialers** icon.

Result: The system displays a window and prompt for your root password.

5 At the *Password* field,

- Enter your [root password]
- Press **ENTER**

Result: The system displays the selected file.

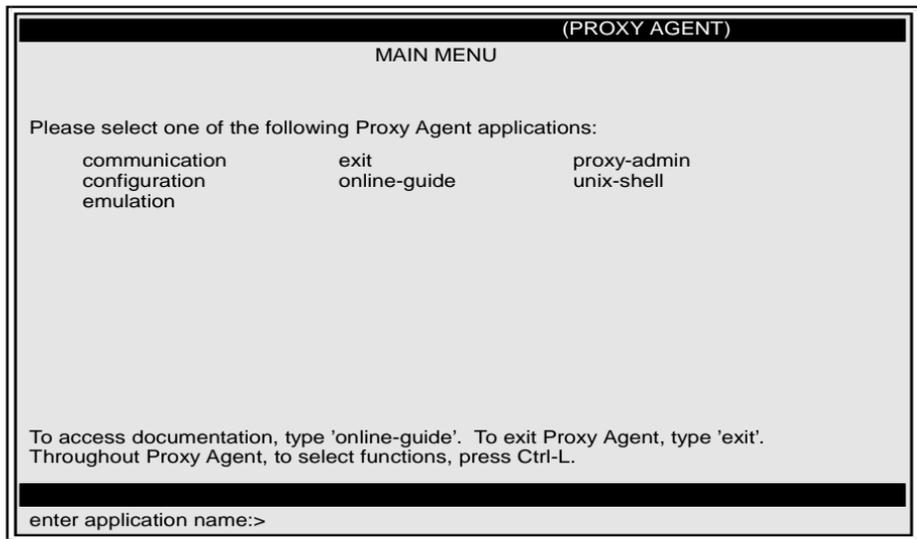
6 For special instructions to edit the Devices file or the Dialers file, refer to [Chapter 15, "I/O Setup Application"](#).

7 To exit file from the Menu Bar, select **File > Exit**.

Result: The system displays the DEFINITY_Proxy folder.

Review of the Main Menu

The Proxy Agent MAIN MENU contains the commands to access the Proxy Agent application screens, as show in the figure below.



sdnmmain LJK 040798

Figure 10. Proxy Agent MAIN MENU

The table below contains the descriptions of the commands on the Proxy Agent MAIN MENU.

Table 11. Proxy Agent MAIN MENU

| Command | Description |
|---------------|---|
| communication | Accesses the Communication application and displays the COMMUNICATION MANAGER screen. Users can manually connect and disconnect a Proxy Agent to and from managed nodes for real-time administration. Refer to Chapter 12, "Communication Application" |
| emulation | Accesses the Emulation application. The Emulation screen provides direct communication with a managed node for real-time administration. Refer to Chapter 13, "Emulation Application" |
| configuration | Accesses the Configuration application. This application contains two commands to edit either of the configuration screens: <ul style="list-style-type: none">• change hardware to edit the CHANGE HARDWARE screen• change user-interface to edit of the CHANGE USER_INTERFACE screens (4 pages) Refer to Chapter 14, "Configuration Application" |
| | 1 of 3 |

Table 11. Proxy Agent MAIN MENU

| Command | Description |
|-------------|--|
| proxy-admin | <p>Accesses the PROXY ADMIN menu. This menu contains the commands listed below:</p> <ul style="list-style-type: none"> • The change and display commands allow users to administer or view the application screens listed below: <ul style="list-style-type: none"> – Alarm Path – Filter Set – Default Location – Managed Nodes – Network Managers – Default Login • The add and remove commands allow users to access the FILTER SET screen and create or delete filter sets • The start and stop commands allow users to turn on or turn off the Proxy Agent • The quit command allows users to exit the PROXY ADMIN menu <p>Refer to "Review of the Proxy Admin Menu" on page 160</p> |
| exit | Closes the Proxy Agent MAIN MENU. |
| | 2 of 3 |

Table 11. Proxy Agent MAIN MENU

| Command | Description |
|--------------|---|
| online-guide | Displays a window with instructions to access the UnixWare Desktop in order to view the Proxy Agent Installation Guide and the User Guide. The Online Guide has been removed from the Proxy Agent. Refer to "Access the User Documentation" on page 150 |
| unix-shell | Accesses the UNIX prompt. |
| | 3 of 3 |

Review of the Proxy Admin Menu

The PROXY ADMIN menu contains the commands to access the Proxy Agent administration screens and to start and stop the Proxy Agent. The figure below shows the commands on the PROXY ADMIN screen.

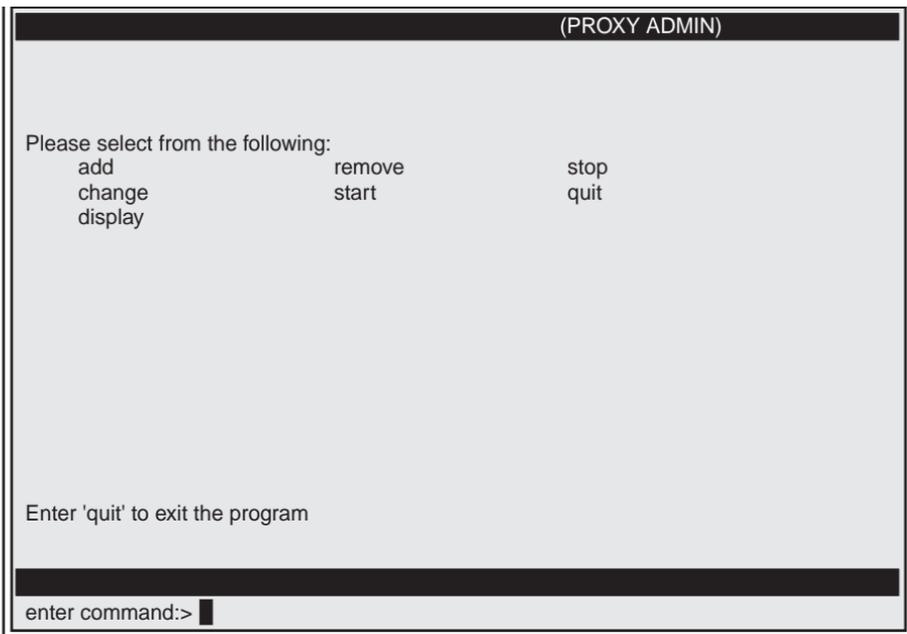


Figure 11. PROXY ADMIN screen

Command descriptions

The table below describes the commands on the PROXY ADMIN screen. Users must have a *g3maadm* login to execute the commands and administer the Proxy Agent.

Table 12. PROXY ADMIN screen

| Command | Description |
|---------|--|
| add | <p>Accesses the FILTER SET screen in the “add” mode. Users create the alarm filtering criteria for a new filter set with this command.</p> <p>Note: Users must STOP the Proxy Agent before executing the add command.</p> <p>Refer to Chapter 9, "Filter Set Administration".</p> |
| remove | <p>Accesses the FILTER SET screen in the “remove” mode. Users can delete existing alarm filters with this command.</p> <p>Note: Users must STOP the Proxy Agent before executing the remove command.</p> <p>The Proxy Agent executes one of the options listed below:</p> <ul style="list-style-type: none"> • Deletes the filter set if it is not assigned to any managed node • Replaces the filter set with the <i>default</i> filter if the filter is assigned to managed nodes <p>Refer to Chapter 9, "Filter Set Administration".</p> |
| | 1 of 3 |

Table 12. PROXY ADMIN screen

| Command | Description |
|---------|--|
| change | <p>Accesses the administration screens listed below. The <i>change</i> command allows users to edit the selected screen.</p> <p>Note: Users must STOP the Proxy Agent before executing the <i>change</i> command.</p> <ul style="list-style-type: none">• change network-managers Refer to Chapter 6, "Network Managers Administration"• change default-location Refer to Chapter 7, "Default Location Administration"• change alarm-path Refer to Chapter 8, "Alarm Path Administration"• change filter-set Refer to Chapter 9, "Filter Set Administration"• change managed-nodes Refer to Chapter 11, "Managed Nodes Administration"• change default login Refer to Chapter 10, "Review of the Default Login Screen" |
| | 2 of 3 |

Table 12. PROXY ADMIN screen

| Command | Description |
|---------|--|
| display | <p>Shows the administration screens and the STATUS screen in the view-only mode. The display command does not allow users to change the screens.</p> <p>Note: Users do not have to STOP the Proxy Agent before executing the <i>display</i> command.</p> <ul style="list-style-type: none"> • display alarm-path • display filter-set • display default-location • display default-login • display managed-nodes • display status -- Refer to "Display the Status Screen" on page 170 |
| start | <p>Initiates a Proxy Agent connection to the managed nodes. Refer to "Start the Proxy Agent" on page 164</p> |
| stop | <p>Drops the Proxy Agent connection to the managed nodes. Refer to "Stop the Proxy Agent" on page 171</p> |
| quit | <p>Closes the PROXY ADMIN screen and displays the Proxy Agent MAIN MENU.</p> |
| | 3 of 3 |

Start the Proxy Agent

The PROXY ADMIN screen contains the command to **start** the Proxy Agent System connection to the administered managed nodes.

Each time users start the Proxy Agent, they should also display the STATUS screen to verify that the Proxy Agent is active.

Procedure

Complete the procedure below to start the Proxy Agent connection.

- 1 Access the PROXY ADMIN screen. In the command line,
 - Type **start proxy-agent**
 - Press **ENTER**

Result: The system displays the command window that contains the prompt:
Do you wish to continue? Yes No

- 2 To select Yes, press **ENTER**.

Result: The system starts the Proxy Agent. Then, the system displays the PROXY ADMIN screen with the confirmation message:

```
Command completed successfully.
```

Display of the Status Screen

The STATUS screen is a **view-only** screen that contains the information listed below:

- Proxy Agent connection state
- Alarm forwarding state
- Connection statistics **only** for the ECS, G3, and MCU managed nodes

The STATUS screen does **not** display any connection statistics for the managed nodes listed below:

- DEFINITY Audix
- INTUITY Audix
- INTUITY Interchange
- Call Management System (CMS)
- Conversant

The Proxy Agent **only** supports alarm handling for these products.

Figure

The figure below shows an example of a STATUS screen, which is a view-only screen.

| Node Name | | State | Last Connection | Attempts | Requests | Errors |
|-----------|---------|-------------------|-----------------|-----------|-------------------|--------|
| Con Type | Timeout | Last Used | Connects | Responses | Counters | Reset |
| ecs1 | up | 12/01/99 14:37:48 | 1 | 85 | 0 | |
| static | | 12/01/99 15:08:51 | 1 | 85 | | |
| g3 | idle | | 0 | 0 | 0 | |
| dynamic | 60 | | 0 | 0 | 12/05/99 11:03:55 | |

Command successfully completed, select Cancel to return to the menu

sdnmdst LJK 092299

Figure 12. STATUS screen

Review of the Status Screen Fields

The table below contains the description for each column on the STATUS screen. Several of the columns contain two types of data in the column.

Table 13. STATUS screen

| Column | Description |
|-------------------|---|
| Proxy Agent State | Identifies the current activity status of the Proxy Agent: active -- The Proxy Agent has been started not active -- The Proxy Agent has been stopped |
| Alarm Forwarding | Identifies the current state of the alarm forwarding feature. The alarm forwarding feature is active only if the user has administered the ALARM PATH screen. Users can turn-off alarm forwarding for individual managed nodes from the MANAGED NODES screen. The states include: ok -- Alarm forwarding is active and functioning failed -- Alarm forwarding is active, but is not functioning other -- Identifies one of the following conditions: <ul style="list-style-type: none"> • Proxy Agent is not active • Alarm forwarding feature is not turned on |
| | <i>1 of 3</i> |

Table 13. STATUS screen

| Column | Description |
|-----------|---|
| Node Name | Identifies the name of the managed node that is associated with the Proxy Agent. |
| Con Type | Identifies the type of Proxy Agent connection that users administer for ECS, G3, and MCU systems. A connection can be one of the types listed below: <ul style="list-style-type: none"> • static (continuous connection) • dynamic (temporary connection on an as-needed basis) |
| State | The State field identifies the current status of the Proxy Agent connection to a managed node. The states include: <ul style="list-style-type: none"> init (initiate) -- A connection attempt is in progress up -- The connection is established down -- The connection attempt has failed off -- The connection has been turned off idle -- A dynamic connection is not connected in standby mode other -- The connection has failed and the state is unknown |
| | 2 of 3 |

Table 13. STATUS screen

| Column | Description |
|-----------------|--|
| Timeout | Contains the number of minutes a dynamic connection will remain up without receiving data transmission. |
| Last Connection | The date and time of the last successful connection . |
| Last Used | The date and time of the last successful data retrieval . |
| Attempts | The number of connection attempts since the counter was reset to zero. |
| Connects | The number of successful connections since the counter was reset to zero. |
| Data Requests | The number of requests for data since the counter was reset to zero. |
| Data Responses | The number of successful responses to data requests since the counter was reset to zero. |
| Errors | The number of errors that occurred during data requests since the counter was reset to zero. |
| Counters Reset | The date and time the counter was reset to zero. |
| | 3 of 3 |

Display the Status Screen

Users should display the STATUS screen each time they start the Proxy Agent so that they can review the information listed below:

- Verify that the Proxy Agent connection is active
- View the status of the Alarm Forwarding feature
- View the connection statistics for the G3, ECS, and MCU managed nodes

Procedure

Complete the procedure below to display the STATUS screen.

- 1 Access the PROXY ADMIN menu. In the command line,
 - Type **display status**
 - Press **ENTER**

Result: The system displays the STATUS screen.

- 2 Check the STATUS screen to verify the current state of the Proxy Agent connections and statistics.
- 3 Press **Ctrl-X** to exit the screen.

Result: The system closes the STATUS screen and displays the PROXY ADMIN screen.

Stop the Proxy Agent

The PROXY ADMIN screen contains the command to **stop** a Proxy Agent connection to the administered managed nodes.

Users must **stop** the Proxy Agent **before** they can enter a **change** command to edit an administration screen.

Users do **not** have to stop the Proxy Agent entering a **display** command. Users can view an administration screen while the Proxy Agent is running.

Complete the procedures below to stop the Proxy Agent connection.

- 1 Access the PROXY ADMIN screen. In the command line,
 - Type **stop proxy-agent**
 - Press **ENTER**

Result: The system displays the command window that contains the prompt:
Do you wish to continue? Yes No

- 2 To select Yes, press **ENTER**.

Result: The system stops the Proxy Agent. Then, displays the PROXY ADMIN screen with the confirmation message: Command completed successfully.

6 Network Managers Administration

Chapter Contents

- [Introduction](#) [173](#)
- [Review the Network Managers Screen](#) [174](#)
- [Administer the Network Managers](#) [179](#)

Introduction

The purpose of the NETWORK MANAGERS screen is to administer the communication link between the Proxy Agent and the Network Management System (NMS).

see also:

- Management Information Base (MIB) [Chapter 1, "Management Information Base \(MIB\)"](#)
- Cache Mechanism [Chapter 1, "Cache mechanism"](#)
- SNMP Traps [Chapter 1, "SNMP Access"](#)

The sections below describe interactions between the network managers and the Proxy Agent.

Review the Network Managers Screen

The figure below shows the fields on the NETWORK MANAGERS screen.



Figure 13. Network Managers screen

The table below contains the field descriptions for the NETWORK MANAGERS screen.

Table 14. Network Managers Screen

| Field | Description |
|----------------------|---|
| Get Community String | <p>Identifies the Proxy Agent's SNMP Get Community String. The NMS network manager uses the get community string to validate SNMP get requests.</p> <p>Valid options for this field are:</p> <ul style="list-style-type: none">• public (default)• Any name that identifies a private network <p> CAUTION:</p> <p>Users must administer the name of the get community string (public or private) in the comparable fields on the NMS screens. The name must match on both systems, otherwise the get request will fail.</p> <p>Required field.</p> <p>Field size: 15 characters</p> |

Table 14. Network Managers Screen

| Field | Description |
|----------------------|---|
| Set Community String | <p data-bbox="557 218 1177 311">Identifies the Proxy Agent's Get Community String. The NMS network manager uses the set community string to validate SNMP set requests.</p> <p data-bbox="557 329 940 355">The default for this field is: g3pa</p> <p data-bbox="557 381 759 422"> CAUTION:</p> <p data-bbox="557 433 1177 557">Users must administer the g3pa as the name of the set community string in the comparable fields on the NMS screens. The name must match on both systems, otherwise the set request will fail.</p> <p data-bbox="557 588 732 614">Required field.</p> <p data-bbox="557 629 850 655">Field size: 15 characters</p> |
| | 2 of 4 |

Table 14. Network Managers Screen

| Field | Description |
|----------------|---|
| TYPE OF ACCESS | <p data-bbox="557 220 1177 277">Identifies the type of access a network manager has to the Proxy Agent.</p> <p data-bbox="557 298 1177 355">The HELP list (Ctrl-Y) contains the valid options for this field:</p> <p data-bbox="605 370 996 396">READ/WRITE ACCESS TO MIB</p> <p data-bbox="605 412 900 438">READ ACCESS TO MIB</p> <p data-bbox="605 453 822 479">RECEIVE TRAPS</p> <ul data-bbox="581 495 1177 831" style="list-style-type: none"> <li data-bbox="581 495 1177 619">• Read/Write access to MIB -- allows the NMS to read and write data to the MIB. The network manager has complete access to the MIB. The DNM applications <i>require</i> read/write access. <li data-bbox="581 629 1177 754">• Read access to MIB -- allows the NMS to <i>only</i> read data in the MIB. The NMS cannot change MIB objects that are set with the SNMP SET command. <li data-bbox="581 764 1177 831">• Receive Traps -- allows the NMS to receive SNMP traps from the Proxy Agent. <p data-bbox="557 852 1135 909">Note: DNM Applications also require SNMP trap reception.</p> <p data-bbox="557 930 1147 956">Default: READ/WRITE ACCESS TO MIB in line 1</p> |
| | 3 of 4 |

Table 14. Network Managers Screen

| Field | Description |
|------------|---|
| IP ADDRESS | <p data-bbox="557 220 1141 277">Identifies the Internet Protocol (IP) address of the NMS network manager.</p> <p data-bbox="557 298 912 324">The valid options for this field:</p> <ul data-bbox="581 339 1184 588" style="list-style-type: none"><li data-bbox="581 339 1184 458">• Asterisk (*) -- default in line 1. The asterisk allows access to all NMS network managers. The asterisk is not valid for RECEIVE TRAPS access.<li data-bbox="653 479 677 500">or<li data-bbox="581 521 1039 588">• IP address of the NMS in dot format. Example: 126.1.205.86 <p data-bbox="557 614 1117 723"> SECURITY ALERT: Users should enter the IP address for each network manager to limit access to the MIB.</p> <p data-bbox="557 754 732 780">Required field.</p> <p data-bbox="557 795 852 821">Field size: 15 characters</p> |

Administer the Network Managers

The NETWORK MANAGERS screen contains the fields to administer the communication link between the Proxy Agent and Network Management System (NMS).

Users administer each NMS as a **network manager** and assign the type of access each network manager has to the Proxy Agent Management Information Base (MIB)

Required access

Users must administer **three** types of access for each network manager:

- Read/Write Access to MIB
- Read only Access to MIB
- Receive Traps

Users assign each type of access on a separate line in the NETWORK MANAGERS screen.

PA001 form

The data that users enter in the fields on the NETWORK MANAGERS screen must **match** the data on the PA001 form in the Proxy Agent section.

Procedure

Complete the procedure below to **add** new network managers or to **change** data for existing network managers.

1 At the Proxy Agent MAIN MENU,

- Type **proxy-admin**
- Press **ENTER**

Result: The system displays the PROXY ADMIN menu.

2 In the command line,

- Type **change network-managers**
- Press **ENTER**

Result: The system displays the NETWORK MANAGERS screen.

3 Compare the data on the PA001 form to the fields on the NETWORK MANAGERS screen:

Get Community String: **public**

Set Community String: **g3pa**

If the data does **not** match, then change the fields to match the data on the PA001 form.

- 4 For **each** network manager, complete the fields below to add the READ/WRITE ACCESS TO MIB permission:
 - In the **TYPE OF ACCESS** column, move the cursor to a blank line number.
 - Press **Ctrl-Y** to display the Help list
 - Select **READ/WRITE ACCESS TO MIB**
 - Press **ENTER** to display the selection in the field
 - In the **IP ADDRESS** column, type the [**IP address**] in the field for the same line number. Example of an IP Address in the dot format: **126.1.205.86**
- 5 For **each** network manager, complete the fields below to add the RECEIVE TRAPS permission. The IP address should match the address in step [4](#) for each network manager.
 - In the **TYPE OF ACCESS** column, move the cursor to a blank line number.
 - Press **Ctrl-Y** to display the Help list
 - Select **RECEIVE TRAPS**
 - Press **ENTER** to display the selection in the field
 - In the **IP ADDRESS** column, type the [**IP address**] in the field for the same line number.
- 6 Repeat steps [4](#) and [5](#) to administer **each** network manager.
- 7 Press **Ctrl-E** to submit the changes.

Result: The system save the data and displays the PROXY ADMIN menu.
- 8 **New Installations.** Complete the procedure to ["Administer the Default Location" on page 191.](#)

7 Default Location Administration

Chapter Contents

- [*Introduction*](#) [*183*](#)
- [*Review of the Default Location Screen*](#) [*185*](#)
- [*Administer the Default Location*](#) [*191*](#)

Introduction

The DEFAULT LOCATION screen allows users to designate the type of submap that shows the location of managed nodes and their associated Proxy Agents.

The Network Management System (NMS) displays the submaps in a graphical format with icons that represent the managed nodes and the Proxy Agent. Users can easily monitor the health and status of all the managed nodes from the submaps.

Users can organize the managed nodes by location or by custom categories.

The examples below offer some suggestions for organizing the managed nodes:

- **Generic submap** -- Select the generic submap to view all the managed nodes and Proxy Agents on one submap. The generic submap is the system default.
- **USA submap** -- Select the USA submap to show the location of managed nodes in the lower 48 states and in Alaska and Hawaii. The associated **State** submap shows the Proxy Agent icon with connecting lines to the managed nodes icons that are located in that state.
- **Custom submap** -- Select the custom submap to organize the managed nodes by categories, such as private networks, regions, functions, or international locations. Use the associated **Submap Name** to identify groups or locations within the categorizes, such as:
 - Private Network may consist of the Lab and Testing groups
 - Regions may consist of North, East, South, and West groups

- Functions may consist of Telemarketing, Sales, and Customer Service groups
- International locations may consist of Africa, Spain, Greece groups

Users can organize the managed nodes by selecting one type of submap or any combination of the three submaps.

Managed Nodes screen

Users can change the type of submap on the MANAGED NODES screen for individual managed nodes. The change **overrides** the submap selection on the DEFAULT LOCATION screen **only** for the individual managed node.

NMS submaps

The submaps that display on the NMS network servers provide the current status of the managed nodes through the use of colored icons and different types of connecting lines.

The **color** of the managed node icons identifies the health status of the managed nodes. The icon color changes to indicate the highest severity level of any DNM exception that has occurred on the managed nodes.

The **type** of the connecting lines (broken or solid lines) between the Proxy Agent and managed nodes icons identify either a static or dynamic connection. The **color** of the line indicates the connection status of the Proxy Agent.

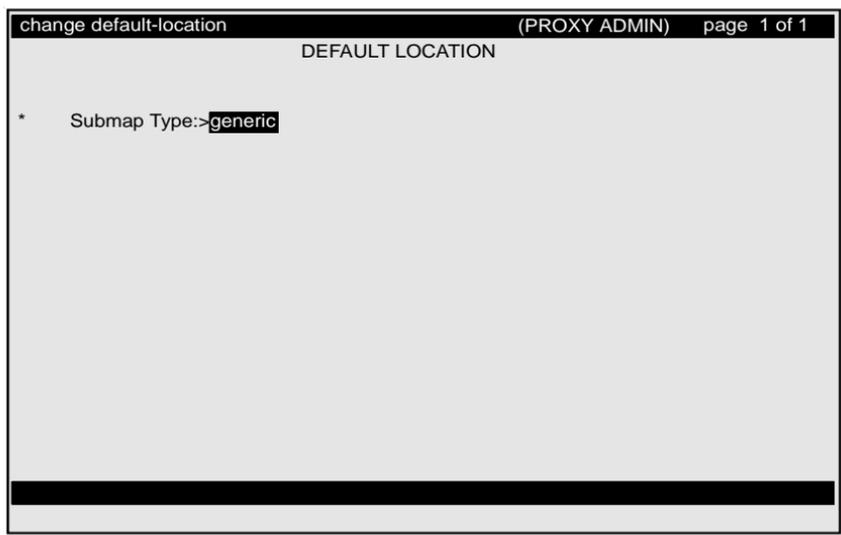
Review of the Default Location Screen

The fields that display on the DEFAULT LOCATION screen depend on the type of submap that users select as the default location for new managed nodes.

The figures, on the next pages, show the fields that display on the DEFAULT LOCATION screen for the submaps listed below:

- Generic submap (default)
- USA submap
- Custom submap

Generic submap screen The figure below shows the DEFAULT LOCATION screen for the generic submap. Only the Submap Type field displays for generic submaps.



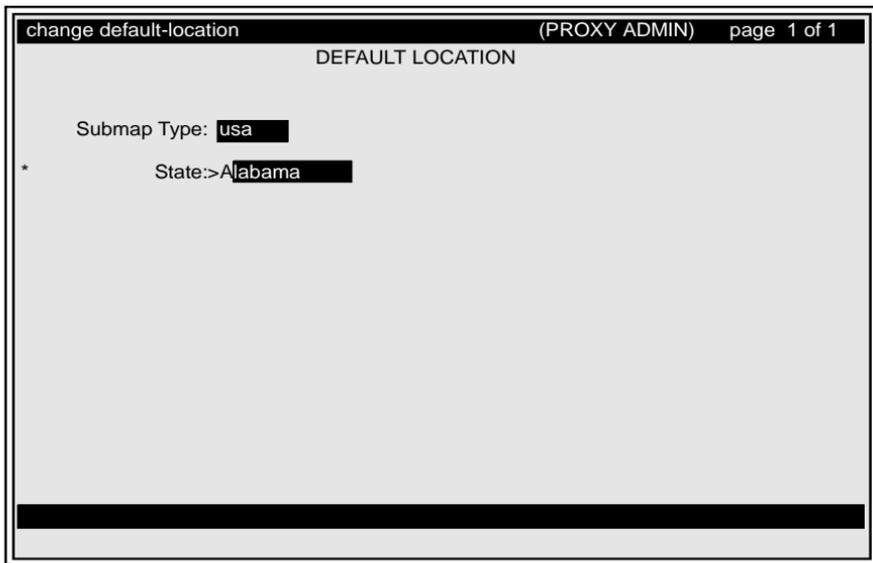
sdnmdefg LJK 040798

Figure 14. Generic submap field

USA submap screen

The figure below shows the DEFAULT LOCATION screen for the USA submap with the following fields:

- Submap Type
- State (Alabama is the default state)



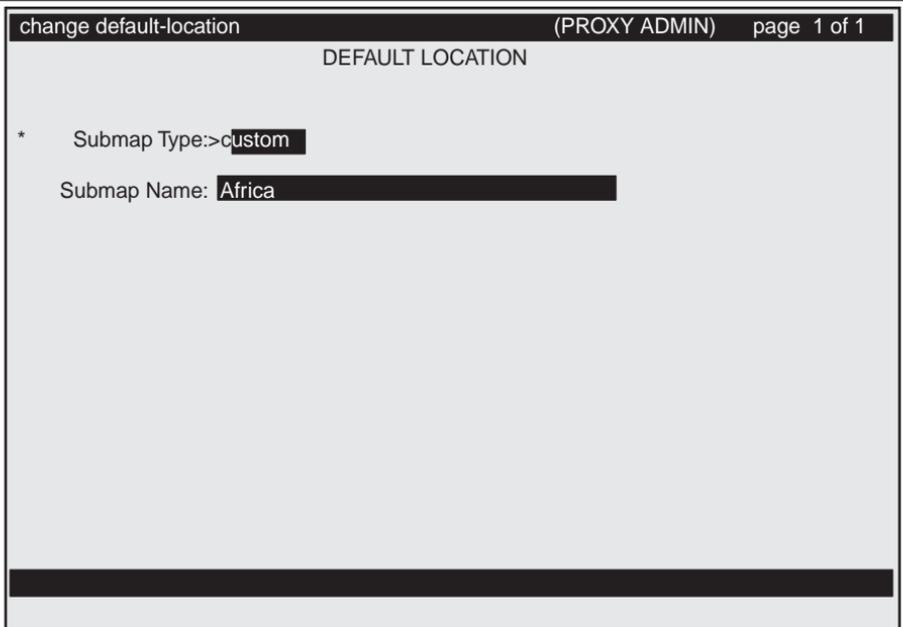
sdnmdefu LJK 040798

Figure 15. USA submap fields

**Custom
submap screen**

The figure below shows the DEFAULT LOCATION screen for the custom map with the following fields:

- Submap Type
- Submap Name



The screenshot displays a web-based configuration interface. At the top, a dark header bar contains the text "change default-location" on the left, "(PROXY ADMIN)" in the center, and "page 1 of 1" on the right. Below the header, the main content area is titled "DEFAULT LOCATION" in a large, centered font. Underneath the title, there are two configuration fields. The first field is labeled "Submap Type:" followed by a dropdown menu showing the selected value "custom". The second field is labeled "Submap Name:" followed by a text input field containing the value "Africa". The entire interface is enclosed in a thin black border.

Figure 16. Custom submap fields

Field descriptions The table below contains the field descriptions for the DEFAULT LOCATION screen.

Table 15. Default Location Screen

| Field | Description |
|-------------|---|
| Submap Type | <p>Identifies the type of submap.</p> <p>The Help list (Ctrl-y) contains the valid options for this field:</p> <ul style="list-style-type: none">generic (default)usacustom <p>The fields that display on the DEFAULT LOCATION screen will change depending on the type of submap:</p> <ul style="list-style-type: none">• If users select usa, the system displays the State field• If users select custom, the system displays the Submap Name field <p>Users can change the submap type for individual managed nodes on page C of the MANAGED NODES screen. The changes override the submap type selected on the DEFAULT LOCATION screen only for the individual managed node.</p> |
| | 1 of 2 |

Table 15. Default Location Screen

| Field | Description |
|-------------|--|
| State | <p>If users select usa in the <i>Submap Type</i> field, the system displays the State field.</p> <p>The Help list (ctrl-y) contains 50 states as valid options for this field.</p> <p>Users select the appropriate state for the location of the managed nodes.</p> <p>When users administer the managed nodes on the MANAGED NODES screen, they can change the state location for individual managed nodes.</p> <p>System default: Alabama</p> |
| Submap Name | <p>If users select custom in the <i>Submap Type</i> field, the system displays the Submap Name field.</p> <p>Users can type a default name for the custom submaps.</p> <p>When users administer the managed nodes on the MANAGED NODES screen, then they can change the submap name for individual managed nodes.</p> <p>Default: Blank</p> <p>Field size: 40 characters</p> |
| | <i>2 of 2</i> |

Administer the Default Location

This section contains the procedures to select a submap as the **system** default location for new managed nodes.

Note: To save time during the administration of many managed nodes with different locations, users can change the submap selection on the DEFAULT LOCATION **before** they administer managed nodes with the same on the MANAGED NODES screen.

Procedure

Complete the procedure below to select the system **default** location for new managed nodes.

- 1 Access the PROXY ADMIN menu.
- 2 Stop the Proxy Agent, if running.
- 3 In the command line on the PROXY ADMIN menu,
 - Type **change default-location**
 - Press **ENTER**

Result: The system displays the DEFAULT LOCATION screen.

4 In the *Submap Type* field,

- Press **Ctrl-Y** to display the Help list
- Select a submap type from the list.
- Press **ENTER**.
- Then, go to the appropriate step for the selected submap:
 - generic** (go to step [7](#))
 - usa** (go to step [5](#))
 - custom** (go to step [6](#))

5 **USA submap type.** In the *State* field select a state as the default location:

- Press **Ctrl-Y** to display the Help list
- Select a **state** from the list
- Press **ENTER**
- Go to step **7**

6 **Custom submap type.** In the *Submap Type* field,

- Type a [**custom name**] for the default location
- Go to step **7**

7 Press **Ctrl-E** to submit the changes.

Result: The system saves the changes and displays the PROXY ADMIN menu.

8 **New Installation.** Complete the procedure to ["Administer the Alarm Path" on page 199.](#)

8 Alarm Path Administration

Chapter Contents

- [Introduction](#) [194](#)
- [Review of the Alarm Path Screen](#) [196](#)
- [Administer the Alarm Path](#) [199](#)

Introduction

The ALARM PATH screen contains the fields to administer the alarm stream to enable the Proxy Agent to receive alarms from managed nodes and to forward alarms to the Initialization and Administration System (INADS).

In this release, the Proxy Agent only **receives** alarms from the managed nodes listed below:

- DEFINITY ECS, G3, MCU, and Prologix systems
- DEFINITY Audix
- INTUITY Audix
- INTUITY Interchange
- Call Management System (CMS)
- Conversant system

The Proxy Agent **forwards** the alarms received from the managed nodes to INADS, which is the default destination. Users can edit the alarm destination fields in order to forward the alarms to an alarm reception device that is supported by the **current** release of the Proxy Agent.

Alarm forwarding

The alarm forwarding feature is active **only** if the user administers all of the *alarm source* and *alarm destination* fields on the ALARM PATH screen.

On page **A** of the MANAGED NODES screen, users can turn off alarm forwarding for individual managed nodes **without** changing the ALARM PATH screen.

See also

To troubleshoot alarm problems, refer to ["View Alarm and Error Logs" on page 338](#).

Review of the Alarm Path Screen

The first time the user accesses the ALARM PATH screen, only the ALARM SOURCE fields display on the screen. The ALARM DESTINATION fields display after the user enters data in the ALARM SOURCE fields.

| change alarm-path (PROXY ADMIN) Page 1 of 1 | |
|---|---------------------|
| ALARM PATH | |
| ALARM SOURCE | ALARM DESTINATION |
| * TTY Port: >tty1a16 | TTY Port: tty1a15 |
| Phone: 555-123-4567 | Phone: 800-535-3573 |

Figure 17. Alarm Path screen

Field descriptions The table below contains the descriptions of the alarm source fields and alarm destination fields on the ALARM PATH screen,

Table 16. Alarm Path Screen

| Field | Description |
|---------------------------------|--|
| ALARM SOURCE TTY Port | <p>Identifies port name of the Proxy Agent device that receives alarms from the managed nodes.</p> <p>The Proxy Agent only receives alarms from supported systems that users administer on the MANAGED NODES screen.</p> <p>Note: The Proxy Agent does not support the receipt of alarms from Trouble Trackers.</p> <p>Default: Blank</p> <p>Field size: 12 characters</p> |
| ALARM SOURCE Phone | <p>Identifies the Proxy Agent phone number for the device that receives alarms from the managed nodes.</p> <p>Required field</p> <p>Default: Blank</p> <p>Field size: 16 characters</p> |
| <i>1 of 2</i> | |

Table 16. Alarm Path Screen

| Field | Description |
|--------------------------------------|---|
| ALARM DESTINATION TTY Port | Identifies the port name of the Proxy Agent device that forwards alarms to INADS, which is the default destination. Default: Blank Field size: 12 characters |
| ALARM DESTINATION Phone | Contains the INADS phone number (1-800-535-3573) for the device that receives alarms from the Proxy Agent. If necessary, users can edit the INADS phone number to add an number (9) to access an outside line (9-1-800-535-3573). <i>Note:</i> Users can edit the <i>alarm destination</i> fields in order to forward the alarms to an alarm reception device that supports the alarm format from the current release of the Proxy Agent. Required field Default: INADS phone number: 1-800-535-3573 Field size: 30 characters |
| | 2 of 2 |

Administer the Alarm Path

The ALARM PATH screen enables the Proxy Agent to **receive** alarms from managed nodes and to **forward** alarms to INADS.

PA001 form

Users should refer to the sections below on PA001 form to get the data that they must enter on the ALARM PATH screen:

- In the **Devices** section, refer to the *Device Name* fields for the TTY ports that Receive Alarms and Send (forward) Alarms.
- In the **Proxy Agent** section, refer to *Alarm Path* table for phone numbers of the devices for the alarm source and alarm destination.

The default for the destination phone number is INADS phone number. Users can enter a different phone number in the field.

Procedure

Complete the procedure below to administer the ALARM PATH screen to receive and forward alarms.

- 1 Access the PROXY ADMIN menu.
- 2 Stop the Proxy Agent, if running.
- 3 In the command line on the PROXY ADMIN menu,
 - Type **change alarm-path**
 - Press **ENTER**

Result: The system displays the ALARM PATH screen.

- 4 In the ALARM SOURCE column, refer to the PA001 form and type the data in the fields below.

ALARM SOURCE fields

TTY Port: Type [ttyxxx] for the Proxy Agent device that **receives** alarms

Phone: Type the [phone number] for the Proxy Agent device

- 5 In the ALARM DESTINATION column, refer to the PA001 form and type the data in the fields below.

ALARM DESTINATION fields

TTY Port: Type [ttyxxx] for the Proxy Agent device that **forwards** (sends) alarms

Phone: **1-800-535-3573** to forward alarms to INADS (default)

Note: You enter a different number for the destination of the alarm **if** the alarm reception device supports alarm format from the current release of the Proxy Agent.

- 6 Press **Ctrl-E** to submit the changes.

Result: The system saves the changes and displays the PROXY ADMIN screen.

- 7 **New Installation.** Complete the procedure to ["Administer the Filter Sets" on page 219.](#)
- 8 Restart the Proxy Agent.

9

Filter Set Administration

Chapter Contents

- [Introduction](#) [202](#)
- [Examples of Filter Sets](#) [206](#)
- [Review of the Filter Set Screen](#) [211](#)
- [Administer the Filter Sets](#) [219](#)
 - [Add a New Filter Set](#) [220](#)
 - [Change an Existing Filter Set](#) [223](#)
 - [Display the Filter Set Screen](#) [226](#)
 - [Remove a Filter Set](#) [227](#)

Introduction

The new Filter Set application allows users to create filters that the Proxy Agent applies to alarms in order to block the forwarding of certain alarms to INADS.

Users can create filtering criteria on the FILTER SET screen and then administer the filter sets to all or individual systems on the MANAGED NODES screen.

When a managed node generates an alarm, the Proxy Agent compares each criteria in the filter for a **match** against the alarm. If a match is *found* for any filter criteria, then the Proxy Agent does *not* forward the alarm to INADS. If match is *not* found, then the Proxy Agent *forwards* the alarm to INADS.

Filter set definition

A **filter set** is a group of filters that contains one or more of the four types of filtering criteria listed below:

- Pattern matching -- can include pattern files and character strings
- Alarm severity
- Day of the Week
- Time of Day

For each filter set, users can create a maximum of **12** filters that contain all or any combination of the four types of filtering criteria.

An alarm must match all four sets of criteria for a filter before the Proxy Agent blocks the alarm.

Default filter-set When users install or upgrade to release 3.0 of the Proxy Agent, the system supplies a **blank** default filter set. Users can implement one of the options below to set up the system default for alarm filtering:

- Leave the default filter set blank. The system default would be that the Proxy Agent forwards alarms without filtering.
- or
- Add filtering criteria to the default filter set. The system default would be the criteria in the default filter set.

In either event, the Proxy Agent applies the default filter set to all alarms **unless** the user executes one of the options below for individual managed nodes:

- Selects a different filter
- or
- Selects no filter set

Users need to select one of the alarm filtering options since the Proxy Agent does **not** allow the default filter set to be removed.

Filter set commands

Users can administer or view the FILTER SET screen from the PROXY ADMIN menu by executing the commands listed below:

- **add filter-set** to create new filter sets
- **change filter-set** to modify existing filter sets
- **remove filter-set** to delete filter sets, except the *default* filter
- **display filter-set** to view filter sets

**Pattern
matching**

On the FILTER SET screen, the users can enter two types of pattern matching criteria:

- Individual character strings that users enter in the field
- File names that user select from a list

File names refer to *pattern* files that contain groups of character strings. Only the system administrator should create a pattern file.

All pattern files must reside in the **/usr/g3-ma/agent/patterns** directory. The format for the pattern file contains a group character strings that the Proxy Agent matches on a per line basis. The file can contain comment lines that start with one of the characters listed below:

- Number symbol (#)
- Tab
- Space

Once the pattern file is created, users can add the file to any filter set on the FILTER SET screen.

**Boolean
operator**

On the FILTER SET screen, users can specify the *boolean* operator "**not**" if they want the Proxy Agent to block alarms that do **not** match a specified pattern matching criteria.

If the boolean operator (BOOL OPER) field is **blank**, then the Proxy Agent blocks alarms if they match one or more of the pattern matching criteria in the filter set.

Alarm severity On the FILTER SET screen, users can block alarms based on the severity of the alarm. Users can select one or more of the alarm severity levels listed below:

Note: The abbreviated titles are **vertically** stacked above the ALARM SEVERITY columns.

- Major (MAJ)
- Minor (MIN)
- Warning (WRN)
- Downgraded Warning (DGW)
- Cleared Alarm Notification (CLR)
- System Restart (RST)
- Resolved (RES)

The Proxy Agent **blocks** alarms if they match any of the selected alarm severity criteria and the other filter criteria, if any.

Day of week On the FILTER SET screen, users can block alarms based on the day of the week (Monday through Sunday). The Proxy Agent **blocks** alarms if they match any of the selected days of the week and the other filter criteria, if any.

Time of day On the FILTER SET screen, users can block alarms that the Proxy Agent receives during a specified window of time. Users can enter the hours (based on the 24-hour clock) in the *Start* and *End* fields.

The Proxy Agent **blocks** alarms if they match any of the time of day criteria and the other filter criteria, if any.

Examples of Filter Sets

To better understand the workings of the new Filter Set application, this section contains two examples of a some common scenarios that users may choose to create.

The examples use two pattern files described below. All pattern files must reside in the **/usr/g3-ma/agent/patterns** directory. The lists of objects in the examples below are not intended to be complete. The lists only serve as examples of the types of objects that users can include in a pattern file.

The **station** pattern file contains a list of DEFINITY station maintenance object names:

- ANL_LINE
- ANL_BD
- DIG_LINE
- MET_LINE
- MET_BD

The **trunk** pattern file contains a list of DEFINITY trunk maintenance object names:

- AUX_TRK
- CO_TRK
- DID_TRK
- TIE_TRK
- ISDN_TRK

Explanation

Filter Set 1 consists of five filters to block the alarm streams that contain one or more of the patterns listed in the **station** pattern file and the **trunk** pattern file.

Each filter is explained below:

- Filter 1 blocks the forwarding of all **station** alarms.
- Filter 2 blocks the forwarding of all **trunk** alarms received during **working** hours. The criteria below defines the working hours for this filter:
 - The *Day of Week* criteria block alarms Monday through Friday
 - The *Time of Day* criteria block alarms between 8:00 and 17:00 hours (8:00 a.m. to 5:00 p.m.)
- Filters 3 through 5, together, block the forwarding of all **non-major trunk** alarms received during **off** hours:
 - Filter 3 blocks non-major trunk alarms on Saturday and Sunday
 - Filter 4 blocks non-major trunk alarms on Monday through Friday *before* working hours (0:00 to 07:59)
 - Filter 5 blocks non-major trunk alarms on Monday through Friday *after* working hours (17:01 through 23:59)

Review of Filter Set 2

As shown in the figure below, the purpose of Filter Set 2 (fset2) is to **block** the forwarding of the alarm streams listed below:

- All cleared alarm notifications
- All minor alarms that are **not** listed in the trunk pattern file
- All alarms from the board located in port network 3, carrier C, slot 8
- All restart notifications that do **not** contain the COLD1 level

| change filter-set | | | (PROXY ADMIN) page 1 of 1 | | | | | | | | | | | | | | | | | | | | | | |
|---------------------------|------|------------------|---------------------------|---|---|---|---|---|---|-------------|---|---|---|---|-------------|---|---|---|---|---|---|---|---|-------|-----|
| FILTER SET: fset2 | | | | | | | | | | | | | | | | | | | | | | | | | |
| PATTERN MATCHING CRITERIA | | | ALRM SEVERITY | | | | | | | | | | | | | | | | | | | | | | |
| FILE/ | BOOL | FILE NAME OR | M | M | W | D | C | R | R | DAY OF WEEK | | | | | TIME OF DAY | | | | | | | | | | |
| STRING OPER | | CHARACTER STRING | A | I | R | G | L | S | E | J | N | N | W | R | T | S | M | T | W | T | F | S | S | START | END |
| 1:* | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2: file | not | trunk | | | | | | | | | | | | X | | | | | | | | | | | |
| 3: string | | 03C08 | | | | | | | | | | | | | | | | | | | | | | | |
| 4: string | not | COLD1 | | | | | | | | | | | | | | | | | | | | | | | |
| 5: | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6: | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7: | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8: | | | | | | | | | | | | | | | | | | | | | | | | | |
| 9: | | | | | | | | | | | | | | | | | | | | | | | | | |
| 10: | | | | | | | | | | | | | | | | | | | | | | | | | |
| 11: | | | | | | | | | | | | | | | | | | | | | | | | | |
| 12: | | | | | | | | | | | | | | | | | | | | | | | | | |

Figure 19. Example of Filter Set 2

Explanation

Filter Set 2 consists of four filters that contain a pattern file, two character strings, and two boolean operators. These filters target very specific conditions for blocking alarm forwarding.

Each filter is explained below:

- Filter 1 blocks alarm forwarding of all **cleared alarm notifications** (CLR) for the alarm severity criteria.
- Filter 2 blocks alarm forwarding of **non-trunk** alarms with a **minor** (MIN) alarm severity criteria.
- Filter 3 blocks alarm forwarding of all alarms from the **board** located in port network 3, carrier C, slot 8 (03C08)
- Filter 4 blocks alarm forwarding of all **restart notifications** (RST) with a alarm severity level that is **not** COLD1.

Review of the Filter Set Screen

The figure below shows the fields on the blank FILTER SET screen.

| change filter-set | | (PROXY ADMIN) | | page 1 of 1 | | | | | | | | | | | | | | |
|---------------------------|------------|---------------|---------------|-------------|------------|------------|------------|------------|------------|-------------|-------------|------------|------------|------------|------------|------------|------------|------------|
| FILTER SET: [REDACTED] | | | | | | | | | | | | | | | | | | |
| PATTERN MATCHING CRITERIA | | | ALRM SEVERITY | | | | | | | | | | | | | | | |
| ----- | | | ----- | | | | | | | | | | | | | | | |
| FILE/ | BOOL | FILE NAME OR | M | M | W | D | C | R | R | DAY OF WEEK | TIME OF DAY | | | | | | | |
| STRING | OPER | CHARACTER | A | I | R | G | L | S | E | ----- | ----- | | | | | | | |
| | | STRING | J | N | N | W | R | T | S | M | T | W | T | F | S | S | START | END |
| 1:* | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| 2: | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| 3: | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| 4: | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| 5: | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| 6: | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| 7: | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| 8: | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| 9: | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| 10: | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| 11: | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| 12: | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |

sdhmfsl LJK 092399

Figure 20. Blank Filter Set screen

Screen layout The FILTER SET screen contains 12 lines to allow users to enter up to 12 filters in any of the fields in the four criteria columns:

- Pattern Matching Criteria (3 fields)
- Alarm Severity (7 fields)
- Day of Week (7 fields)
- Time of Day (2 fields)

Field descriptions

The table below contains the field descriptions for the FILTER SET screen.

Table 17. Filter Set Screen

| Field | Description |
|------------|---|
| FILTER SET | Contains the name of the filter set. To add a new filter set, the user types the name of the filter set in this field. To change, remove, or display an existing filter set, the user presses Ctrl-y in the field to display the HELP list and selects a filter set name from the list. Field size: 8 characters Default: Blank |
| | 1 of 7 |

Table 17. Filter Set Screen

| Field | Description |
|---|--|
| Pattern Matching Criteria FILE/STRING | <p>Identifies the type of pattern matching for the filter set.</p> <p>The HELP list (Ctrl-y) contains the valid options:</p> <ul style="list-style-type: none">file = a pattern file that contains a group of character strings and resides in the /usr/g3-ma/agent/patterns directorystring = a character string <p>Only the system administrator should create a <i>pattern</i> file.</p> <p>The format for the pattern file contains character strings that the Proxy Agent matches on a per line basis. The file can contain comment lines that start with one of the characters listed below:</p> <ul style="list-style-type: none">• Number symbol (#)• Tab• Space <p>Field size: 6 characters Default: Blank</p> |
| | <i>2 of 7</i> |

Table 17. Filter Set Screen

| Field | Description |
|---|--|
| Pattern Matching Criteria BOOL OPER | <p>Identifies the boolean operator “not” as a pattern matching criteria.</p> <p>Users can specify the <i>boolean</i> operator “not” if they want the Proxy Agent to block alarms that do <i>not</i> match a specified pattern matching criteria.</p> <p>If the boolean operator (BOOL OPER) field is blank, then the Proxy Agent blocks alarms if they match one or more of the pattern matching criteria in the filter set.</p> <p>The HELP list (Ctrl-y) only contains the not option.</p> <p>Field size: 4 characters</p> <p>Default: Blank</p> |
| | 3 of 7 |

Table 17. Filter Set Screen

| Field | Description |
|---|---|
| Pattern Matching Criteria FILE NAME or CHARACTER STRING | <p>Identifies the pattern file name or character string based on the selection in the FILE/STRING field.</p> <p>Users can execute one of the options (a, b, or c) below:</p> <ul style="list-style-type: none">a If <i>file</i> was selected in FILE/STRING field, then users must select a pattern file name from the Help list. The Help list (Ctrl-y) only contains the pattern files names that reside in the <i>/usr/g3-ma/agent/patterns</i> directory.b If <i>string</i> was selected in the FILE/STRING field, then users must type a character string in the field.c If <i>no</i> selection was made in the FILE/STRING field, then users must leave the field blank. <p>Field size: 20 characters Default: Blank</p> |
| | <i>4 of 7</i> |

Table 17. Filter Set Screen

| Field | Description |
|----------------------|---|
| ALRM SEVERITY | <p>Identifies the severity of the alarm filter.</p> <p>Users can select one or more of the days listed below.</p> <p>Note: The abbreviated titles are vertically stacked above the ALARM SEVERITY columns.</p> <p>MAJ = Major</p> <p>MIN = Minor</p> <p>WRN = Warning</p> <p>DGW = Downgraded Warning</p> <p>CLR = Cleared Alarm Notification</p> <p>RST = Restart Notification</p> <p>RES = Resolved Alarm</p> <p>Users can execute one of the options (a or b) below:</p> <p>a Type “x” in one or more of the fields to select the alarm severity criteria.</p> <p>b Leave the fields blank.</p> <p>Field size: 1</p> <p>Default: Blank</p> |
| | 5 of 7 |

Table 17. Filter Set Screen

| Field | Description |
|--------------------|---|
| DAY OF WEEK | <p>Identifies the day or days in the week to block alarm forwarding.</p> <p>Users can select one or more of the days listed below:</p> <ul style="list-style-type: none">M = MondayT = TuesdayW = WednesdayT = ThursdayF = FridayS = SaturdayS = Sunday <p>Users can execute one of the options (a or b) below:</p> <ul style="list-style-type: none">• Type “x” in one or more of the fields to select the day of week criteria.• Leave the fields blank. <p>Field size: 1</p> <p>Default: Blank</p> |
| | 6 of 7 |

Table 17. Filter Set Screen

| Field | Description |
|--------------------|--|
| TIME OF DAY | <p>Identifies the time window to block alarm forwarding.</p> <p>The Time of Day column contains the fields below:</p> <ul style="list-style-type: none">START field contains the time to begin alarm filteringEND field contains the time to stop alarm filtering <p>Users must use the 24-hour clock to enter start and end times</p> <p>Users can execute one of the options below:</p> <ul style="list-style-type: none">a Type the hours in <i>both</i> the START and END fields to select the time of day criteria.b Leave the fields blank. <p>Note: Start time must be earlier than end time. Wraparound time of day is not permitted. The solution is use of two entries (i.e. 5pm - 8am is not valid, instead use: one entry 00:00 - 07:59 and a second entry 17:01 - 23:59).</p> |
| | 7 of 7 |

Administer the Filter Sets

This section contains the procedures to administer filter sets on the Proxy Agent.

Users can access the FILTER SET screen from the PROXY ADMIN menu by executing the commands listed below:

- ***add filter-set*** to create a new filter set
- ***change filter-set*** to modify an existing filter set
- ***remove filter-set*** to delete a filter set
- ***display filter-set*** to view a filter set

On the FILTER SET screen, the user names each new filter set and enters the filters in the fields for the four types criteria:

- Pattern Matching Criteria (3 fields)
- Alarm Severity (7 fields)
- Day of Week (7 fields)
- Time of Day (2 fields)

Add a New Filter Set

Complete the procedure below to create a new filter set in the Proxy Agent.

Note: To use pattern files as part of the filtering criteria, only the system administrator should create the pattern files.

- 1 Access the PROXY ADMIN menu.
- 2 Stop the Proxy Agent, if running.
- 3 In the command line on the PROXY ADMIN menu,
 - Type **add filter-set**
 - Press **ENTER**

Result: The system displays a **blank** FILTER SET screen.

- 4 In the **FILTER SET** field, type the [name] of the new filter set.
- 5 In line 1 for the **PATTERN MATCHING CRITERIA** fields, complete the appropriate options below:

FILE/STRING: Execute **one** of the options (a or b) below:

- a Press **Ctrl-y** and select **file** or **string** from the list. Press **ENTER**.
- b Leave the field blank.

BOOL OPER: Execute one of the options (a or b) below:

- a Leave the field blank.
- b Press **Ctrl-Y** and select **not** from the list. Press **ENTER**.

FILE NAME OR CHARACTER STRING: Execute **one** of the options (a, b, or c) below based on your selection in the FILE/STRING field:

- a If you selected **file**, then press **Ctrl-Y** and select a **pattern file** from the list. Press **ENTER**.
 - b If you selected **string**, then type a **[character string]** in the field.
 - c If you left the field **blank**, then do not enter data in this field.
- 6 In line 1 for the **ALARM SEVERITY** filter, execute **one** of the options (a or b) below:
- a Type **X** in any or all of the fields below:
 - MAJ** = Major
 - MIN** = Minor
 - WRN** = Warning
 - DGW** = Downgraded Warning
 - CLR** = Cleared Alarm Notification
 - RST** = Restart Notification
 - RES** = Resolved Alarm
 - b Leave the fields blank.

- 7 In line 1 for the **DAY OF WEEK** filter, execute **one** of the options (a or b) below:
 - a Type **X** in any or all of the fields below:
 - M** = Monday
 - T** = Tuesday
 - W** = Wednesday
 - T** = Thursday
 - F** = Friday
 - S** = Saturday
 - S** = Sunday
 - b Leave the fields blank.
- 8 In line 1 for the **TIME OF DAY** filter, execute **one** of the options (a or b) below:
 - a Use the 24-hour clock to enter time in the both of the fields below:
 - START:** Type the [time] to begin the filter
 - END:** Type the [time] to stop the filter
 - b Leave the fields blank.
- 9 In lines 2 through 12, repeat steps [5](#) through [8](#) to add additional filters to the filter set, if appropriate.
- 10 Press **Ctrl-E** to submit the filter set.

Result: The system saves the new filter set and displays the PROXY ADMIN screen.
- 11 **New Installation.** Complete the procedure to ["Administer the Default Login" on page 235](#).

Change an Existing Filter Set

Complete the procedure below to change the criteria of an existing filter set.

- 1 Access the PROXY ADMIN menu.
- 2 Stop the Proxy Agent, if running.
- 3 In the command line on the PROXY ADMIN menu,
 - Type **change filter-set**
 - Press **ENTER**

Result: The system displays a **blank** FILTER SET screen.

- 4 In the **FILTER SET** field,
 - Press **Ctrl-Y** and select the [name] of the filter set from the list
 - Press **ENTER**

Result: The system displays the filter criteria for the selected filter-set name.

- 5 In line 1 for the **PATTERN MATCHING CRITERIA** fields, complete the appropriate options below:

FILE/STRING: Execute **one** of the options (a or b) below:

- a Press **Ctrl-Y** and select **file** or **string** from the list. Press **ENTER**.
- b Leave the field blank.

BOOL OPER: Execute one of the options (a or b) below:

- a Leave the field blank.
- b Press **Ctrl-Y** and select **not** from the list. Press **ENTER**.

Change an Existing Filter Set

FILE NAME OR CHARACTER STRING: Execute **one** of the options (a, b, or c) below based on your selection in the FILE/STRING field:

- a If you selected **file**, then press **Ctrl-Y** and select a **pattern file** from the list. Press **ENTER**.
 - b If you selected **string**, then type a **[character string]** in the field.
 - c If you left the field **blank**, then do not enter data in this field.
- 6 In line 1 for the **ALARM SEVERITY** filter, execute **one** of the options (a or b) below:
- a Type **X** in any or all of the fields below:
 - MAJ** = Major
 - MIN** = Minor
 - WRN** = Warning
 - DGW** = Downgraded Warning
 - CLR** = Cleared Alarm Notification
 - RST** = Restart Notification
 - RES** = Resolved Alarm
 - b Leave the fields blank.

Change an Existing Filter Set

- 7 In line 1 for the **DAY OF WEEK** filter, execute **one** of the options (a or b) below:
 - a Type **X** in any or all of the fields below:
 - M** = Monday
 - T** = Tuesday
 - W** = Wednesday
 - T** = Thursday
 - F** = Friday
 - S** = Saturday
 - S** = Sunday
 - b Leave the fields blank.
- 8 In line 1 for the **TIME OF DAY** filter, execute **one** of the options (a or b) below:
 - a Use the 24-hour clock to enter time in the both of the fields below:
 - START:** Type the [time] to begin the filter
 - END:** Type the [time] to stop the filter
 - b Leave the fields blank.
- 9 In lines 2 through 12, repeat steps [5](#) through [8](#) to add additional filters to the filter set, if appropriate.
- 10 Press **Ctrl-E** to submit the changes to the filter set.

Result: The system saves the changes and displays the PROXY ADMIN screen.
- 11 **New Installation.** Complete the procedure to ["Administer the Default Login" on page 235](#).

Display the Filter Set Screen

Complete the procedure below to display the FILTER SET screen. The **display** command only allows users to view the screen. Users cannot make changes to any of the fields.

Note: Users do not have to stop the Proxy Agent to execute the **display** command.

- 1 Access the PROXY ADMIN menu.
- 2 In the command line on the PROXY ADMIN menu,
 - Type **display filter-set**
 - Press **ENTER**

Result: The system displays a blank FILTER SET screen.

- 3 In the **FILTER SET** field,
 - Press **Ctrl-Y** and select the **[name]** of the filter set from the list
 - Press **ENTER**
 - View the criteria for the filter set.
- 4 Press **Ctrl-X** to exit the screen.

Result: The system closes FILTER SET screen and the displays the PROXY ADMIN screen.

Remove a Filter Set

The Proxy Agent allows users to delete all filter sets *except* the **default** filter set.

If users attempt to remove a filter set that has been assigned to one or more systems on the MANAGED NODES screen, then the Proxy Agent displays a window with a warning message. The message explains that if users remove the filter set, the Proxy Agent replaces this filter set with the **default** filter set for the affected the managed nodes.

If users do not want the **default** filter set to be assigned to individual managed nodes, then they can clear the default filter set in the *Filter Set Name* field on page A of the MANAGED NODES screen.

Procedure

Complete the procedure below to delete a filter set from the Proxy Agent.

- 1 Access the PROXY ADMIN menu.
- 2 Stop the Proxy Agent, if running.
- 3 In the command line on the PROXY ADMIN menu,
 - Type **remove filter-set**
 - Press **ENTER**

Result: The system displays a **blank** FILTER SET screen.

- 4 In the **FILTER SET** field,
 - Press **Ctrl-Y** and select the **[name]** of the filter set to be removed
 - Press **ENTER**

Result: The system displays the criteria for the selected filter set.

- 5 To remove the selected filter set, press **Ctrl-E**

Result: The system displays **one** of the options (a or b) below:

- a If the filter set is **not assigned** to any managed node, then the system deletes the filter set and displays the PROXY ADMIN screen.
Go to step [7](#) below.
- b If the filter set is **assigned** to one or more managed nodes, then system displays a window with a warning message. The message explains that the selected filter set will be replaced with the **default** filter set for the affected managed nodes. The message also contains a confirmation prompt: `Do you wish to continue?`
Go to step [6](#) to complete the procedure.

- 6 At the prompt, select **one** of the options (a or b) below:

- a To remove the filter set, select **Yes**.

Result: The system removes the selected filter set and replaces it with the **default** filter set for the affected managed nodes. Then, the system displays the PROXY ADMIN screen.

- b To cancel the remove request, select **No**.

Result: The system cancels the remove request and displays the PROXY ADMIN screen.

7 From the PROXY ADMIN menu, **start** the Proxy Agent.

8 Display the STATUS screen.

- Verify the Proxy Agent is active
- Press **Ctrl-X** to exit the screen

Result: The system closes the STATUS screen and displays the PROXY ADMIN menu.

10 Default Login Administration

Chapter Contents

- [*Introduction*](#) [*231*](#)
- [*Review of the Default Login Screen*](#) [*232*](#)
- [*Administer the Default Login*](#) [*235*](#)

Introduction

The DEFAULT LOGIN screen allows users to enter a system-wide **default** login and password or Access Security Gateway (ASG) key for DEFINITY systems. The Proxy Agent automatically displays the login and allows the user to modify the password on page F of the MANAGED NODES screen.

This feature reduces the time to administer large numbers of new DEFINITYs on the Proxy Agent. With this feature, users do **not** have to **manually** connect to the system on the COMMUNICATION MANAGER screen and save the login data.

Users can change the default login data for individual DEFINITYs on page F of the MANAGED NODES screen.



SECURITY ALERT:

When users enter the data in the Password/ASG Key field, the characters that display in the field are periods. The periods only display in the field during the time that the user is entering the password or ASG key. When users return to the screen later, the system displays only the data in the Login field. For security reasons, the Proxy Agent stores the password or ASG key but leaves the Password/ASG Key field blank.

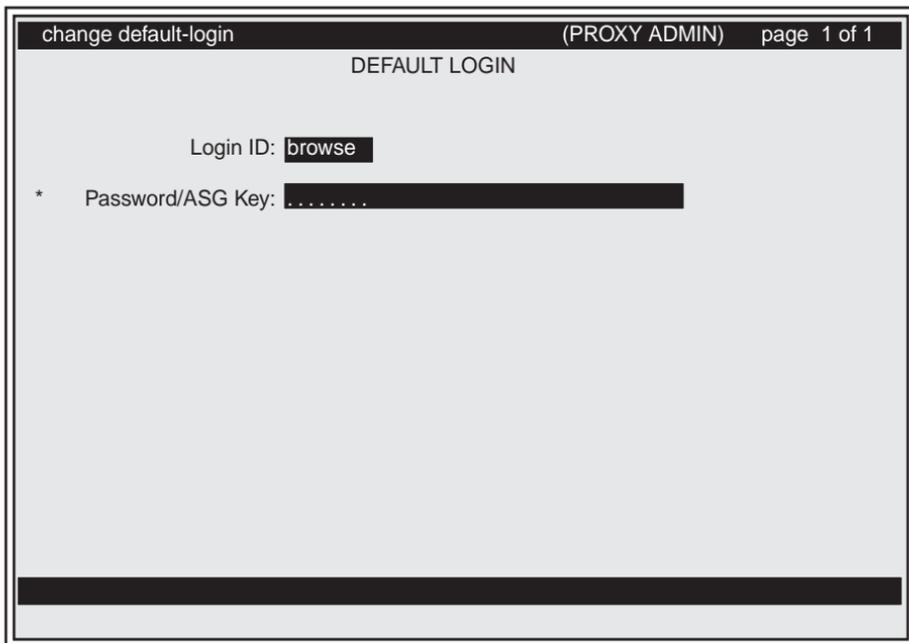
ASG login

For DEFINITY systems that are protected by the Access Security Gateway (ASG) system, the Proxy Agent uses the default ASG Key to automatically generate a response to a challenge when connecting automatically to a DEFINITY system.

The procedure to ["Connect to DEFINITY Systems with ASG" on page 287](#) contain the steps to **manually** enter the response and challenge to login to an ASG-protected DEFINITY system.

Review of the Default Login Screen

The figure below shows the fields on the DEFAULT LOGIN screen.



The screenshot displays a web interface for the DEFAULT LOGIN screen. At the top, a dark header bar contains the text "change default-login" on the left, "(PROXY ADMIN)" in the center, and "page 1 of 1" on the right. Below the header, the title "DEFAULT LOGIN" is centered. The main content area contains two input fields: "Login ID:" followed by a text box containing the word "browse", and "* Password/ASG Key:" followed by a password field with a series of dots. A dark horizontal bar is visible at the bottom of the screen area.

Figure 21. Default Login screen

Field descriptions

The table below contains the field descriptions for the DEFAULT LOGIN screen.

Table 18. Default Login Screen

| Field | Description |
|----------|--|
| Login ID | Identifies the login name for the DEFINITY system. The Proxy Agent displays the login ID on this screen and on page F of the MANAGED NODES screen when users administer new DEFINITYs on the Proxy Agent. Field size: 20 characters Validation: None Default: Blank |
| | <i>1 of 2</i> |

Table 18. Default Login Screen

| Field | Description |
|------------------|--|
| Password/ASG Key | <p>Displays periods while entering the password or ASG key in this field for the default password or ASG key to access all DEFINITYs administered on the Proxy Agent.</p> <p>The Proxy Agent saves the default password or ASG key but leaves the fields blank on the DEFAULT LOGIN screen. On page F of the MANAGED NODES screen, the Proxy Agent displays periods in the field.</p> <p>For DEFINITY systems that are protected by the Access Security Gateway (ASG) system, the Proxy Agent uses the default ASG Key to automatically generate a response to a challenge when connecting automatically to a DEFINITY system.</p> <p>Field size: 20 characters</p> <p>Validation: None</p> <p>Default: Blank</p> |

Administer the Default Login

This section contains the procedure to administer the **default** login and password or ASG key on the DEFAULT LOGIN screen.

Required materials

Users need the following information and materials:

- DEFINITY login name
- DEFINITY password or ASG secret key



SECURITY ALERT:

For security reasons, the PA001 form does NOT contain the password or ASG secret key for the DEFINITY systems.

Procedure

Complete the procedure below to administer the login data for new DEFINITY systems.

- 1 Access the PROXY ADMIN menu.
- 2 Stop the Proxy Agent, if running.
- 3 In the command line on the PROXY ADMIN menu,
 - Type **change default-login**
 - Press **ENTER**

Result: The system displays the DEFAULT LOGIN screen.

- 4 In the *Login ID* field, type [**default login**] **used** when adding new DEFINITY systems to the Managed Node screen.

- 5 In the *Password/ASG Key* field, type the [**password** or **ASG secret key**] used when adding new DEFINITY systems to the Managed Node screen.
- 6 Press **Ctrl-E** to submit the changes.

Result: The system saves the changes and displays the PROXY ADMIN menu.
- 7 **New Installation.** Complete the procedure to ["Administer the Managed Nodes" on page 265](#).
- 8 Restart the Proxy Agent.

11 Managed Nodes Administration

Chapter Contents

- [Introduction](#) [238](#)
- [Review of the Managed Nodes Screen](#) [241](#)
 - [Review of the Fields on Page A](#) [242](#)
 - [Review of the Fields on Page B](#) [250](#)
 - [Review of the Fields on Page C](#) [254](#)
 - [Review of the Fields on Pages D and E](#) [257](#)
 - [Review of the Fields on Page F](#) [262](#)
- [Administer the Managed Nodes](#) [265](#)

Introduction

The MANAGED NODES screen contain the individual values for each managed node administered on the Proxy Agent.

Users access the MANAGED NODES screen to execute the tasks listed below:

- Add new managed nodes to the Proxy Agent
- Change data for existing managed nodes
- Set the “forward alarms” option for managed nodes
- Select a filter set for individual managed nodes
- Select the Proxy Agent connection type and “start state” for individual managed nodes
- Change the submap type for individual managed nodes
- Change the system parameters of communication devices for individual managed nodes
- Reset the statistics counter for the Proxy Agent
- Select login ID and password/ASG key for new DEFINITYs administered on the Proxy Agent

Default parameters

The Proxy Agent automatically loads the system-wide, **default** parameters in the applications listed below:

- DEFAULT LOGIN
- FILTER SET
- ALARM PATH
- DEFAULT LOCATION
- CHANGE HARDWARE

When users add new managed nodes, the system displays the default parameters in the fields on the MANAGED NODES screens.

Users can change the parameters on the MANAGED NODES screen for individual managed nodes. The changes **override** the system default values only for the specific managed node.

SNMP polling

During the installation of the Proxy Agent, users have the option to enable or disable SNMP polling:

- If users **enable** SNMP polling, then the Proxy Agent only supports **150** managed nodes.
- If users **disable** SNMP polling, then the Proxy Agent can support up to **600** managed nodes.

To change these options **after** the Proxy Agent has been installed, users must reinstall the Proxy Agent software and change the options at the appropriate prompts in the installation script.

Static and Dynamic connections

The Proxy Agent 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 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 with dynamic connections.
- 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 with dynamic connections.

Lucent **recommends** 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.

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

Review of the Managed Nodes Screen

The MANAGED NODES screen is similar to a spreadsheet. The screen contains 40 pages, with 15 lines per page. The lines on each page are consecutively numbered 1 to 600 to identify each managed node that is connected to a specific Proxy Agent.

The example below shows the line numbers on the pages:

- Page 1 contains numbered lines 1 through 15
- Page 2 contains numbered lines 16 through 30, *etc.*

In addition, each of the 40 pages contains 5 subpages (a through e). The subpages contain fields to administer each managed node.

The example below shows the page number for subpages (1 through 40):

- Page 1 subpages are numbered: 1a/40, 1b/40, 1c/40, 1d/40, 1e/40
- Page 2 subpages are numbered: 2a/40, 2b/40, 2c/40, 2d/40, 2e/40, *etc.*

Review of the Fields on Page A

The figure below shows page **A** of the MANAGED NODES screen. Page **A** contains the basic fields to administer managed nodes and the Proxy Agent.

| change managed-nodes (PROXY ADMIN) page 1a/40 | | | | | | | | | |
|---|-----------|-----------|----------------|-----------------------|--------------------------|------------|-------------|-------------------------|-------------|
| MANAGED NODES | | | | | | | | | |
| | NODE NAME | NODE TYPE | FORWARD ALARMS | PRODUCT ID FOR ALARMS | FILTER SET NAME (IF REQ) | START TYPE | START STATE | DYNAMIC TIMEOUT MINUTES | RESET COUNT |
| 1: | ecs1 | ECS | n | 1111111111 | default | static | init | | n |
| 2: | g3 | G3 | y | 1222222222 | fset1 | dynamic | init | 60 | n |
| 3: | mcu | MCU | y | 1333333333 | | static | off | | n |
| 4: | daudix1 | DAUDIX | y | 2211111111 | default | | | | |
| 5: | iaudix1 | IAUDIX | y | 2222222222 | default | | | | |
| 6: | intrchg1 | INTRCHG | y | 2233333333 | default | | | | |
| 7: | cms1 | CMS | y | 2099999999 | default | | | | |
| 8: | conv1 | CNVRST | y | 2188888888 | default | | | | |
| 9: | | | | | | | | | |
| 10: | | | | | | | | | |
| 11: | | | | | | | | | |
| 12: | | | | | | | | | |
| 13: | | | | | | | | | |
| 14: | | | | | | | | | |
| 15: | | | | | | | | | |

sdnmmgna LJK 092299

Figure 22. Page A of the MANAGED NODES screen

Page A field descriptions

The table below contains the field descriptions for page **A** of the MANAGED NODES screen.

Table 19. Page A of the Managed Nodes screen

| Field | Description |
|-----------|---|
| NODE NAME | <p>Identifies the name of the system that users administer on Proxy Agent as a managed node. The node name occupies the same line number on each of the five (5) lettered pages.</p> <p>The node name on the Proxy Agent must match the managed node name on the Network Management System (NMS).</p> <p>Users can change the node name without having to re-enter data in the other fields.</p> <p>If users delete the NODE NAME field, the system automatically clears the data from all fields in the numbered row on each of the 5 lettered subpages.</p> <p>Field size: 9 characters</p> <p>Required field.</p> |
| | 1 of 7 |

Table 19. Page A of the Managed Nodes screen

| Field | Description |
|-----------|--|
| NODE TYPE | <p>Identifies the type of managed node that is associated with a specific Proxy Agent.</p> <p>The HELP list (Ctrl-Y) contains the valid options below:</p> <p>ECS (default) = DEFINITY release 5 and later</p> <p>G3 = DEFINITY G3V4</p> <p>MCU = Multipoint Conferencing Unit</p> <p>* DAUDIX = DEFINITY AUDIX</p> <p>* IAUDIX = INTUITY AUDIX</p> <p>* INTRCHG = INTUITY Interchange</p> <p>* CMS = Call Management System</p> <p>* CNVRST = Conversant</p> <p>* If users select one of these systems, the screen does not display the following fields: Reset Count; Start State; Start Type; or Dynamic Timeout.</p> |
| | <i>2 of 7</i> |

Table 19. Page A of the Managed Nodes screen

| Field | Description |
|-----------------------|--|
| FORWARD ALARMS | <p>Indicates the alarm forwarding feature is on or off for the individual managed nodes.</p> <p>The HELP list (Ctrl-Y) contains the valid options below:</p> <p>Y = (yes) alarm forwarding is on</p> <p>N = (no) alarm forwarding is off</p> <p>The default values differ for type of managed nodes:</p> <p>Y = default for G3, MCU, DAUDIX, IAUDIX, INTRCHG, CMS, and CNVRSNT</p> <p>N = default for ECS</p> <p>Note: If users turn on the FORWARD ALARM option, they should verify that the ALARM PATH screen is administered to receive alarms from managed nodes and to forward alarms to INADS. Forwarding is subject to filtering as defined in filter set field.</p> |
| PRODUCT ID FOR ALARMS | <p>Identifies the product identification (ID) number of the managed node.</p> <p>Size: 10 characters</p> <p>Required field.</p> |
| | 3 of 7 |

Table 19. Page A of the Managed Nodes screen

| Field | Description |
|-----------------------------|--|
| FILTER SET NAME (IF REQ) | <p>Identifies the name of the filter set that the Proxy Agent applies to alarms received from the managed node. The Proxy Agent assigns the default filter set to new managed nodes.</p> <p>To activate the filter set features, users must administer the screens described below:</p> <ul style="list-style-type: none"> • Users must administer the alarm source and alarm destination fields on the ALARM PATH screen. Refer to "Administer the Alarm Path" on page 199. • Users can add, change, or remove filters on the FILTER SET screen. For new installations, the default filter set is blank. Users can add filtering criteria to the default filter set or leave it blank. Refer to "Administer the Filter Sets" on page 219. • Users must also select "Y" (yes) in the FORWARD ALARM field on the page A of the MANAGED NODES screen. Refer to procedures to "Administer the Managed Nodes" on page 265. <p>Size: 10 characters</p> <p>Default: "default" is the name of the default filter set.</p> |
| | 4 of 7 |

Table 19. Page A of the Managed Nodes screen

| Field | Description |
|---------------|--|
| START TYPE | <p>Identifies the type of connection between the Proxy Agent and a managed node.</p> <p>The HELP list (Ctrl-Y) contains the valid options below:</p> <ul style="list-style-type: none">static (default)dynamic (see DYNAMIC TIMEOUT field) <p>A static connection maintains a continuous link for 24 hours per day, 7 days per week. Select static connections to monitor critical managed nodes.</p> <p>A dynamic connection maintains a temporary link with the managed node on an as-needed basis. Select dynamic connections to monitor less critical managed nodes.</p> <p>A dynamic connection stays up as long as the Proxy Agent is actively processing SNMP requests and then times-out after a specified period.</p> <p>The Network Management System (NMS) does not poll for health data if a dynamic connection is assigned to a managed node.</p> |
| | 5 of 7 |

Table 19. Page A of the Managed Nodes screen

| Field | Description |
|-------------|--|
| START STATE | <p data-bbox="479 220 1184 277">Identifies the connection state of the Proxy Agent at the time the user starts the Proxy Agent.</p> <p data-bbox="479 296 1184 322">The HELP list (Ctrl-Y) contains the valid options below:</p> <ul data-bbox="503 337 1184 581" style="list-style-type: none"><li data-bbox="503 337 1184 508">• init = initiates the connection types as defined below:<ul data-bbox="543 379 1184 508" style="list-style-type: none"><li data-bbox="543 379 1184 405">– Starts the static connection to the managed node<li data-bbox="543 420 1184 508">– Places the dynamic connection in an idle state to be initiated by minor or major alarms from the managed node<li data-bbox="503 524 1184 581">• off = (default) indicates that the connections are turned off <p data-bbox="479 607 1184 695">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.</p> <p data-bbox="479 721 1184 746">The valid start states are:</p> <ul data-bbox="503 762 1184 829" style="list-style-type: none"><li data-bbox="503 762 1184 788">• static init or static off<li data-bbox="503 803 1184 829">• dynamic init or dynamic off |
| | 6 of 7 |

Table 19. Page A of the Managed Nodes screen

| Field | Description |
|--------------------|---|
| DYNAMIC TIMEOUT | <p>Identifies the number of minutes that a dynamic connection can be inactive before the Proxy Agent drops the connection to a managed node.</p> <p>The HELP list (Ctrl-Y) contains the valid minute below:</p> <p>5</p> <p>15</p> <p>30</p> <p>60 (default)</p> <p>120</p> |
| RESET COUNT | <p>Allows users to reset the status counters to zero.</p> <p>While the Proxy Agent is running, the counters track the number of attempts, connections, requests, responses, and errors that occur.</p> <p>The Proxy Agent updates the numbers from the counters on the STATUS screen.</p> <p>The HELP list (Ctrl-Y) contains the valid options below:</p> <p>N = no (default) -- do not reset counters</p> <p>Y = yes to reset the status counters to zero</p> |
| | <i>7 of 7</i> |

Review of the Fields on Page B

The figure below shows page **B** of the MANAGED NODES screen. Page **B** contains the fields to administer the transmission options for the communication devices that connect the Proxy Agent to each managed node.

Note: It is recommended that the values of these fields remain at their default values, unless a Lucent representative instructs you to change their value(s).

| NODE NAME | SPEED | STOP BITS | FLOW CNTRL | PARITY | CHAR SIZE |
|-------------|-------|-----------|------------|--------|-----------|
| 1:*ecs1 | >9600 | 1 | n | none | 8 |
| 2: g3 | 9600 | 1 | n | none | 8 |
| 3: mcu | 9600 | 1 | n | none | 8 |
| 4: daudix1 | 9600 | 1 | n | none | 8 |
| 5: iaudix1 | 9600 | 1 | n | none | 8 |
| 6: intrchg1 | 9600 | 1 | n | none | 8 |
| 7: cms1 | | | | | |
| 8: conv1 | | | | | |
| 9: | | | | | |
| 10: | | | | | |
| 11: | | | | | |
| 12: | | | | | |
| 13: | | | | | |
| 14: | | | | | |
| 15: | | | | | |

sdnrmgnb LJK 092299

Figure 23. Page B of the MANAGED NODES screen

Page B field descriptions

The table below contains the field descriptions for page **B** of the MANAGED NODES screen.

Table 20. Page B of the Managed Nodes screen

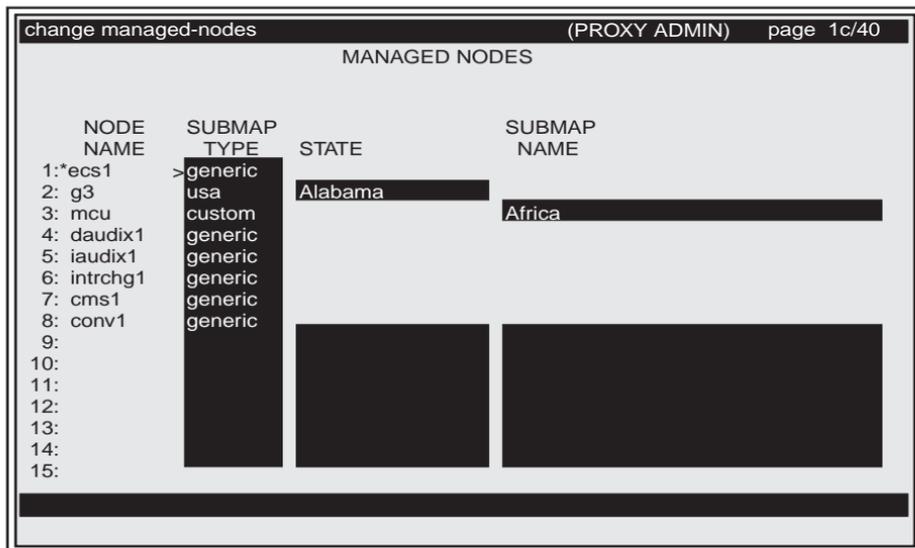
| Field | Description |
|-----------|---|
| NODE NAME | Identifies the name of the managed node. The node name occupies the same line number on each of the lettered pages. |
| SPEED | Identifies the baud rate for the communication device that connects the Proxy Agent to each managed node. The HELP list (Ctrl-Y) contains the valid options below: 9600 (default) 4800 2400 1200 |
| STOP BITS | Identifies the stop bit setting on the communication device. The HELP list (Ctrl-Y) contains the valid options below: 1 (default) 2 |
| | <i>1 of 2</i> |

Table 20. Page B of the Managed Nodes screen

| Field | Description |
|---------------|--|
| FLOW CNTRL | Identifies the flow control setting on the communication device. The HELP list (Ctrl-Y) contains the valid options below: n (no) (default) -- Turn-off y (yes) -- Turn-on |
| PARITY | Identifies the parity setting on the communication device. The HELP list (Ctrl-Y) contains the valid options below: none (default) odd even |
| CHAR SIZE | Identifies the character size setting on the communication device. The HELP list (Ctrl-Y) contains the valid options below: 8 (default) 7 |
| | <i>2 of 2</i> |

Review of the Fields on Page C

The figure below shows page **C** of the **MANAGED NODES** screen. Page **C** contains the submap type and location of the *individual* managed nodes.



The screenshot shows a terminal window titled "change managed-nodes (PROXY ADMIN) page 1c/40". The main heading is "MANAGED NODES". Below it is a table with four columns: "NODE NAME", "SUBMAP TYPE", "STATE", and "SUBMAP NAME". The table lists 15 nodes. Node 1 is highlighted with a greater-than sign (>). The "STATE" and "SUBMAP NAME" columns for nodes 2, 4, and 8 are redacted with black boxes.

| NODE NAME | SUBMAP TYPE | STATE | SUBMAP NAME |
|-------------|-------------|---------|-------------|
| 1:*ecs1 | >generic | | |
| 2: g3 | usa | Alabama | |
| 3: mcu | custom | | Africa |
| 4: daudix1 | generic | | |
| 5: iaudix1 | generic | | |
| 6: intrchg1 | generic | | |
| 7: cms1 | generic | | |
| 8: conv1 | generic | | |
| 9: | | | |
| 10: | | | |
| 11: | | | |
| 12: | | | |
| 13: | | | |
| 14: | | | |
| 15: | | | |

sdnmmgnc LJK 092299

Figure 24. Page **C** of the **MANAGED NODES** screen

Page C field descriptions

The table below contains the field descriptions for Page **C** of the MANAGED NODES screen.

Table 21. Page C of the Managed Nodes screen

| Field | Description |
|-------------|--|
| NODE NAME | Identifies the name of the managed node. The node name occupies the same line number on each of the lettered pages. |
| SUBMAP TYPE | Identifies the type of location map to display on the Network Management System (NMS). The HELP list (Ctrl-Y) contains the valid options below: generic (default) usa (see associated STATE field) custom (see associated SUBMAP NAME field) Field size: 7 characters |
| | <i>1 of 2</i> |

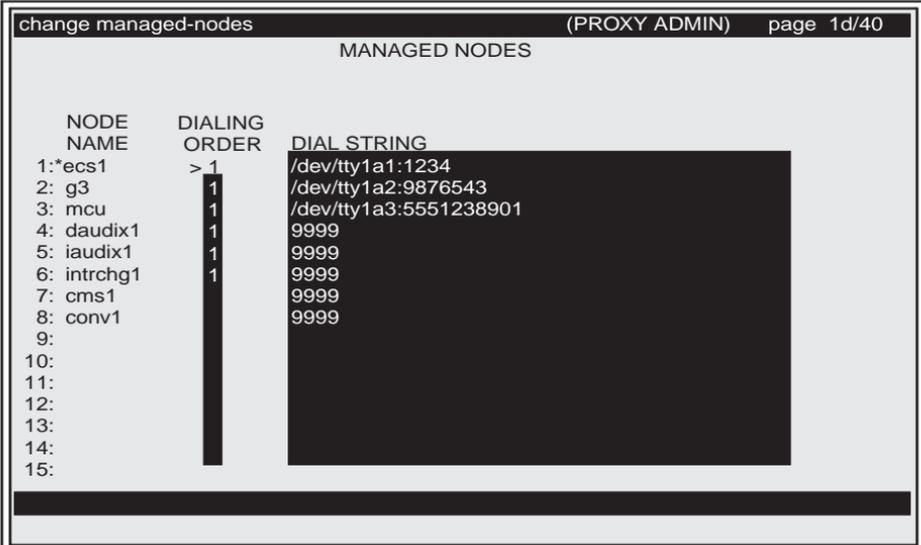
Table 21. Page C of the Managed Nodes screen

| Field | Description |
|-------------|--|
| STATE | <p>Identifies the name of the state where a managed node is located on the USA map.</p> <p>The STATE field only displays if the user selects the usa option in the SUBMAP TYPE field.</p> <p>The HELP list (Ctrl-Y) contains the valid options for this field which include all 50 states.</p> <p>The default option is set on the DEFAULT LOCATION screen. Users can change the <i>State</i> name for individual managed nodes</p> <p>Field size: 14 characters</p> |
| SUBMAP NAME | <p>Identifies the name of the custom location submap for individual managed nodes.</p> <p>The SUBMAP NAME field only displays if the user selects the custom option in the SUBMAP TYPE field.</p> <p>Field size: 40 characters. The system accepts any name that users type the in the SUBMAP NAME field.</p> |
| | 2 of 2 |

Review of the Fields on Pages D and E

Pages **D** and **E** of the MANAGED NODES screen contain the same fields to administer the dialing orders and dial strings that the Proxy Agent uses to connect with each managed node.

The figure below shows page **D** of the MANAGED NODES screen.



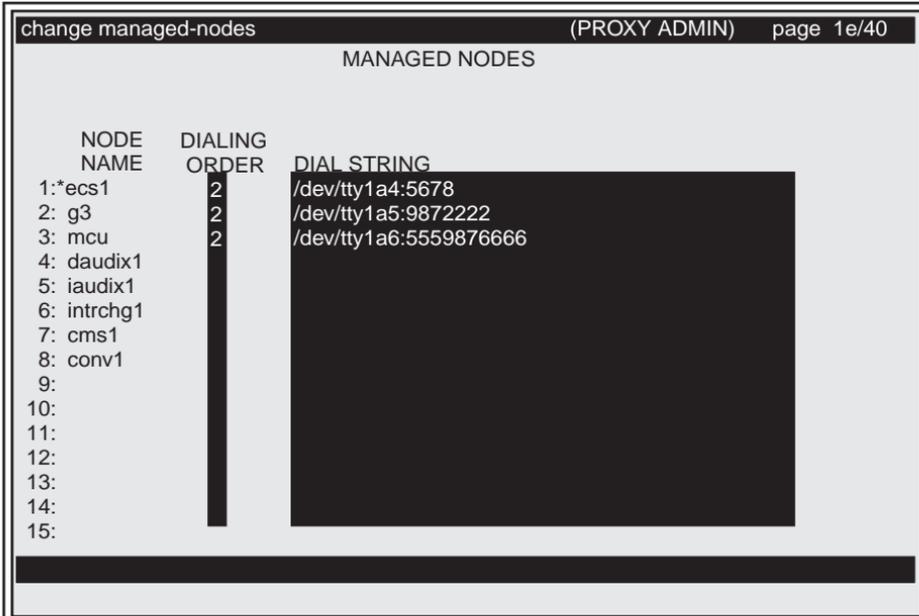
The screenshot shows a terminal window titled "change managed-nodes (PROXY ADMIN) page 1d/40". The main heading is "MANAGED NODES". Below it is a table with three columns: "NODE NAME", "DIALING ORDER", and "DIAL STRING". The table contains 15 rows of data. The first row is highlighted with a black background. The "DIALING ORDER" column has a vertical bar to its right, and the first row has a ">" symbol next to its value "1".

| NODE NAME | DIALING ORDER | DIAL STRING |
|-------------|---------------|------------------------|
| 1:*ecs1 | > 1 | /dev/tty1a1:1234 |
| 2: g3 | 1 | /dev/tty1a2:9876543 |
| 3: mcu | 1 | /dev/tty1a3:5551238901 |
| 4: daudix1 | 1 | 9999 |
| 5: iaudix1 | 1 | 9999 |
| 6: intrchg1 | 1 | 9999 |
| 7: cms1 | 1 | 9999 |
| 8: conv1 | 1 | 9999 |
| 9: | | |
| 10: | | |
| 11: | | |
| 12: | | |
| 13: | | |
| 14: | | |
| 15: | | |

sdnmmgnd LJK 092399

Figure 25. Page **D** of the MANAGED NODES screen

The figure below shows page **E** of the MANAGED NODES screen.



The screenshot shows a terminal window titled "change managed-nodes (PROXY ADMIN) page 1e/40". The main heading is "MANAGED NODES". Below it is a table with three columns: "NODE NAME", "DIALING ORDER", and "DIAL STRING". The table contains three rows of data, with the rest of the rows (4-15) being obscured by a black redaction box.

| NODE NAME | DIALING ORDER | DIAL STRING |
|-------------|---------------|------------------------|
| 1:*ecs1 | 2 | /dev/tty1a4:5678 |
| 2: g3 | 2 | /dev/tty1a5:9872222 |
| 3: mcu | 2 | /dev/tty1a6:5559876666 |
| 4: daudix1 | | |
| 5: iaudix1 | | |
| 6: intrchg1 | | |
| 7: cms1 | | |
| 8: conv1 | | |
| 9: | | |
| 10: | | |
| 11: | | |
| 12: | | |
| 13: | | |
| 14: | | |
| 15: | | |

sdnmmgne LJK 092399

Figure 26. Page **E** of the MANAGED NODES screen

**Pages D and E
field
descriptions**

The table below contains the field description for pages **D** and **E** of the MANAGED NODES screen.

Table 22. Pages D and E of the Managed Nodes screen

| Field | Description |
|--------------|---|
| NODE NAME | Identifies the name of the managed node. The node name occupies the same line number on each of the lettered pages. |
| | <i>1 of 3</i> |

Table 22. Pages D and E of the Managed Nodes screen

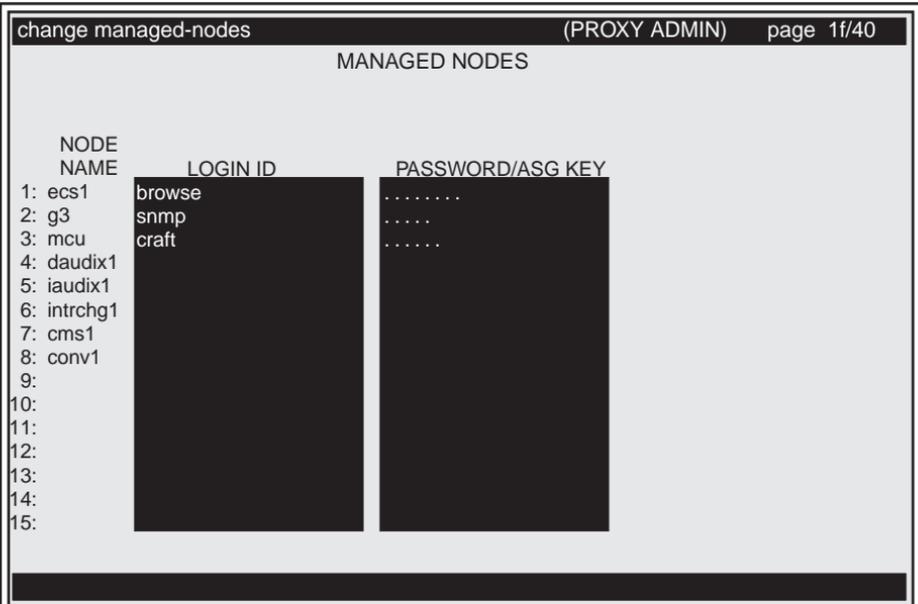
| Field | Description |
|---------------|---|
| DIALING ORDER | <p>Specifies which dial string the Proxy Agent will use to connect to a managed node.</p> <p>The Proxy Agent will always use the number 1 dial string first. If the number 1 dial string is busy or out-of-order, then the Proxy Agent will use the number 2 dial string, <i>if</i> number 2 exists.</p> <p>The HELP list (Ctrl-y) contains the valid options below:</p> <ul style="list-style-type: none">1 -- required field (default)2 -- optional field <p>Generally, users designate page D as the number 1 dialing order and page E as the number 2 dialing order.</p> <p>If users enter two dial strings, they can change the dialing orders between the subpages D and E. One of the dial strings <i>must</i> contain the number 1 in the DIALING ORDER column.</p> |
| | <i>2 of 3</i> |

Table 22. Pages D and E of the Managed Nodes screen

| Field | Description |
|-------------|---|
| DIAL STRING | <p>Specifies the dial string that the Proxy Agent uses to connect to a managed node.</p> <p>A dial string can be an extension number, the telephone number, or the area code and telephone number.</p> <p>The following are examples of valid dial strings:</p> <ul style="list-style-type: none">• Dial string can be a combination of the area code, phone number, and extension. Examples: 3035551212; 5551212; or 1212• Device path (/dev/tty001)• Device path and dial string (dev/tty001:3035551212) <p>Required field for the number 1 dialing order for the primary dial string.</p> <p>Required field for the number 2 dialing order only if users entered a 2 in the DIALING ORDER field for the secondary dial string.</p> |
| | 3 of 3 |

Review of the Fields on Page F

The figure below shows page **F** of the MANAGED NODES screen. Page **F** contains the **default** login ID for DEFINITY systems from the DEFAULT LOGIN screen. The system does not display the password or ASG key entered on the DEFAULT LOGIN screen.



The screenshot shows a terminal window titled "change managed-nodes" with "(PROXY ADMIN)" and "page 1f/40" in the top right. The main title is "MANAGED NODES". Below it is a table with three columns: "NODE NAME", "LOGIN ID", and "PASSWORD/ASG KEY". The table lists nodes 1 through 15. Nodes 1-3 have visible login IDs: "browse", "snmp", and "craft". Nodes 1-3 also have visible passwords: ".....", ".....", and ".....". Nodes 4-15 have no visible data.

| NODE NAME | LOGIN ID | PASSWORD/ASG KEY |
|-------------|----------|------------------|
| 1: ecs1 | browse | |
| 2: g3 | snmp | |
| 3: mcu | craft | |
| 4: daudix1 | | |
| 5: iaudix1 | | |
| 6: intrchg1 | | |
| 7: cms1 | | |
| 8: conv1 | | |
| 9: | | |
| 10: | | |
| 11: | | |
| 12: | | |
| 13: | | |
| 14: | | |
| 15: | | |

Figure 27. Page F of Managed Nodes screen

Page F field descriptions

The table below contains the field descriptions for Page F of the MANAGED NODES screen.

Table 23. Page F of the Managed Nodes screen

| Field | Description |
|-----------|---|
| NODE NAME | Identifies the name of the managed node. The node name occupies the same line number on each of the lettered pages. |
| Login ID | <p>Identifies the login name for the DEFINITY system.</p> <p>The Proxy Agent displays the login ID data for DEFINITY systems.</p> <p>The feature reduces the time to administer large numbers of new DEFINITYs on the Proxy Agent. With this feature, users do not have to manually connect to the system on the COMMUNICATION MANAGER screen and save the login data.</p> <p>To override the default login ID from the DEFAULT LOGIN screen, users can change the login ID for individual DEFINITY systems on page F.</p> <p>Field size: 20 characters</p> <p>Validation: None</p> <p>Default: Blank</p> |
| | 1 of 2 |

Table 23. Page F of the Managed Nodes screen

| Field | Description |
|------------------|--|
| Password/ASG Key | <p>Displays periods in field as the password or ASG key is entered.</p> <p>The Proxy Agent saves the default password or ASG key that users administered on the DEFAULT LOGIN screen. For security reasons, the Proxy Agent displays periods in the field on the MANAGED NODES screen.</p> <p>For DEFINITY systems that are protected by the Access Security Gateway (ASG) system, the Proxy Agent automatically generates the <i>response</i> to the <i>challenge</i> when users administer new DEFINITYs on the Proxy Agent.</p> <p>To override the default password or ASG Key from the DEFAULT LOGIN screen, users can change the password or ASG secret key for individual DEFINITY systems on page F.</p> <p>Field size: 20 characters</p> <p>Validation: None</p> <p>Default: Blank</p> |
| | 2 of 2 |

Administer the Managed Nodes

The MANAGED NODES screen provides an overview of the configuration for each managed node that users administer on the Proxy Agent.

This section contains the procedures to:

- Add new managed nodes to the Proxy Agent and save the login data
- Change data for individual managed nodes
- Delete existing managed nodes

Procedure

The procedures below contain the steps to add or change managed nodes and one step to delete a managed node.

The examples in the procedure below show **default** values in the fields.

Note: To complete the fields, refer to the **Managed Nodes** section of the PA001 form.

- 1 Access the PROXY ADMIN menu.
- 2 Stop the Proxy Agent, if running.
- 3 In the command line on the PROXY ADMIN menu,
 - Type **change managed-nodes**
 - Press **ENTER**

Result: The system displays the page **A** of the MANAGED NODES screen.

| change managed-nodes (PROXY ADMIN) page 1a/40 | | | | | | | | | |
|---|-----------|-----------|----------------|-----------------------|--------------------------|------------|-------------|-------------------------|-------------|
| MANAGED NODES | | | | | | | | | |
| | NODE NAME | NODE TYPE | FORWARD ALARMS | PRODUCT ID FOR ALARMS | FILTER SET NAME (IF REQ) | START TYPE | START STATE | DYNAMIC TIMEOUT MINUTES | RESET COUNT |
| 1: | ecs1 | ECS | n | 1111111111 | default | static | init | | n |
| 2: | g3 | G3 | y | 1222222222 | fset1 | dynamic | init | 60 | n |
| 3: | mcu | MCU | y | 1333333333 | | static | off | | n |
| 4: | daudix1 | DAUDIX | y | 2211111111 | default | | | | |
| 5: | iaudix1 | IAUDIX | y | 2222222222 | default | | | | |
| 6: | intrchg1 | INTRCHG | y | 2233333333 | default | | | | |
| 7: | cms1 | CMS | y | 2099999999 | default | | | | |
| 8: | conv1 | CNVRSENT | y | 2188888888 | default | | | | |
| 9: | | | | | | | | | |
| 10: | | | | | | | | | |
| 11: | | | | | | | | | |
| 12: | | | | | | | | | |
| 13: | | | | | | | | | |
| 14: | | | | | | | | | |
| 15: | | | | | | | | | |

- 4 On page **A**, access the appropriate page number (1 through 40). In the **NODE NAME** column, execute one of the options below:
 - To **add** a new managed node: Go to the next blank line and follow the steps below.
 - To **change** a managed node: Go to the line number for that managed node. Then, go to the fields to be changed and make the appropriate changes on each subpage.
 - To **delete** an existing managed node: Go to the line number for that managed node. Press the **SPACE BAR**. The system deletes the managed node and clears the fields on all subpages for that line.
- 5 On page **A**, go to the first **blank** line and complete the fields below to add a new managed node. The fields contain the default settings.

NODE NAME: Type the [**system name**]

NODE TYPE: **ECS** (default).

FORWARD ALARMS: **n** (default for ECS); **y** (default for all other node types)

PRODUCT ID FOR ALARMS: Type the [**product/alarm ID**] for the node type

FILTER SET NAME: **default** -- Execute one of the options (a or b) below:

- a To select a different filter name, press **Ctrl-Y** to display the options list; highlight a filter name; and press **ENTER**
- b To clear the field of any filter name, press the **SPACE BAR**

START TYPE: **static** (default)

START STATE: **off** (default) -- Press **Ctrl-y** and select **init** (initiate)

DYNAMIC TIMEOUT MINUTES: **60** (default) -- Press **Ctrl-y** to select an option from the list, if appropriate. If you select **static**, the field is blanked out.

RESET COUNT: **n** (default) -- Type **y** to reset, if necessary

Press **ENTER** to display page B.

Result: The system displays page **B** as shown in the example below.

| change managed-nodes | | (PROXY ADMIN) | | page 1b/40 | |
|----------------------|-------|---------------|------------|------------|-----------|
| MANAGED NODES | | | | | |
| NODE NAME | SPEED | STOP BITS | FLOW CNTRL | PARITY | CHAR SIZE |
| 1:*ecs1 | >9600 | 1 | n | none | 8 |
| 2: g3 | 9600 | 1 | n | none | 8 |
| 3: mcu | 9600 | 1 | n | none | 8 |
| 4: daudix1 | 9600 | 1 | n | none | 8 |
| 5: iaudix1 | 9600 | 1 | n | none | 8 |
| 6: intrchg1 | 9600 | 1 | n | none | 8 |
| 7: cms1 | | | | | |
| 8: conv1 | | | | | |
| 9: | | | | | |
| 10: | | | | | |
| 11: | | | | | |
| 12: | | | | | |
| 13: | | | | | |
| 14: | | | | | |

- 6 On page **B**, change the values of the communication devices for individual managed nodes, *if* necessary.

NODE NAME: (carried over to each page)

SPEED: **9600** (check the PA001 form)

STOP BITS: **1**

FLOW CNTRL: **n**

PARITY: **none**

CHAR SIZE: **8**

Press **ENTER** to display page **C**.

Result: The system displays page **C** of the Managed Nodes screen.

| change managed-nodes | | (PROXY ADMIN) page 1c/40 | |
|----------------------|-------------|--------------------------|-------------|
| MANAGED NODES | | | |
| NODE NAME | SUBMAP TYPE | STATE | SUBMAP NAME |
| 1:*ecs1 | >generic | | |
| 2: g3 | usa | Alabama | |
| 3: mcsu | custom | | Africa |
| 4: daudix1 | generic | | |
| 5: iaudix1 | generic | | |
| 6: intrchg1 | generic | | |
| 7: cms1 | generic | | |
| 8: conv1 | generic | | |
| 9: | | | |
| 10: | | | |
| 11: | | | |
| 12: | | | |
| 13: | | | |
| 14: | | | |
| 15: | | | |

7 On page **C**, change the location for each managed node, where appropriate.

Generic location

SUBMAP TYPE: **generic** (default)

USA location

SUBMAP TYPE: **usa**

STATE: **Alabama** (default) Press **Ctrl-y** to select a state from the list

Custom location

SUBMAP TYPE: **custom**

SUBMAP NAME: Type the [**location name**]

Press **ENTER** to display page D.

Result: The system displays page **D** as shown in the example below.

```
change managed-nodes (PROXY ADMIN) page 1d/40
MANAGED NODES

NODE   DIALING
NAME   ORDER  DIAL_STRING
1:*ecs1 > 1    /dev/tty1a1:1234
2: g3   1      /dev/tty1a2:9876543
3: mcu  1      /dev/tty1a3:5551238901
4: daudix1 1      9999
5: iaudix1 1      9999
6: intrchg1 1      9999
7: cms1   1      9999
8: conv1  1      9999
9:
10:
11:
12:
13:
14:
15:
```

- 8 On page **D**, complete the fields for the **primary** communication device. The Proxy Agent uses this device to connect to the managed node.

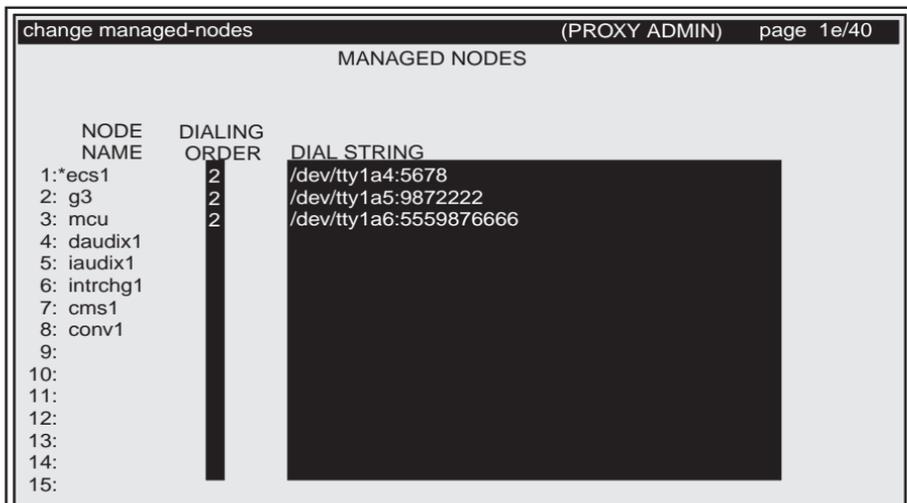
NODE NAME: (carried over to each page)

DIALING ORDER: **1**

DIAL STRING: Type the [dial string] for the **primary** device. Go to the PA001 form, and refer to the Dial String 1 field on the *Managed Nodes* section.

Press **ENTER** to display page E.

Result: The system displays page **E** as shown in the example below.



The screenshot shows a terminal window titled "change managed-nodes" with "(PROXY ADMIN) page 1e/40" in the top right. The main content is a table titled "MANAGED NODES". The table has three columns: "NODE NAME", "DIALING ORDER", and "DIAL STRING". The data rows are as follows:

| NODE NAME | DIALING ORDER | DIAL STRING |
|-------------|---------------|------------------------|
| 1: ecs1 | 2 | /dev/tty1a4:5678 |
| 2: g3 | 2 | /dev/tty1a5:9872222 |
| 3: mcu | 2 | /dev/tty1a6:5559876666 |
| 4: daudix1 | | |
| 5: iaudix1 | | |
| 6: intrchg1 | | |
| 7: cms1 | | |
| 8: conv1 | | |
| 9: | | |
| 10: | | |
| 11: | | |
| 12: | | |
| 13: | | |
| 14: | | |
| 15: | | |

9 OPTIONAL. On page **E**, complete the fields for a **secondary** communication device. The Proxy Agent uses this device if the first device is not available.

NODE NAME: (carried over to each page)

DIALING ORDER: Type **2** in the field

DIAL STRING: Type the [dial string] for the **secondary** device. Go to the PA001 form, and refer to the Optional. Dial String 2 field on the *Managed Nodes* section.

Press **Ctrl-N** to display page F.

Result: The system displays page F as shown in the example below.

| change managed-nodes | | (PROXY ADMIN) | page 1f/40 |
|----------------------|----------|------------------|------------|
| MANAGED NODES | | | |
| NODE NAME | LOGIN ID | PASSWORD/ASG KEY | |
| 1: ecs1 | browse | | |
| 2: g3 | snmp | | |
| 3: mcu | craft | | |
| 4: daudix1 | | | |
| 5: iaudix1 | | | |
| 6: intrchg1 | | | |
| 7: cms1 | | | |
| 8: conv1 | | | |
| 9: | | | |
| 10: | | | |
| 11: | | | |
| 12: | | | |
| 13: | | | |
| 14: | | | |
| 15: | | | |

- 10 The fields on page F contain the default login data from the DEFAULT LOGIN screen for new DEFINITY systems, as show in the example below.

NODE NAME: (carried over to each page)

LOGIN ID: [**system name**] for the new DEFINITY system

PASSWORD/ASG KEY: [.....] periods are displayed as the password or ASG secret key is entered.

- 11 Press **Ctrl-E** to submit the data.

Result: The system saves the data and displays the PROXY ADMIN menu.

- 12 From the PROXY ADMIN menu, **start** the Proxy Agent.

- 13 Display the STATUS screen.

- Verify the Proxy Agent is active
- Press **Ctrl-X** to exit the screen

Result: The system closes the STATUS screen. Then, displays the PROXY ADMIN menu.

12 Communication Application

Chapter Contents

- [Introduction](#) [275](#)
- [Review of the Communication Manager Screen](#) [278](#)
- [Connect to Managed Nodes](#) [281](#)
 - [Connect to Managed Nodes](#) [281](#)
 - [Connect to DEFINITY Systems with ASG](#) [287](#)
- [Disconnect from Managed Nodes](#) [296](#)

Introduction

The purpose of the **Communication** application is to execute the specific tasks listed below:

- To troubleshoot connections between the Proxy Agent and managed nodes.
- To connect to one or two managed nodes **before** starting an administration session from the EMULATION screen.

In all other instances, users access the MANAGED NODES screen to initiate the Proxy Agent connection with individual managed nodes.

Connection procedures

This chapter contains two types of connection procedures to manually log in to the managed nodes.

- ["Connect to Managed Nodes" on page 281](#)
- ["Connect to DEFINITY Systems with ASG" on page 287](#)

The login prompts display in separate popup windows on the COMMUNICATION MANAGER screen.

Saving login data

Users should administer the DEFAULT LOGIN screen to save the login data the for **new** DEFINITY systems. Refer to the procedure to ["Administer the Default Login" on page 235](#),

When users administer new DEFINITY systems, the Proxy Agent displays the default login data on page F of the MANAGED NODES screen. Users do **not** have to complete the procedures on the COMMUNICATION MANAGER screen to save new login data.

At the COMMUNICATION MANAGER screen, generally users should **not** save the login data unless the system prompts them to enter a new password. The prompt to resave login data displays if the "password aging" feature is enabled on the managed node. The system permanently stores the login data until users change and save login data at a later time.

Emulation sessions

The EMULATION application allows users to directly connect with **one** managed node and conduct an administration session on the system. Therefore, users do **not** need to execute the connection procedures in this chapter. Refer to ["Connect to Two Managed Nodes" on page 303](#).

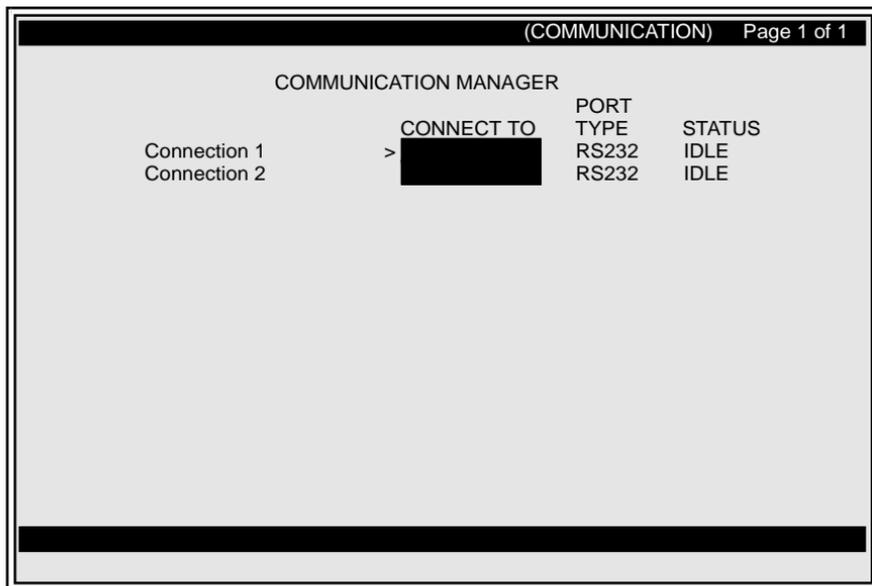
Users can connect to **two** managed nodes before starting an administration session from the EMULATION application. The EMULATION application allows users to start and quit a session with the managed nodes **without** dropping the connections.

To conduct an emulation session with two managed nodes connections, users must execute the procedures in the order listed below:

- Access the COMMUNICATION MANAGER screen and connect the two managed nodes. Do **not** save the login data. Refer to the appropriate procedure below:
 - ["Connect to Managed Nodes" on page 281](#)
 - ["Connect to DEFINITY Systems with ASG" on page 287](#)
- Access the EMULATION application and conduct the administration session. Refer to ["Connect to Two Managed Nodes" on page 303](#).
- Access the COMMUNICATION MANAGER screen and disconnect the managed nodes at the **end** of the administration session. Refer to ["Disconnect from Managed Nodes" on page 296](#).

Review of the Communication Manager Screen

The figure below shows the COMMUNICATION MANAGER screen with the two connections fields.



sdnmcomm LJK 040798

Figure 28. Communication Manager screen

Field descriptions The table below contains the descriptions for the fields on the COMMUNICATION MANAGER screen.

Table 24. Communication Manager screen

| Field | Description |
|--------------------------|---|
| CONNECT TO Fields | |
| Connection 1 | <p>Contains the first managed node that is currently connected to the Proxy Agent.</p> <p>The field is blank if a managed node is NOT currently connected.</p> <p>The Help list (Ctrl-Y) contains the valid options for this field:</p> <ul style="list-style-type: none">• List of all managed nodes administered on the Proxy Agent• The disconnect command if a managed node is currently connected. The disconnect command does not appear on the list if the field is blank. |
| | <i>1 of 2</i> |

Table 24. Communication Manager screen

| Field | Description |
|--------------|---|
| Connection 2 | <p>Contains the second managed node that is currently connected to the Proxy Agent.</p> <p>The field is blank if a second managed node is not currently connected.</p> <p>The Help list (Ctrl-Y) contains the valid options for this field:</p> <ul style="list-style-type: none"> • List of all managed nodes administered on the Proxy Agent • The disconnect command if a managed node is currently connected. The disconnect command does not appear on the list if the field is blank. |
| PORT TYPE | <p>Identifies the type of communication port the Proxy Agent uses to connect to the managed node.</p> <p>This is a view-only field.</p> |
| STATUS | <p>Identifies the current state of the Proxy Agent connection to a managed node.</p> <p>The valid options for the STATUS states include:</p> <p style="padding-left: 40px;">IDLE -- A dynamic connection is not connected</p> <p style="padding-left: 40px;">CONNECTED -- A managed node is connected</p> <p>This is a view-only field.</p> |
| | 2 of 2 |

Connect to Managed Nodes

This section contains the procedure to **manually** login to one or two managed nodes and execute the tasks below:

- To troubleshoot connections between the Proxy Agent and managed nodes.
- To connect to two managed nodes **before** starting an administration session from the EMULATION screen.

Required materials

Users must know the information listed below to complete the procedure:

- Login name for each managed node
- Password to access the each managed node

Procedure

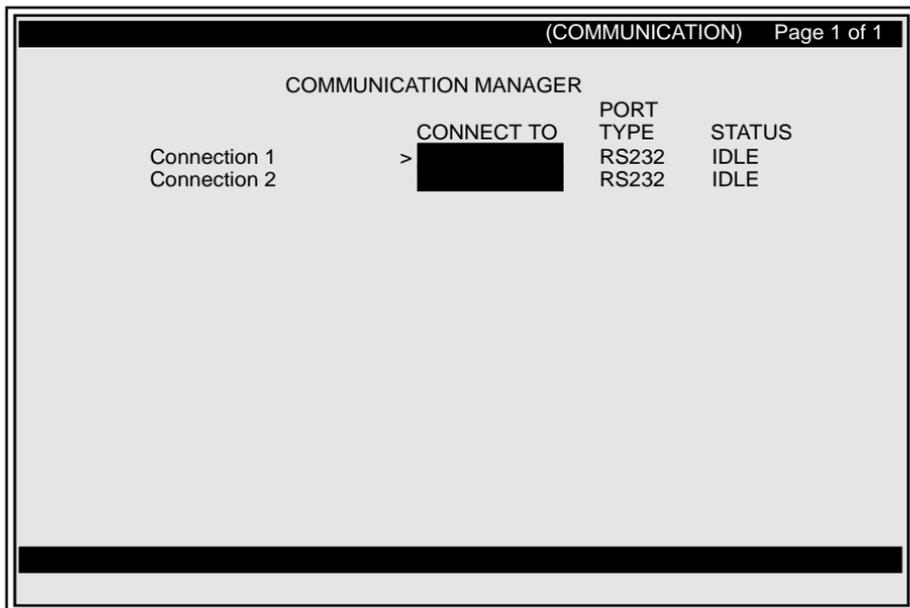
Complete the procedure below to **manually** login to managed nodes.

- 1 Access the Proxy Agent MAIN MENU.

In the command line,

- Type **communication**
- Press **ENTER**

Result: The system displays the COMMUNICATION MANAGER screen, as shown in the example below.



- 2 In the *Connection 1* field, execute **one** of the options (a or b) below:
 - a If the field is **blank**, connect the **first** managed node:
 - Press **Ctrl-Y** to display the Help list
 - Select a **[managed node]** from the list
 - Press **ENTER**

- b** If the field contains a connection that you want to change, then disconnect the managed node and select a different managed node:
- Press **Ctrl-Y** to display the Help list
 - Select **disconnect** to *drop* the current connection
 - Press **ENTER**
 - Press **Ctrl-Y** again
 - Select a different [**managed node name**] for the **first** connection
 - Press **ENTER**

Result: The system displays the selected node name in the *Connection 1* field.

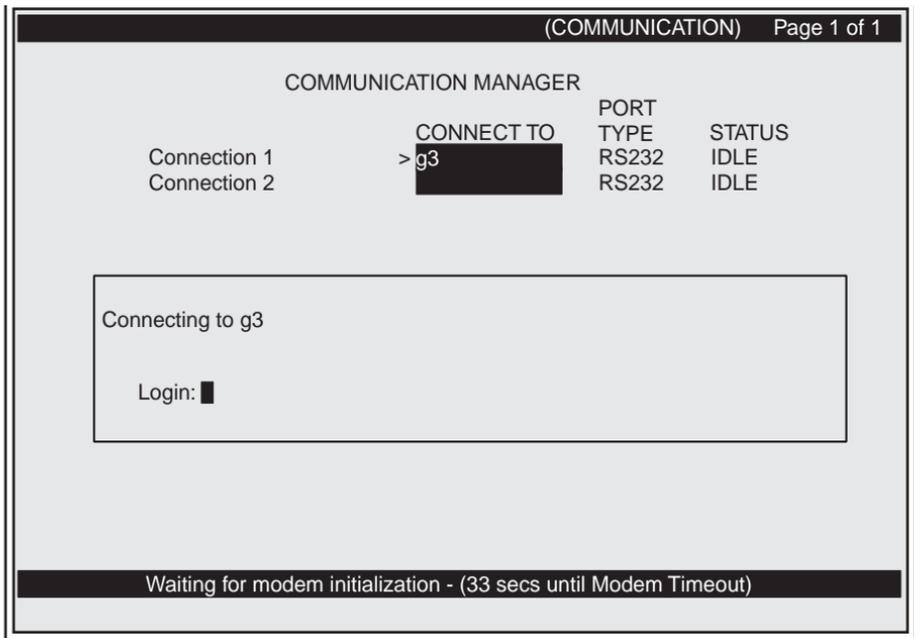
- 3 Optional.** In the *Connection 2* field, execute **one** of the options (a or b) in step [2](#) above to connect to a **second** managed node:

Result: The system displays the selected node name in the *Connection 2* field.

Note: If users selected a second node name in the *Connection 2* field, the system displays the login windows for each of the selected node names. Users must repeat steps [4](#) through [8](#) below for the second connection.

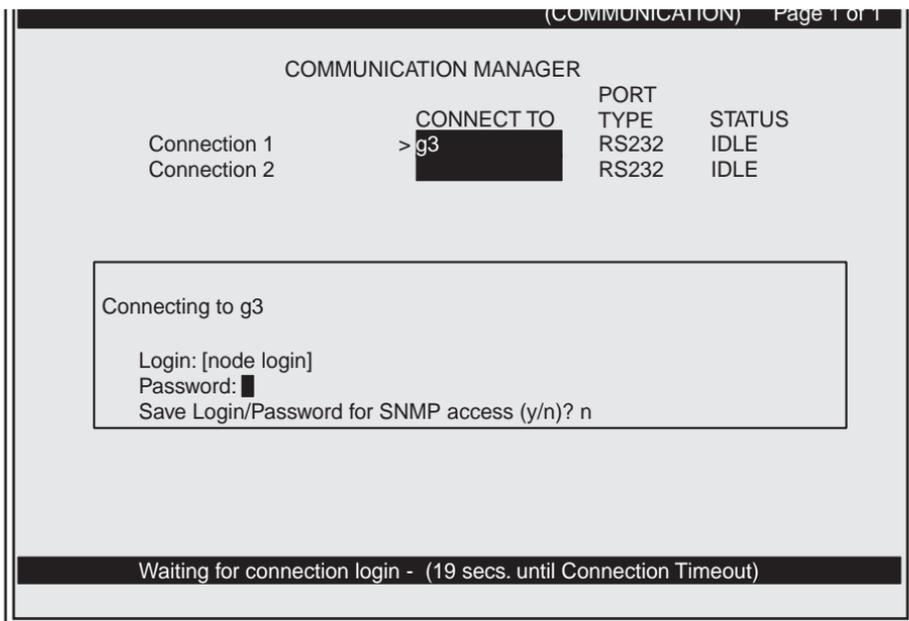
4 Press **Ctrl-E** to submit the changes.

Result: The system saves the changes and displays the *login* window below for the node name selected in the *Connection 1* field.



- 5 In the *Login* field,
- Type the [managed node login]
 - Press **ENTER**

Result: The system displays the *password* window below.



6 In the *Password* field,

- Type the [**managed node password**]
- Press **ENTER**

Result: The system displays the prompt: Save Login/Password for
SNMP access (y/n)? n

7 Execute **one** of the options (a or b) below:

a To save **new** login data the first time,

- Press **Y** (yes)
- Press **ENTER**

b To connect to two managed nodes for an administration session, do **NOT** save the login data if the data has been previously saved:

- Press **ENTER** to select **N** (no)

Result: The system displays the message: Negotiating protocol
communication

Then, the system displays the Proxy Agent MAIN MENU that
contains the confirmation message: Connected To [managed
node]

8 At the completion of the task, complete the procedure to ["Disconnect from Managed Nodes" on page 296](#).

Connect to DEFINITY Systems with ASG

This section contains the procedure to manually connect to DEFINITY systems that are protected by the Access Security Gateway (ASG) and execute the tasks below:

- To troubleshoot connections between the Proxy Agent and managed nodes.
- To connect to two managed nodes **before** starting an administration session from the EMULATION screen.

The ASG login procedure includes the tasks below:

- The user enters a login and optionally saves the ASG **secret key** at the prompts on the screen. The secret key is a 20-character octal string.
- The system responds with a numeric **challenge** that contains a 7-digit number.
- To generate a **response** to the challenge, the user enters the secret key, challenge, and other required data into a hand-held ASG device. The device generates a 7-digit numeric response to the system challenge.
- Then the user enters the numeric response in the field to gain access to the DEFINITY system.

Required materials

Users must know the information listed below and have the ASG device to complete the ASG login procedure:

- Login name for the DEFINITY system
- ASG secret key to access the DEFINITY system
- Challenge from the DEFINITY system

- Hand-held ASG device to generate a response to the challenge from the DEFINITY system

ASG Procedure Complete the procedure below to manually log in to ASG-protected DEFINITY systems.

- 1 Access the Proxy Agent MAIN MENU. In the command line,
 - Type **communication**
 - Press **ENTER**

Result: The system displays the COMMUNICATION MANAGER screen:

```
(COMMUNICATION) Page 1 of 1

COMMUNICATION MANAGER

Connection 1      > ██████████  PORT
Connection 2      > ██████████  TYPE
                                     RS232  STATUS
                                     RS232  IDLE
                                     IDLE
```

- 2 In the *Connection 1* field, execute **one** of the options (a or b) below:
 - a If the field is **blank**, connect the **first** managed node:
 - Press **Ctrl-Y** to display the Help list
 - Select a [**managed node**] from the list
 - Press **ENTER**
 - b If the field contains a connection that you want to change, then disconnect the managed node and select a different managed node:
 - Press **Ctrl-Y** to display the Help list
 - Select **disconnect** to drop the current connection
 - Press **ENTER**
 - Press **Ctrl-Y** again
 - Select a different [**managed node name**] for the first connection
 - Press **ENTER**

Result: The system displays the selected node name in the *Connection 1* field.

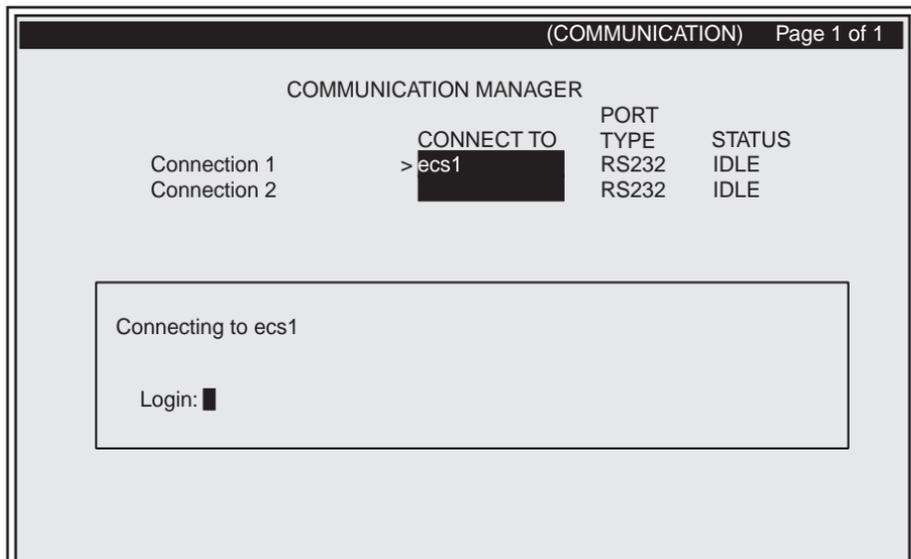
- 3 **Optional.** In the *Connection 2* field, execute **one** of the options (a or b) in step [2](#) above to connect to a second managed node:

Result: The system displays the selected node name in the *Connection 2* field.

Note: If users selected a second node name in the *Connection 2* field, the system displays the ASG login windows for each of the selected node names. Users must repeat steps [4](#) through [10](#) below for the second connection.

4 Press **Ctrl-E** to submit the changes.

Result: The system saves the changes and displays the *login* window below for the node name selected in the *Connection 1* field.



5 In the *Login* field,

- Type the [managed node login]
- Press **ENTER**

Result: The system displays the one of two windows depending on whether or not the login and secret key have been saved. Execute one of the options (a or b) listed below:

- To save the login and secret key for **new** managed nodes, go to step [6](#).
- To **not** save the login and secret key for managed nodes, go to step [7](#).

6 Save the Login. If the login and ASG secret key have **NOT** been saved, the system displays a window with the prompt:

```
COMMUNICATION MANAGER

Connection 1      CONNECT TO      PORT      STATUS
Connection 2      > ecs1          RS232     IDLE
                  [REDACTED]    RS232     IDLE
```

Connecting to ecs1

A Login and Access Security Gateway (ASG) Secret Key have NOT been saved for SNMP access

Would you like to save Login/ASG Secret Key for SNMP access (y/n)?

To save the login data, execute the steps (a through d) below:

- a At the prompt, type **Y** (yes) and press **ENTER**

Result: The system displays a window with the first prompt: Access Security Gateway (ASG) Secret Key:

- b At the prompt, type the **[secret key]** and press **ENTER**

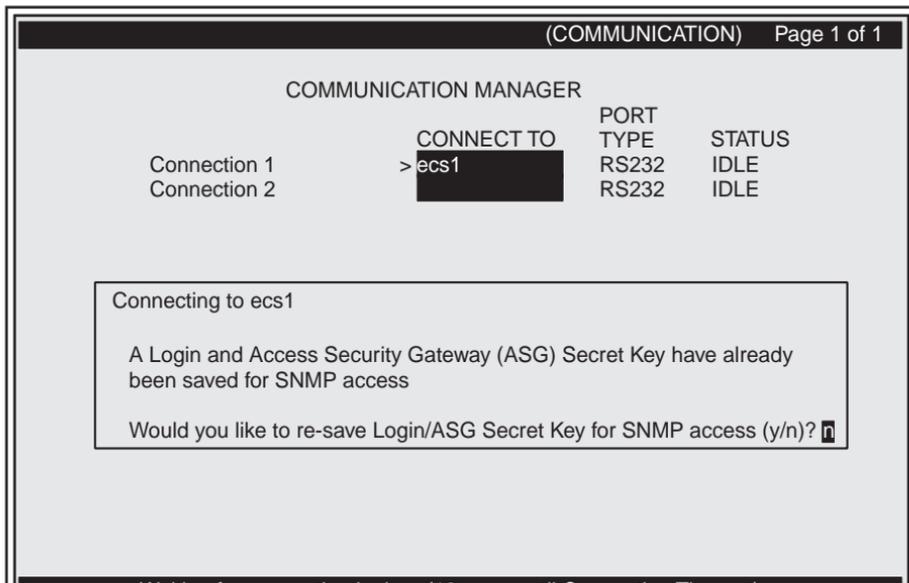
Result: The system displays a second prompt: Save Login & ASG Secret Key for SNMP access (y/n)?

- c At the prompt, type **Y** (yes) and press **ENTER**

Result: The system displays the window with the numeric challenge: Challenge: XXX-XXXX

- d Go to step [8](#) to complete the remaining steps in the procedure.

7 Do NOT Save the Login. If the login and ASG secret key have previously been saved, the system displays a window with the prompt below:



To connect to a managed node without saving the ASG and secret key for an emulation session, execute the steps (a and b) below:

- At the prompt, type **N** (no) and press **ENTER**

Result: The system displays the window with the numeric challenge:

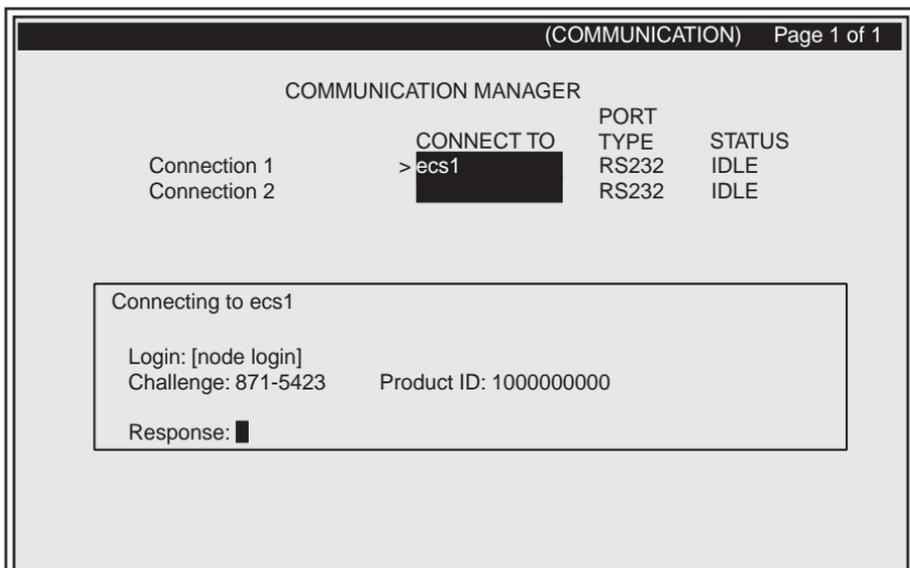
Challenge: XXX-XXXX

- Go to step [8](#) to complete the remaining steps in the procedure.

- 8 ASG Device.** Access the hand-held ASG device and enter the required data in the device (secret key, challenge, etc.).

Result: The ASG device displays a 7-digit numeric response.

- 9 Response to the Challenge.** In the `Response` field on the window shown below, execute the steps below:



- Type [**response number**] from the ASG device
- Press **ENTER**

Result: The system displays the message: Negotiating protocol communication

Then, the system displays the Proxy Agent MAIN MENU that contains the confirmation message:

Connected To [managed node]

- 10 At the completion of the task, complete the procedure to ["Disconnect from Managed Nodes" on page 296](#).

Disconnect from Managed Nodes

Complete the procedure below to manually disconnect the managed nodes.

- 1 Access the Proxy Agent MAIN MENU.

In the command line,

- Type **communication**
- Press **ENTER**

Result: The system displays the COMMUNICATION MANAGER screen.

- 2 In the *Connection 1* field,

- Press **Ctrl-Y** to select the Help list
- Select **disconnect**
- Press **ENTER**

- 3 **Optional.** In the *Connection 2* field,

- Press **Ctrl-Y** to select the Help list
- Select **disconnect**
- Press **ENTER**

- 4 Press **Ctrl-E** to submit the changes.

Result: The system drops the connections and displays the Proxy Agent MAIN MENU.

13 Emulation Application

Chapter Contents

- [*Introduction*](#) [*298*](#)
- [*Review the Emulation Screen*](#) [*299*](#)
- [*Conduct an Emulation Session*](#) [*300*](#)
 - [*Connect to One Managed Node*](#) [*301*](#)
 - [*Connect to Two Managed Nodes*](#) [*303*](#)

Introduction

The **Emulation** application provides direct communication with one or two managed nodes for real-time administration.

Users can access all commands and forms that are available from the Generic 3 Management Terminal.

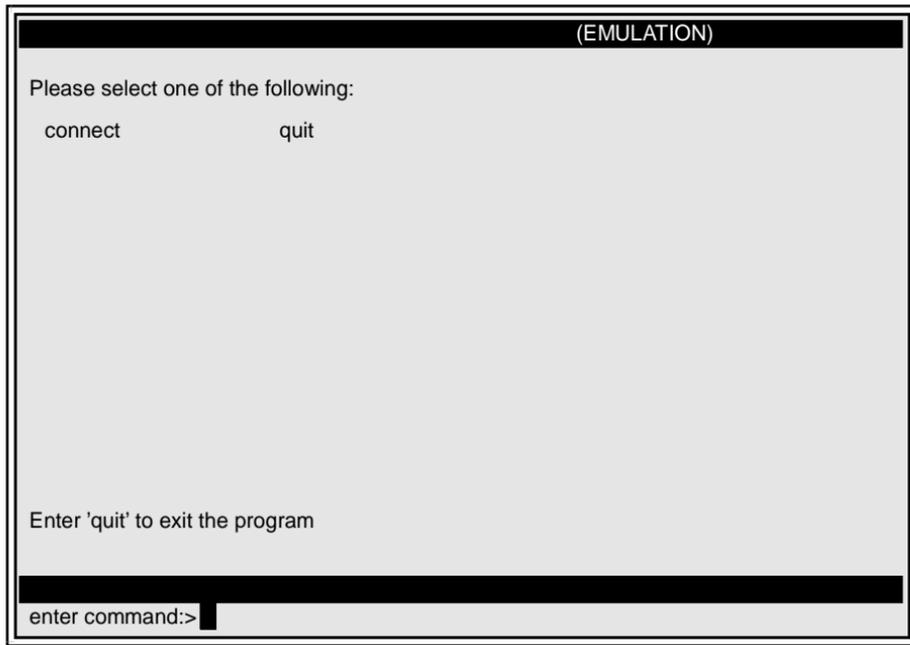
For DEFINITY systems, the emulation application adds the following features:

- Reliable communications using a protocol
- Pop-up help
- Direct page selection
- Color

See also Refer to [Chapter 12, "Communication Application"](#) for procedures to connect two managed nodes **before** an emulation session and to disconnect the two managed nodes at the **end** of a session.

Review the Emulation Screen

The figure below shows the two commands available on the EMULATION screen:



sdnmemu LJK 040798

Figure 29. Emulation screen

Conduct an Emulation Session

The **Emulation** application allows users to establish a direct connection with **one** managed node during an emulation session.

Users do **not** need to connect a managed node on the COMMUNICATION MANAGER screen before they begin the emulation session with one managed node.

If users want to connect with **two** managed nodes during an emulation session, then refer to the ["Connect to Two Managed Nodes" on page 303.](#)

The commands that are available on the Generic 3 Management Terminal are also available on the Proxy Agent emulation application.

Connect to One Managed Node

Complete the procedure below to establish an emulation session with **one** managed node.

- 1 Access the Proxy Agent MAIN MENU.

In the command line,

- Type **emulation**
- Press **ENTER**

Result: The system accesses the EMULATION application.

- 2 In the command line,

- Type **connect [managed node]**
- Press **ENTER**

Result: The system displays one (a or b) of the results below:

- a If the managed node is **not** connected, then the system displays the *login* window. Execute the steps [3](#) and [4](#) to log in.
 - b If the managed node is **connected**, then the system displays the MAIN MENU for the managed node. Go to step [5](#).
- 3 In the *Login* field,
 - Type the **[managed node login]**
 - Press **ENTER**

4 In the *Password* field,

- Type the [managed node password]
- Press **ENTER**

Result: The system displays the prompt: Save Login/Password for
SNMP access (y/n)? n

5 Press **ENTER** to select no.

Result: The system displays the message: Negotiating protocol
communication

Then, displays the MAIN MENU for the managed node.

6 Conduct an administration session on the managed node. The commands that you can normally use with the login you selected will be available to you during this session.

7 To end the emulation session,

- Type **quit**
- Press **ENTER**

Result: The system exits the Emulation screen. Then, the system displays the Proxy Agent MAIN MENU.

Connect to Two Managed Nodes

To conduct an emulation session with **two** connections, users must complete the following procedures in the order listed below:

- Access the COMMUNICATION MANAGER screen to connect two managed nodes. Do **not** save the login data.
- Access the EMULATION screen to conduct the administration session with both managed nodes.
- Access the COMMUNICATION MANAGER to disconnect the two managed nodes.

Procedure

Complete the procedure below to establish **two** connections for an emulation session.

- 1 Access the Proxy Agent MAIN MENU. In the command line,
 - Type **communication**
 - Press **ENTER**

Result: The system displays the COMMUNICATION MANAGER screen.

- 2 In the connection fields, connect two managed nodes for the emulation session. Do not save the login data. Refer to the appropriate procedure:
 - ["Connect to Managed Nodes" on page 281](#)
 - ["Connect to DEFINITY Systems with ASG" on page 287](#)

Result: The system saves the data and displays the Proxy Agent MAIN MENU.

3 In the command line on the Proxy Agent MAIN MENU,

- Type **emulation**
- Press **ENTER**

Result: The system displays the EMULATION menu.

4 To establish the connection with the **first** managed node,

- Type **connect [managed node]**
- Press **ENTER**

Result: The system displays the system MAIN MENU for the **first** managed node.

5 Conduct an administration session on the **first** managed node. The commands that you can normally use with the login you selected will be available to you during this session.

6 To end the emulation session with the **first** managed node,

- Type **quit**
- Press **ENTER**

Result: The system exits the emulation session with the **first** managed node. Then, displays the EMULATION menu.

7 To establish the connection with the **second** managed node,

- Type **connect [managed node]**
- Press **ENTER**

Result: The system displays the system MAIN MENU for the **second** managed node.

- 8 Conduct an administration session on the **second** managed node. All G3 switch commands are available during the emulation session.
- 9 To end the emulation session with the **second** managed node,

- Type **quit**
- Press **ENTER**

Result: The system exits the emulation session with the **second** managed node. Then, displays the EMULATION menu

Note: Users can move back and forth between the connections from the EMULATION menu.

- 10 To end the emulation session with **both** connections,
 - Type **quit**
 - Press **ENTER**

Result: The system exits the EMULATION menu. Then, the system displays the Proxy Agent MAIN MENU.

- 11 In the command line on the Proxy Agent MAIN MENU,
 - Type **communication**
 - Press **ENTER**

Result: The system displays the COMMUNICATION MANAGER screen.

- 12 On the COMMUNICATION MANAGER screen, disconnect the two managed nodes. Refer to ["Disconnect from Managed Nodes" on page 296.](#)

14 Configuration Application

Chapter Contents

- [Introduction](#) [307](#)
- [Administer the Change Hardware Screen](#) [309](#)
 - [Review the Change Hardware Screen](#) [310](#)
 - [Administer the Change Hardware Options](#) [314](#)
- [Administer the Change User-Interface Screen](#) [316](#)
 - [Review the Change User-Interface Screen](#) [317](#)
 - [Administer the Change User-Interface Options](#) [322](#)

Introduction

The purpose of the **Configuration** application is to administer the system-wide, default parameters on the two configuration screens that are described below.

Change Hardware screen

The CHANGE HARDWARE screen contains two types of information:

- Software release and versions of the UNIX operating system and the Proxy Agent that are currently installed on the Proxy Agent computer
- Default parameters for the serial ports

Change User-Interface screens

The CHANGE USER-INTERFACE screens contains four pages of configuration and color options.

Page 1 contains the **configuration** options to:

- Set the color options on the monitor
- Turn on or turn off the audible beep tone

Typically, the configuration options on page 1 are the only options that users may want to change.

Pages 2 through 4 contain the options to **customize** the colors for the elements listed below:

- Screen elements
- Activity Area elements
- Popup Display Window elements

**Installation
process**

During the installation process, the installation script updates the software versions on the CHANGE HARDWARE screen.

The Configuration application contains the system-wide, default parameters for both of the CHANGE HARDWARE screen and the CHANGE USER_INTERFACE screen.

Generally, users will ***not*** need to change the default settings on either of the Configuration screens.

Administer the Change Hardware Screen

The CHANGE HARDWARE screen contains two types of information:

- Software versions for the UNIX operating system and the Proxy Agent software that are currently installed on the Proxy Agent computer
- Default parameters for the serial ports

Lucent **recommends** that users do **not** change the default settings for the serial ports on the CHANGE HARDWARE screen. These settings work well with most communication devices.

However, users can change the parameters for **individual** managed nodes on the page **B** of the MANAGED NODES screen. The new settings will override the system-wide parameters and become the custom settings for the individual managed node.

PA001 form

The Managed Nodes section of the PA001 form should contain the speed setting for serial port that the Proxy Agent uses to connect to individual managed nodes.

Review the Change Hardware Screen

In the figure below, the “**xx**” in the *Proxy Agent Version* field refers to the load number of the software which may vary for the current release.

The screenshot shows a terminal window titled "change hardware (CONFIGURATION) Page 1 of 1". The content is as follows:

```
change hardware (CONFIGURATION) Page 1 of 1
CHANGE HARDWARE
SOFTWARE VERSIONS
  UNIX Release: 4.2MP
  UNIX Version: 2.1.3
  Proxy Agent Version: 3.0.XXX
SERIAL PORT DEFAULT PARAMETERS
  Speed: >9600
  Stop Bits: 1
  Flow Control? n
  Parity: none
  Character Size: 8
```

sdnmhard LJK 092299

Figure 30. Change Hardware screen

Field descriptions

The table below contains descriptions of the fields on the CHANGE HARDWARE screen. The screen contains the two sections listed below:

- Software Versions (view-only)
- Serial Port Default Parameters

Table 25. Change Hardware screen

| Field | Description |
|-------------------------------------|---|
| SOFTWARE VERSION (view-only) | |
| UNIX Release | Identifies the release number of the UnixWare operating system that is currently installed on the Proxy Agent computer. This is a view-only field. |
| UNIX Version | Identifies the version number of the UnixWare operating system that is currently installed on the Proxy Agent computer. This is a view-only field. |
| Proxy Agent Version | Identifies the version number of the Proxy Agent software that is currently installed on the Proxy Agent computer. This is a view-only field. |
| | <i>1 of 3</i> |

Table 25. Change Hardware screen

| Field | Description |
|---------------------------------------|---|
| SERIAL PORT DEFAULT PARAMETERS | |
| Speed | <p>Sets the baud rate for the modem that connects the Proxy Agent to the managed node.</p> <p>The HELP list (Ctrl-Y) contains the valid options for this field:</p> <ul style="list-style-type: none">9600 (default)480024001200 |
| Stop Bits | <p>Sets the stop bit parameter on the modem.</p> <p>The HELP list (Ctrl-Y) contains the valid options for this field:</p> <ul style="list-style-type: none">1 (default)2 |
| | <i>2 of 3</i> |

Table 25. Change Hardware screen

| Field | Description |
|----------------|--|
| Flow Control | <p>Turns-off or turns-on the flow control parameter on the modem.</p> <p>The HELP list (Ctrl-Y) contains the valid options for this field:</p> <p>n (no) (default) -- Turn off</p> <p>y (yes) -- Turn on</p> |
| Parity | <p>Sets the parity parameter on the modem.</p> <p>The HELP list (Ctrl-Y) contains the valid options for this field:</p> <p>none (default)</p> <p>odd</p> <p>even</p> |
| Character Size | <p>Sets the character size parameter on the modem.</p> <p>The HELP list (Ctrl-Y) contains the valid options for this field:</p> <p>8 (default)</p> <p>7</p> |
| | <i>3 of 3</i> |

Administer the Change Hardware Options

Complete the procedure below to access the CHANGE HARDWARE screen.

Generally, users will **not** change the system-wide, default parameters for the serial port on the CHANGE HARDWARE screen.

Note: Users can make changes to the parameters for individual managed nodes on page **B** of the MANAGED NODES screen. The changes made on the MANAGED NODES will **override** the system-wide parameters on the CHANGE HARDWARE screen.

Procedure

- 1 Access the Proxy Agent MAIN MENU. In the command line,
 - Type **configuration**
 - Press **ENTER**

Result: The system accesses the *Configuration* application. Then, displays a blank command line on the Proxy Agent MAIN MENU.

- 2 In the command line on the Proxy Agent MAIN MENU:
 - Type **change hardware**
 - Press **ENTER**

Result: The system displays the CHANGE HARDWARE screen.

- 3 In the SOFTWARE VERSION column, verify the release numbers for the UnixWare and the Proxy Agent software. The fields are **view-only**. Users cannot change the data.

- 4 The data in the SERIAL PORT DEFAULT PARAMETERS fields contain the system-wide, default parameters shown below:

Speed: **9600**

Stop Bits: **1**

Flow Control: **n** (no)

Parity: **none**

Character Size: **8**

To **change** the default system parameters, which is **NOT** recommended:

- Press **Ctrl-Y** in each field to display the Help list
- Select a **new** value from the list
- Press **ENTER** to change the value

- 5 Execute **one** of the options (a or b) below:

- a If users made any changes, press **Ctrl-E** to save the changes and exit the CHANGE HARDWARE screen.
- b If users do **not** make any changes, press **Ctrl-X** to exit the CHANGE HARDWARE screen.

Result: The system exits the screen and displays the Proxy Agent MAIN MENU.

Administer the Change User-Interface Screen

The CHANGE USER-INTERFACE screen contains four (4) pages of configuration options.

Page 1 contains the **configuration** options to:

- Set the color options of the monitor
- Turn-on or turn-off the audible beep tone

Pages 2 through 4 contain the fields to **customize** the colors of the elements listed below:

- Screen elements on page 2
- Activity Area elements on page 3
- Popup Display Window elements on page 4

Users can experiment with various color combinations and immediately view the results of your changes in the sample screens that appears on pages 2 through 4.

Review the Change User-Interface Screen

The figures in this section show default settings on the four pages of the CHANGE USER-INTERFACE screens.

Page 1

The figure below shows the configuration options on page 1 of the CHANGE USER-INTERFACE screens.

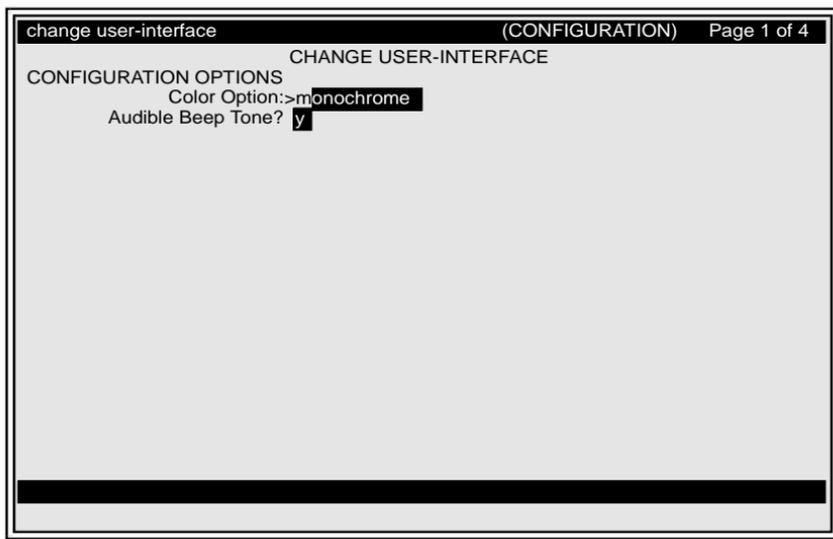


Figure 31. Page 1, Configuration Options

Page 1 field descriptions

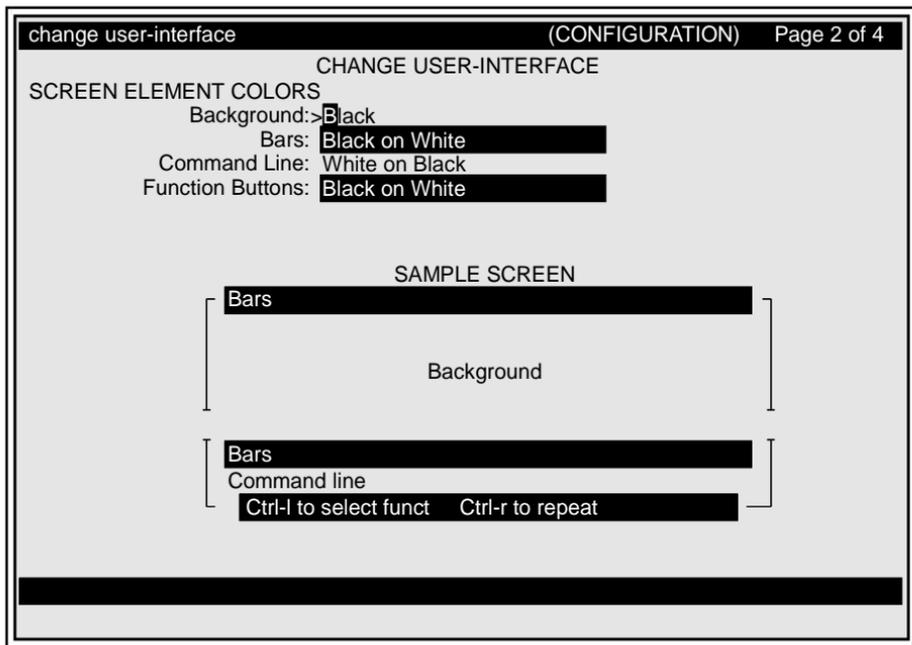
The table below contains the field descriptions for configuration options on page 1 of the CHANGE USER-INTERFACE screens.

Table 26. Configuration options

| Field | Description |
|---------------------------------------|---|
| CONFIGURATION OPTIONS (page 1) | |
| Color Option | Sets the colors for the monitor. The Help list (Ctrl-y) contains the valid options for the field: default -- for color monitors monochrome -- default for black-and-white monitors customize -- change color of screen elements (see pages 2 through 4 below) |
| Audible Beep Tone? | Sets the beep tone to ON or OFF. The Help list (Ctrl-y) contains the valid options for the field: y (yes) -- Turns ON the beep tone (default) n (n) -- Turns OFF the beep tone |
| | |

Page 2

The figure below shows the screen element colors on page 2 of the CHANGE USER-INTERFACE screens.

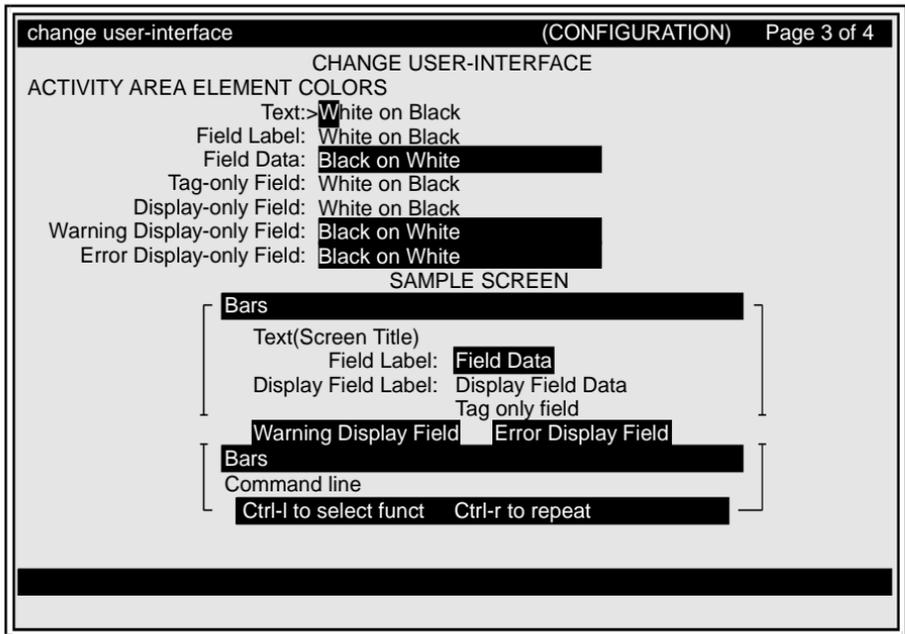


sdnmusr2 LJK 040798

Figure 32. Page 2, Screen Element Colors

Page 3

The figure below shows the activity area element colors on page 3 of the CHANGE USER-INTERFACE screens.



sdnmusr3 LJK 040798

Figure 33. Page 3, Activity Area Element Colors

Page 4

The figure below shows the popup display window element colors on page 4 of the CHANGE USER-INTERFACE screen.

change user-interface (CONFIGURATION) Page 4 of 4

CHANGE USER-INTERFACE

POPUP DISPLAY WINDOW ELEMENT COLORS

Border and Background: White on Black

Field Label: White on Black

Field Data: Black on White

Text: White on Black

Highlight: Black on White

Tag-only Field: White on Black

Display-only Field: White on Black

Activity Message: White on Black

SAMPLE WINDOWS

| | |
|-------------------------------|--------------------|
| Text(Heading) | |
| Field Label: | Field Data |
| Display Field Label: | Display Field Data |
| | Tag only field |
| Activity messages appear here | |

| | |
|-------------------|---|
| Border/Background | |
| element | 1 |
| highlight | 2 |
| element | 3 |

sdnmusr4 LJK 040798

Figure 34. Page 4, Popup Display Window Element Colors

Administer the Change User-Interface Options

Complete the procedure below to change the system-wide, default parameters for the configuration and color options.

Note: For color monitors, users must set the TERM variable to **color or default** so that Proxy Agent screens will be in color.

1 Access the Proxy Agent MAIN MENU. In the command line:

- Type **configuration**
- Press **ENTER**

Result: The system accesses the Configuration application. Then, displays a blank command line on the Proxy Agent MAIN MENU.

2 In the command line on the Proxy Agent MAIN MENU:

- Type, **change user-interface**
- Press **ENTER**

Result: The system displays page 1 of the CHANGE USER-INTERFACE screen.

3 In the *Color Option* field on page 1,

- Press **Ctrl-Y** to display the Help list
- Select one of the options below:
 - default** (for color monitors)
 - monochrome** (default for black- and-white monitors)
 - customize**
- Press **ENTER** to change the option

Administer the Change User-Interface Options

- 4 In the *Audible Beep Tone?* field on page 1,
 - Press **Ctrl-Y** to display the Help list.
 - Select one of the options below:
 - **Y** (yes) to turn-on the beep tone (default)
 - **N** (no) to turn-off the beep tone
 - Press **ENTER** to change the option
- 5 **Optional.** Complete the steps below to customize the colors of the screen elements on pages 2 through 4,
 - Press **Ctrl-Y** in each field to display the Help list
 - Select an option
 - Press **ENTER** to change the option
 - Press **Ctrl-D** to access the next page
- 6 Execute **one** of the options (a or b) below:
 - a If users made any changes, press **Ctrl-E** to save the changes and exit the CHANGE USER-INTERFACE screen.
 - b If users do **not** want to make any changes, press **Ctrl-X** to exit the CHANGE USER- INTERFACE screen.

Result: The system exits the screen and displays the Proxy Agent MAIN MENU.

15 I/O Setup Application

Chapter Contents

- [Introduction](#) [325](#)
- [Devices File](#) [326](#)
 - [Edit the Devices File](#) [327](#)
- [Dialers File](#) [328](#)
 - [Devices and Dial Strings](#) [328](#)
 - [Edit the Dialers File](#) [332](#)

Introduction

The **I/O Setup** application provides direct access to the **Devices** file and the **Dialers** file:

- The **Devices** file contains the **tty port settings** for the communication devices that connect the Proxy Agent to the managed nodes.
- The **Dialers** file contains the device name and **dial strings** that the Proxy Agent uses to dial into the managed node.



CAUTION:

Only the system administrator or root user should edit the **Devices** and **Dialers** files.

Installation process

During the installation process, the installation script updates the **Devices** file and the **Dialers** file with default parameters for this release.

Devices File

The **Devices** file contains the updated **tty port settings** for the communication devices that are described below.

The Lucent-certified **alarm receiver** devices include the following types:

- AT&T 2224CEO
- AT&T 3710 Dataport
- AT&T 3715 Dataport Express
- U.S. Robotics Sportster 33.6
- US Robotics Sportster 56K
- Paradyne Compusphere 3820

The Lucent-certified **alarm sender** devices include the following types:

- AT&T 3710 Dataport
- AT&T 3715 Dataport Express
- U.S. Robotics Sportster 33.6
- US Robotics Sportster 56K

Note: Lucent does **not** certify the AT&T 2224CEO as an **alarm sender** device for Proxy Agent to forward alarms to INADS.

CAUTION:

Lucent recommends that users do **not** change the settings in the Devices file unless their business needs require modification of the file.

Edit the Devices File

Only the system administrator or root user should edit the Devices file.

Required materials

The system administrator must have the following materials and information:

- Root login and password
- PA001 form

Procedure

The procedure to edit the Devices file uses **vi** as the text editor.

- 1 Login as root user.
- 2 At the UNIX prompt, use a UNIX text editor to open the Devices file:
 - Type **vi /etc/uucp/Devices**
 - Press **ENTER**
- 3 In the *Password* prompt field,
 - Type the [root password]
 - Press **ENTER**

Result: The system displays the *Devices* file.

- 4 Edit the appropriate **tty port settings** for the communication devices.
- 5 To write and quit the file,
 - Type **:wq!**
 - Press **ENTER**

Result: The system saves the changes, then displays the UNIX prompt.

Dialers File

This section contains the contents of the Dialers file and the procedure to edit the dial strings.

Devices and Dial Strings

The information below is an excerpt from the Dialers file that contains the list of the Lucent-certified devices and the dial string for each device function.

```
#####
```

Start DG3PA DIAL STRINGS: (DONT MODIFY THIS LINE)

This section is maintained by the DEFINITY G3 Proxy Agent Installation scripts. Any changes manually made to this section may be lost on upgrades.

PA prefix is for Proxy Agent switch/ecs access

PAD prefix is for Proxy Agent switch/ecs access with Terminal Servers that fail to drop DTR correctly during a disconnect

AS prefix is for Proxy Agent Alarm Sending/Forwarding

AR prefix is for Proxy Agent Alarm Reception modem options

RM prefix is for Lucent TSC/ITAC Remote Maintenance Modem options

```
#####
```

Dialers for SNMP Proxy Agent certified devices

2224CEO AT&T 2224CEO modem

PA2224 =+,, "" \M\datzod,o12=y,o4=n,\n3\lc1\lj0\lq0\lg0\r/c \006 at\T\r/c
Connected

AR2224 =+,, "" \M\datzod,o2=n,o12=y,o34=1,o36=0,o41=0\r/c \006

3710 AT&T Paradyne 3710 Dataport Modem

PA3710 =+,, "" \M\dAT&F&C2Q2&D2\N1&Y0&W0 OK ATDT\T CONNECT

AS3710 =+,, "" \M\dAT&F&C0&D0Q2\N1Y0&Y0&W0 OK ATDT\T CONNECT

AR3710 =+,, "" \M\dAT&F\N1Q2&C1&Y0&W0 OK

RM3710 =+,, "" \M\dAT&F&D2&S1&R0\D1&C5Q2S85=1S41=0S43=1S79=1\r/c
OK \dAT\N7S49=0&Y0&W0\r/c OK

3715 AT&T Paradyne 3715 Dataport Express Modem

PA3715 =+,, "" \M\dAT&F&C2Q2&D2\N1&Y0&W0 OK ATDT\T CONNECT

AS3715 =+,, "" \M\dAT&FQ2&C2&R0\Q1\N1%C0S0=0%B1200&Y0&W0 OK
\rATDT\T\r/c CONNECT

AR3715 =+,, "" \M\dAT&FB0Q2&C1&R0\N1\Q0%B1200%C0S78=1&Y0&W0
OK

RM3715 =+,, "" \M\dAT&FB0Q2&C1&R0\N1\Q0%B1200%C0S78=1&Y0&W0
OK

3830**AT&T Paradyne 3830 Modem**

PA3830 =,-, "" \M\dAT&FE1V1X4Q0&C2&D2S7=255S0=0&W0\r/c OK
\EATDT\T\r/c CONNECT \m

RM3830 =,-, "" \M\d\at&f0q2&d2&r0&s1\d1s65=2&w0\r/c OK

**Sportster 33.6
and Sportster
56K****US Robotics Sportster 33.6Kbps Modem**

ASusr336 =+,-, "" \M\d+++dATH0\r/c OK
\dAT&F&M0Q2&C1&D0&R1&H0&U2&N2&K0S0=0S13=1Y0&W0 OK ATDT\T
CONNECT

ARusr336 =+,-, "" \M\d+++dAT&F&M0&C1&U2&N2Q2S0=1Y0&W0 OK

RMusr336 =+,-, "" \M\dAT&F&M0&C1&U2&N2Q2S0=1Y0&W0 OK

PAusr336 =+,-, "" \M\dAT&F&M0&N6Y0&W0 OK ATDT\T CONNECT

**7400A, 7400B,
and 7400B+****Paradyne 7400B/+ Data Module**

PA7400B =,-, "" \M\dAT&F\r/c OK \r\dATE1V1X4Q0&C1&D3S0=0S7=255\r/c
OK ATDT\T\r/c CONNECT \r\m\c

PAD7400B =,-, "" \M\d+++dATH0\r/c\dAT&F\r/c OK
\r\dATE1V1X4Q0&C1&D3S0=0S7=255\r/c OK ATDT\T\r/c CONNECT \r\m\c

8400B+ **Paradyne 8400B+ Data Module** - S24=1 tells 8400B+ it is a stand-alone data mod

PA8400B =,-, "" \M\dAT&F\r/c OK \r\dATS24=1\r/c OK
\r\dATE1V1X4Q0&C1&D3S0=0 S7=255\r/c OK ATDT\T\r/c CONNECT \r\m\c

PAD8400B =,-, "" \M\d+++dATH0\r/c\dAT&F\r/c OK \r\dATS24=1\r/c OK
\r\dATE1V1X4Q0&C1&D3S0=0S7=255\r/c OK ATDT\T\r/c CONNECT \r\m\c

Hot line **Hot Line**

PAhotline "" \K\r\r\r\d in:-\K\r\r\r\d-in:-\K\r\r\r\d-in: \d

ADU **ADU connections**

PAadu =+ "" \M\K\p DIAL: \T ANSWERED \p\c\m

PDM **PDM connections**

PApdm =+ "" \M\K\p DIAL: \T ANSWERED \p\c\m

Direct **Direct connect** into term port on back of switch

PAdirect "" \M\d

PADirect =,-, "" \M\d+++

PAdirect =,-, "" \M\d+++dATH0\r/c\dAT&F\r/c OK

#####

End DG3PA DIAL STRINGS: (DONT MODIFY THIS LINE OR DIALERS BLOCK ABOVE)

#####

Edit the Dialers File

Only the system administrator or root user should edit the Dialers file.

CAUTION:

Lucent recommends that users do **not** change the default dial strings in the Dialers file. If changes must be made, then the system administrator should make those changes outside the DG3PA dialer block, as described in the procedures to edit the Dialers file.

Required materials

The system administrator must have the following materials and information:

- Root login and password
- PA001 form

Procedure

The procedure to edit the Dialers uses **vi** as the text editor.

- 1 Login as root user
- 2 At the UNIX prompt, use a UNIX text editor to open the Dialers file:
 - Type **vi /etc/uucp/Dialers**
 - Press **ENTER**
- 3 In the *Password* prompt field,
 - Type the [**root password**]
 - Press **ENTER**

Result: The system displays the *Dialers* file.

- 4 To verify dial strings are valid for each device, compare the dial strings in the this section to the dial strings in the Dialers file.
- 5 **Optional.** If necessary, complete the steps below to edit the appropriate dial strings *outside* the DG3PA dialer block:
 - Copy the **dialer string** that to be edited
 - Paste the dialer string *outside* the block, after the line: “End DG3PA DIAL STRINGS.”
 - Edit the dialer string
- 6 To write and quit the file,
 - Type **:wq!**
 - Press **ENTER**

Result: The system saves the changes, then displays the UNIX prompt.

16 Maintenance and Troubleshooting

Chapter Contents

- [Introduction](#) [335](#)
- [Add New Devices](#) [336](#)
- [Change Settings for SNMP Access](#) [337](#)
- [View Alarm and Error Logs](#) [338](#)
- [Use Alarm Testing Tools](#) [339](#)

Introduction

The Proxy Agent contains several maintenance and troubleshooting options that only the **system administrator** or root user should execute to manage the Proxy Agent.

These options include tasks listed below:

- Add new devices to the Proxy Agent **after** the Proxy Agent has been installed
- Change settings for SNMP access **after** the Proxy Agent has been installed
- View alarm and error logs to **troubleshoot** the receiving and forwarding of alarms
- Use the **alarm testing tools** to simulate alarm and trap reception on the Proxy Agent and test the event configuration on the Network Management System (NMS)

Add New Devices

The system administrator or root user can add new communications devices to the Proxy Agent from the `/usr/bin/dpa_portadm` file.

System administrators must access the file and respond to the prompts. The prompts are identical to the prompts in the installation script for the function and the device type.

For more information, refer to the sections listed below:

- [*"Function Prompt" on page 100.*](#)
- [*"Device Type Prompt" on page 102.*](#)
- [*"Serial I/O Subsystem" on page 104.*](#)
- [*"Upgrade from Proxy Agent 2.0 and Later" on page 116.*](#)

Change Settings for SNMP Access

The system administrator or root user must **reinstall** the Proxy Agent in order to change settings for SNMP access.

Refer to the procedure to ["Upgrade from Proxy Agent 2.0 and Later" on page 116](#). It is not necessary to remove the Proxy Agent.

At the installation prompts listed below, change the **current setting** for:

- SNMP Polling
- SNMP Traps, **if** SNMP Polling is disabled
- SNMP Set Capability

For more information about the SNMP prompts, refer to the sections below:

- ["SNMP Polling Prompt" on page 99](#)
- ["SNMP Traps Prompt" on page 99](#)
- ["SNMP Set Capability Prompt" on page 100](#)

TSC service

The Technical Services Center (TSC) can change the settings for the SNMP access prompts without reinstalling the Proxy Agent.

The TSC will **bill** the customer for this service on a time and materials basis.

View Alarm and Error Logs

The Proxy Agent maintains a number of alarm and error logs in the **agent** directory. System administrators can view the logs to troubleshoot problems with receiving and forwarding alarms.

To access the logs, edit the directories in the table below.

Table 27. Alarm and error logs

| Log | Directory |
|--|--|
| Event log for alarm receiver device | /usr/g3-ma/agent/logs/alarmlog |
| Error log for alarm receiver device | /usr/g3-ma/agent/logs/errorlog |
| Alarms scheduled to be sent to INADS or other destinations | /usr/g3-ma/agent/alarms/alrms_rcvd.log |
| Alarms successfully sent to INADS or other destinations | /usr/g3-ma/agent/alarms/alrms_sent.log |
| Error log for alarm sender device | /usr/g3-ma/agent/alarms/alarms.log |
| | |

Use Alarm Testing Tools

The Proxy Agent contains a set of Trap Test tools. System administrators can use these tools to:

- Simulate the alarm reception on the Proxy Agent and
- Test the trap reception and event configuration on the Network Management System (NMS)

The Proxy Agent contains a script for each product type. All scripts reside in the **/usr/g3-ma/bin** directory.

Trap Test scripts

The table below contains the command and function for the trap tests scripts:

Table 28. Trap Test Scripts

| Command | Function |
|--------------|------------------------------------|
| TrapTest | DEFINITY and MCU traps |
| CMSTrapTest | Call Management System (CMS) traps |
| ADXTrapTest | DEFINITY Audix traps |
| IADTrapTest | INTUITY Audix traps |
| INTTTrapTest | INTUITY Interchange traps |
| CVSTrapTest | Conversant traps |
| | |

Procedure

The procedure below uses the DEFINITY TrapTest tool as an example of the format for the alarm testing tools. For other products, the script for the TrapTest tool is slightly different.

Note: For the tools to work, the Proxy Agent must be running and the ALARM PATH and MANAGED NODES screens must be properly administered.

- 1 At the UNIX shell, log in to the root (/) directory.
- 2 Access a test script. The steps below show an example of a TrapTest script:
 - Type `/usr/g3-ma/bin/TrapTest`
 - Press **ENTER**

Result: The system opens the file and displays the script for the selected trap test, as shown in the example below. The fields may contain the data from the previous test.

```
DEFINITY Proxy Agent Alarm Trap Test Tool
Current DEFINITY Node Name: NewYork
Current DEFINITY Alarm ID: 111111111
0) Alarm Clear Trap [alarmClear:0]
2) Major Alarm Trap [alarmMajor:2]
3) Minor Alarm Trap [alarmMinor:3]
5) Major External Alarm Trap [extalarmMajor:5]
6) Minor External Alarm Trap [extalarmMinor:6]
7) TSC Dispatch Alarm Trap [alarmDispatch:7]
8) TSC Close Alarm Trap [alarmClose:8]
9) Restart Notification Trap [alarmRestart:9]
```

```
C) Change DEFINITY alarming from
H) Help
Q) Quit
```

```
Send which trap?:
```

3 Select the Change Option. To change to a different DEFINITY node name, go to the field: Send which trap?:

- Type **C** (change)
- Press **ENTER**

Result: The system displays the message:

```
Changing DEFINITY that the Alarms will be coming
from... You must set the Node Name and the Alarm ID for
the DEFINITY you wish alarms to be associated with.
The Name and ID must match those specified in the
managed node form of the Proxy Agent for the switch you
wish to send traps for.
```

```
Enter new DEFINITY Node Name:
```

```
Enter new DEFINITY Alarm ID:
```

4 Enter a New Node Name. As shown in the example below, type a new node name and the alarm ID for a DEFINITY system. Press **ENTER** after each entry:

```
Enter new DEFINITY Node Name: jupiter
```

```
Enter new DEFINITY Alarm ID: 1222222222
```

Result: The system displays the new node name and alarm ID in the fields and displays the prompt to select a trap test, as shown below.

```
DEFINITY Proxy Agent Alarm Trap Test Tool
```

```
Current DEFINITY Node Name: jupiter
```

```
Current DEFINITY Alarm ID: 1222222222
```

```
0) Alarm Clear Trap [alarmClear:0]
2) Major Alarm Trap [alarmMajor:2]
3) Minor Alarm Trap [alarmMinor:3]
5) Major External Alarm Trap [extalarmMajor:5]
6) Minor External Alarm Trap [extalarmMinor:6]
7) TSC Dispatch Alarm Trap [alarmDispatch:7]
8) TSC Close Alarm Trap [alarmClose:8]
9) Restart Notification Trap [alarmRestart:9]
C) Change DEFINITY alarming from
H) Help
Q) Quit
```

```
Send which trap?:
```

5 Select a trap option. As shown in the example below, type a number (0-9) to select a trap test and press **ENTER**.

```
Send which trap?: 5
```

Result: The system displays the message and the fields shown in the example in the next step.

- 6 Execute the trap test.** Users can enter *any* data in the in the free-form fields. The system does not validate the fields. As shown in the example below, type data in each field and press **ENTER** after each entry:

```
Enter alarm trap information for External trap
MIB oid names are show in brackets
Switch [g3clientExternalName]: jupiter
Proxy Agent Sequence Number [g3alarmsAlarmNumber]:
000000012
Switch Port Location [g3alarmsPort]: 01C1201
On-Board Alarm Flag [g3alarmsOnBrd]: Y
External Device Alt. Name [g3extdevAltName]: ENVUPS1
External Device Description [g3extdevDescription]:
PROXY AGENT UPS
External Device ID [g3extdevID]: 2001
External Device Building [g3extdevBuilding]: Building 30
External Device Address [g3extdevAddress]: 1234 Main St
```

Result: The system displays the message: Alarm Trap Emulation Successful

Then, the system displays the UNIX prompt.

- 7** Access the NMS to view the results of the test. Repeat this procedure to execute other trap tests.

Index

- A**
 - ADU
 - with moss adaptor, cable connections for [71](#)
 - analog
 - cable connections for local modems [68](#)
 - Audible Beep Tone field, on Change User-Interface screen [318](#)
- C**
 - cable connections
 - for ADU with moss adaptor [71](#)
 - for digital data modules [70](#)
 - for local analog modems [68](#)
 - Char Size field, on page B of Managed Nodes screen [253](#)
 - Character Size field, on Change Hardware screen [313](#)
 - Connection 1 field, on Communication Manager screen [279](#)
 - custom submap
 - in Submap Name field on Managed Nodes screen [256](#)
- D**
 - Default Login screen
 - procedure to administer login data [235](#)
 - Dial String field, on pages D and E of Managed Nodes screen [261](#)
 - Dialing Order field, on pages D and E of Managed Nodes screen [260](#)
 - digital data module
 - cable connections [70](#)
- F**
 - Filter Set
 - procedure to add new [220](#)
 - Flow Cntrl field, on page B of Managed Nodes screen [253](#)
 - Flow Control field, on Change Hardware screen [313](#)

- M** Managed Nodes screen
 - field descriptions for page F [263](#)
- N** Node Name field
 - on page C of Managed Nodes screen [255](#)
 - on pages D and E of Managed Nodes screen [259](#)
- P** Parity field
 - on Change Hardware screen [313](#)
 - on page B of Managed Nodes screen [253](#)
- Port Type field, on Communication Manager screen [280](#)
- Proxy Agent
 - log in security [43](#)
 - new features [45](#)
- Proxy Agent Version field, on Change Hardware screen [311](#)
- Q** quit command, on Proxy Admin screen [163](#)
- S** security
 - proxy agent access [43](#)
 - SNMP authentication [43](#)
- SNMP
 - security authentication [43](#)
- Speed field
 - on Change Hardware screen [312](#)
- start command, on Proxy Admin screen [163](#)
- State field
 - on page C of Managed Nodes screen [256](#)

Status field, on Communication Manager screen [280](#)

Stop Bits field

 on Change Hardware screen [312](#)

stop command, on Proxy Admin screen [163](#)

Submap Name field

 on page C of Managed Nodes screen [256](#)

Submap Type field

 on page C of Managed Nodes screen [255](#)

U UNIX Release field, on Change Hardware screen [311](#)

UNIX Version field, on Change Hardware screen [311](#)