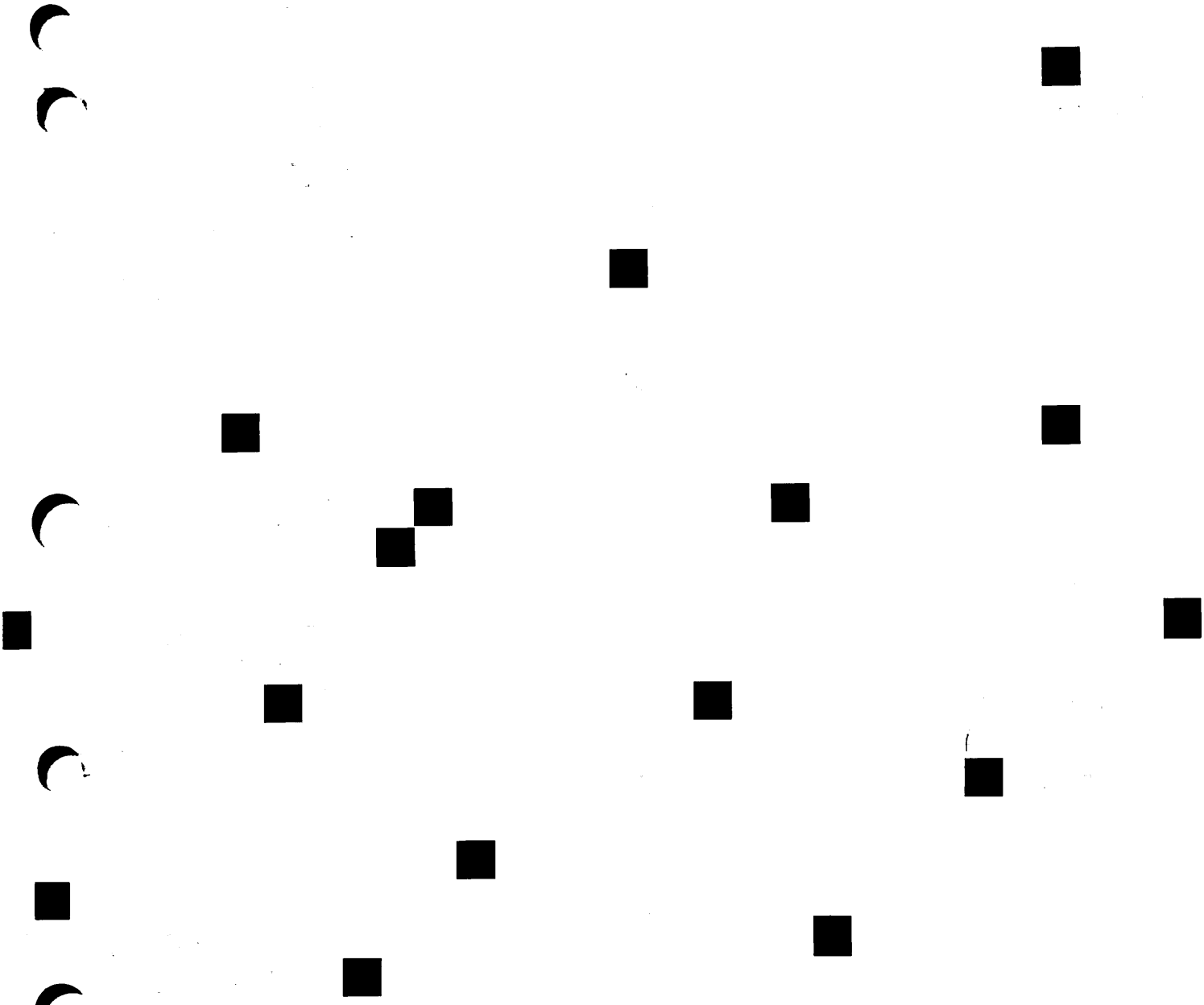

Prime®

DSM User's Guide

Revision 23.0

DOC10061-3LA

DSM User's Guide

Third Edition

UK Technical Publications Team

This guide documents the software operation of the Prime Computer and its supporting systems and utilities as implemented at Master Disk Revision Level 23.0 (Rev. 23.0).

Prime Computer, Inc., Prime Park, Natick, MA 01760

The information in this document is subject to change without notice and should not be construed as a commitment by Prime Computer, Inc. Prime Computer, Inc., assumes no responsibility for any errors that may appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license.

This document was prepared in the United Kingdom by Technical Publications Department, International Systems Marketing and Development, 4 Bramley Road, Mount Farm, Milton Keynes, MK1 1PT, United Kingdom.

PRINTING HISTORY

First Edition (DOC10061-1LA) July 1987
Second Edition (DOC10061-2LA) September 1988
Third Edition (DOC10061-3LA) June 1990

CREDITS

Design:	Richard Merry-West
Editorial:	Fiona Carey
Project Support:	Dave Cheeseman and Vaughn Meads
Illustration:	Will Mallender
Production:	Prime Technical Publications production unit

How to Order Technical Documents

To order copies of documents, or to obtain a catalog and price list:

United States Customers	*International*
Call Prime Telemarketing, toll free, at 1-800-343-2533, Monday through Thursday, 8:30 a.m. to 8:00 p.m. and Friday, 8:30 a.m. to 6:00 p.m. (EST).	Contact your local Prime subsidiary or distributor.

PRIME SERVICE℠

Prime provides the following toll-free number for customers in the United States needing service:

1-800-800-PRIME

For other locations, contact your Prime representative.

Surveys and Correspondence

Please comment on this manual using the Reader Response Form provided in the back of this book. Address any additional comments on this or other Prime documents to:

Technical Publications Department
Prime Computer, Inc.
500 Old Connecticut Path
Framingham, MA 01701

CONTENTS

APPENDICES

ABOUT THIS BOOK

The DSM User's Guide is both a guide and reference to Prime's Distributed Systems Management (DSM) products and services. The book describes how to administer and use DSM on a computer network.

The Guide includes an introduction to DSM, and chapters that describe the administrative and security structure of DSM, startup and operation, DSM configuration, event message handling, log administration and display. It also describes the DSM applications System Information Metering (SIM), and Remote System User (RESUS).

The book contains many new terms and concepts that are exclusive to DSM. It assumes a working knowledge of the PRIMOS® file system and the Access Control List (ACL) security mechanism. All the new terminology used in the manual, together with some PRIMOS terms and concepts, is provided in a glossary at the back of the book.

Chapter Contents

Chapter 1	What is DSM?, introduces Prime's DSM package, outlines the facilities it provides, and describes its main features.
Chapter 2	Administration and Security, describes the administrative and security structure of DSM, explains how DSM user access definitions control access to DSM facilities, and covers administrator-level issues relating to the Unsolicited Message Handler (UMH) and the DSM logging service. The chapter also explains how to use the two facilities jointly, to control and customize system and network event logging.
Chapter 3	Startup and Operation, covers day-to-day operations, including startup, monitoring, and shutdown. It also describes the directory DSM*.

Chapter 4	Configuring DSM, explains how to set up the administrative structures that define how DSM is to be used on a network. It explains how to use the command CONFIG_DSM to create the configuration file, and describes how you use the command DISTRIBUTE_DSM to change the configuration. The STATUS_DSM command is also described.
Chapter 5	UMH Configuration, explains how to use the CONFIG_UM command to configure event message logging and display, on local and remote nodes. Read this chapter in conjunction with the related sections in Chapters 2 and 3, that show how to use the the facilities of the UMH in event logging and message display.
Chapter 6	Log Administration and Display, explains how to use the ADMIN_LOG command to create and administer DSM logs, and DISPLAY_LOG command, to display those logs selectively. Use this chapter in conjunction with the related sections in Chapters 2 and 3, that describe the general DSM logging facility.
Chapter 7	System Information and Metering (SIM), describes how you can use SIM to obtain up-to-the-minute status information about a network of computer systems. The SIM command functions are described in detail, and explanations are formatted for quick reference.
Chapter 8	Remote System User (RESUS), explains how RESUS allows System Administrators and trusted operators to control and monitor any machine on a computer network, from any terminal on that network, by giving them remote access to system commands.
Appendix A	DSM Configuration Files, contains listings of the Empty and Default Configuration Files, and an example configuration.
Appendix B	DSM Product Names, lists the Prime product names that are registered with DSM as senders of unsolicited messages.
Appendix C	Sending Customer Unsolicited Messages, describes the subroutine that you use to send unsolicited messages from customer products registered with DSM.
Appendix D	Glossary, provides definitions of terms used in this book.

Related Documentation

Other Prime manuals referred to in this document are:

- *System Administrator's Guide, Vol I – System Configuration* (DOC10131-3LA). This describes system fundamentals from the Administrator's viewpoint.
- *System Administrator's Guide, Vol II – Communication Lines and Controllers* (DOC10132-2LA) and *Release Note* (RLN10132-21A). This describes Prime's communications controllers, configuring and assigning asynchronous lines, and allocating line buffers.
- *System Administrator's Guide, Vol III – System Access and Security* (DOC10133-3LA). This describes how to configure user access to the system, and how to maintain security.
- *Overview of Prime Networks* (DOC10116-1LA). This is an introduction to Prime's networking software.
- *Operator's Guide to Prime Networks* (DOC10114-11A). This describes how to operate a system on a Prime network.
- *Programmer's Guide to Prime Networks* (DOC10113-11A). This is a user and reference guide to Prime's networking subroutines.
- *PRIMENET Planning and Configuration Guide* (DOC7532-4LA) and *Update Package* (UPD7532-41A). This describes how to configure PRIMENET on a system. For System Administrators.
- *PRIMOS Commands Reference Guide* (DOC3108-7LA) and *Release Note* (RLN3108-71A). This is a dictionary of PRIMOS commands. Full details of operator commands can be found in the relevant Operator's Guides.
- *Subroutines Reference Guide, Vols. I-V*, These are reference guides, in dictionary format, for Prime programmers:

  Vol.I: Using Subroutines – (DOC10080-2LA) and *Update Package* (UPD10080-21A).
  Vol.II: File System – (DOC10081-2LA).
  Vol.III: Operating System – (DOC10082-2LA).
  Vol.IV: Libraries and I/O – (DOC10083-2LA).
  Vol.V: Event Synchronization – (DOC10213-1LA) and *Update Package* (UPD10213-11A).

- *NTS User's Guide* (DOC10117-2LA). This describes Prime's LAN300 local area network software.

Other Prime manuals that may be useful for reference are:

- *Operator's Guide to System Commands* (DOC9304-5LA). This is a reference guide to commands used in the day-to-day operation of Prime systems.
- *Operator's Guide to System Monitoring* (DOC9299-3LA). This describes day-to-day monitoring and maintenance of Prime systems.
- *User's Guide to Prime Network Services* (DOC10115-1LA) and *Update Package* (UPD10115-11A). This describes how to use Prime's networking software.
- *Software Release Document Rev. 23.0* (DOC10001-7PA).
- *Rev. 23.0 Networks Release Notes* (RLN10252-1LA).

PRIME Documentation Conventions

The following conventions are used in command formats, statement formats, and in examples throughout this document. Examples illustrate how you use these commands and statements in typical applications.

Convention	*Explanation*	*Example*
UPPERCASE	In command formats, words in uppercase indicate the actual names of commands, statements, and key words. They can be entered in either uppercase or lowercase.	RESUS
lowercase	In command formats, words in lowercase represent items for which you must substitute a suitable value.	DISPLAY_LOG logname
Abbreviations in option descriptions	If an uppercase word in a command format has an abbreviation it is shown below the name in braces.	**{-PRIVATE_LOG -PLOG}**
Underscore in examples	In examples, user input is underscored but system prompts and output are not.	`OK, RESUS -START`
Boldface	When they first appear in the text, new terms are entered in boldface. These are included in the glossary.	**Application Server**
Italics	Italics, in text, indicate varaible user input, or emphasis. Names of any Prime documentation referenced in the text, is also shown in italics.	`the` *filename* `is...` *Prime NTS User's Guide*
typewriter	User examples, prompts, and program listings are displayed in typewriter font.	`Selection name:`
Angle brackets	In messages, a word or words enclosed within angle brackets indicates a variable for which the program substitutes the appropriate value.	`<filename> not found`
Braces within brackets	Braces within brackets enclose a list of items. Choose either none, or only one of these items; do not choose more than one.	**[{BRIEF FULL format name}]**

Braces	In command formats, chose one, and only one of the options or keywords enclosed in braces,	**-USERS** {**names** | **numbers**}

Changes Since Rev. 21

This section describes changes in DSM commands and services at Rev. 22.0 onwards. The changes are listed below.

- The START_DSM command no longer supports the -MULTI_NODE option. At Rev. 22.0 the network server is started by START_NET, not by START_DSM. To use DSM on remote systems, you need only ensure that PRIMENET is started on those systems.
- The network server no longer appears under the user name DSMNETSR.
- User DSM_LOGGER replaces DSMASR that controlled DSM logging at Rev. 21.0. The command file and runfile for the logging server are kept on DSM*, and are named LOGGER_ASR.cpl and LOGGER_ASR.run.
- You should reset ACLs on all directories that contain DSM logs, replacing DSMASR with DSM_LOGGER.
- The text database file DSM*>MSG_OBJ has been replaced by a language file on the new directory DSM*>SIT_TEXT_DBS. The file is named DSM_*language*.TDIMG.
- At Rev. 22.0 it is no longer necessary to share the database in the PRIMOS coldstart file; DSM.SHARE.COMI is no longer part of the PRIMOS.COMI template, and the file has been removed from the directory SYSTEM.
- Two new operator commands - CAB and LAB - can be controlled by DSM security. Access to the commands is through the DSM functions LIST_ASYNC_BUFFER and CHANGE_ASYNC_BUFFER. The commands use DSM unsolicited message handling to notify errors; messages from the commands are identified by the product name ASYNC$.
- New options and features on some SIM commands are itemized below:
  - LIST_ASYNC
    - The command accepts ranges of line numbers.
    - New option: -DETAIL.
  - LIST_DISKS
    - Displays robust/non-robust information.
    - Disk partitions can be identified by LDEV numbers.
    - -REMOTE option accepts node names.
    - New option -DETAIL
  - LIST_PRIMENET_NODES
    - New options:
      -ADDRESS
      -GATEWAY
      -ACCESS
      -VALIDATION
      -NO_VALIDATION

- LIST_PROCESS
  - System server names are only displayed if you specify -TYPE server.
  - The command accepts ranges of user numbers.
- LIST_UNITS
  - The -PATHNAME option now accepts a normal pathname.
  - Wildcarding can be used on all parts of the pathname.
  - The search path can be restricted by -WALK_FROM and -WALK_TO options.
  - The command accepts ranges of user numbers.
  - New options:
    -FILETYPE
    -DETAIL

1

WHAT IS DSM?

Introduction

This chapter introduces Prime's Distributed Systems Management (DSM), summarizes its main facilities, describes its software architecture, gives a brief description of DSM administration and security, and makes reference to DSM command error message formats.

Overview of DSM

Prime's **Distributed Systems Management (DSM)** is an integrated set of commands and services that you can use to manage, monitor, and control Prime systems and networks.

DSM allows you to treat the network as a single administrative unit. Commands and services can be invoked from any node on a network, on any other point on the network, and from any terminal. Although designed primarily to help with the management of large and small networks, DSM can also be used on single machines.

DSM commands and services are invoked from PRIMOS. They are executed on local and remote nodes by server processes that communicate with each other over the network and perform services on your behalf. For example, when you issue a System Information/Metering (SIM) command, servers on the target nodes gather the data and return it to you through the server on your node. There is no need to login to remote nodes, issue ARIDS, or concern yourself with existing network security.

DSM controls access to its own commands and services, by a special security mechanism that extends to the whole network. Through the configuration subsystem, Administrators can specify users' access to DSM commands, and control DSM independently on any subset of the network.

In summary, DSM is a family of systems management commands and services that help with the administration and day-to-day operation of Prime computer systems, with the added benefit of distributed execution and access control.

What DSM Allows You to Do

Using DSM commands, you can perform the following operations on local and remote nodes:

- Display system information.
- Administer event logging.
- Control the supervisor terminal from a user terminal.

Displaying System Information

The **System Information/Metering (SIM)** commands display system information on a network of machines. Using SIM commands, you can

- Interrogate local and remote systems for status, configuration and resource usage
- Initiate commands to return information at regular intervals
- Record system information in logs throughout the network

Event Logging

You can administer and control event logging on your network by

- Configuring DSM **Unsolicited Message Handling (UMH)** on each system
- Controlling and displaying logs using the log administration and display commands

The DSM Unsolicited Message Handling service automatically routes system and network event messages to log files, users, terminals or assigned devices throughout the network, according to selection criteria you define using the CONFIG_UM command. Using this command, you can

- Record event messages in private or system logs
- Display event messages to users
- Redirect event messages to devices on assigned lines

The DSM logging service records DSM messages in private and system logs, on behalf of the user. It is used to log DSM unsolicited messages, and to record SIM data.

The ADMIN_LOG and DISPLAY_LOG commands allow you to administer and display DSM logs on your system and network. Using the ADMIN_LOG command, you can create logs, control their growth, and perform other log management tasks. Using the DISPLAY_LOG command, you can display and print messages from DSM logs, in several formats.

Customer Products

You can register your own **customer products** in the DSM configuration, and use the DSM Unsolicited Message Handler to service messages issued by these products. A new subroutine is provided to allow your products to issue unsolicited messages.

Controlling Remote Systems

The **Remote System User (RESUS)** facility allows you to control the supervisor terminal on any local or remote machine from any terminal on the network. Access to RESUS can be controlled locally by supervisor terminal commands, and DSM provides additional security across the network.

Software Architecture

DSM contains two levels of software; the **kernel services** that control the DSM networking software, internode communications and security, and **applications** that use these services to invoke DSM commands and facilities. The kernel and application software is replicated on all nodes on which DSM is running.

The kernel services form the high-level communications software that implements secure invocation of DSM commands and message exchange throughout the network. Although invisible when you invoke a command, they are a major part of the DSM software.

Kernel services are controlled by the DSM server process that runs on all nodes where DSM is installed. DSM servers on different nodes communicate with each other through an interserver communication mechanism.

Applications are composed of two parts: the interface that controls dialog with the user, implements syntax checks and displays system prompts; and the software that invokes the command on the target node. The interface software runs in the user's own process, and the software that invokes and executes the command runs in a DSM process called the application server. Application servers invoke DSM commands and services on your behalf through their respective DSM servers, and never communicate directly with each other.

Information is exchanged between DSM applications in the form of message packets that conform to the ASN.1 (CCITT X.409) standard. Text for screen displays is held in the DSM message text database, in local language files.

Administration and Security

You control DSM on a system or network through an administrative system that is independent of existing network security. The system allows you to do two things. Firstly, it allows you to define the sphere of influence of individual administrators within the network, thereby defining independent administrative units. Secondly, it allows individual administrators to define users' access to DSM facilities within and between these units. The mechanism gives you wide discretion and flexibility when assigning access rights to users and user groups, and allows you to tailor security to the needs of your installation and network.

In DSM, the administrator's sphere of influence extends over a group of PRIMENET nodes known as a **configuration group.** Users' access to DSM, both within the group and between different groups, is controlled by administrator-defined **user access definitions.**

User access definitions link users' access to DSM commands and services and where they can be invoked, in any grouping and combination, throughout the network. In effect, they define *who* can do *what*, and *where*. DSM uses a system of user IDs that are unique on the network, and which ensure network-wide security on DSM commands.

DSM is primarily for Systems Administrators and senior operations staff. Other users can be given access to DSM commands at the administrator's discretion. An outline of how access to DSM facilities might be partitioned among different user groups is shown in Figure 1-1.

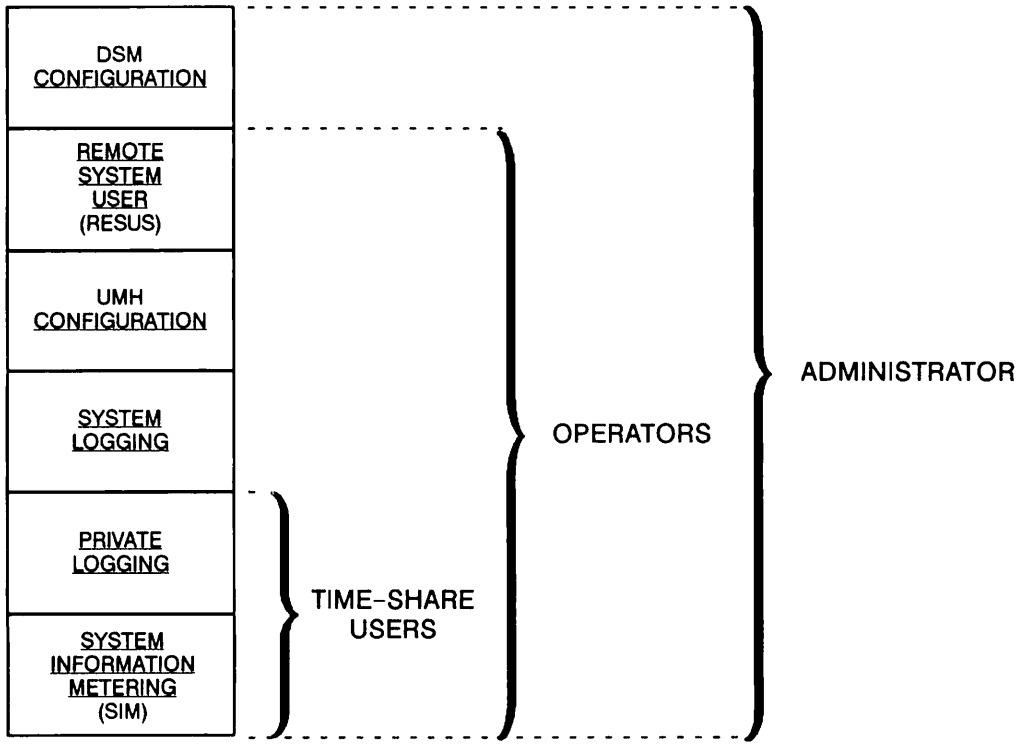

FIGURE 1-1 Example Hierarchy for Access to DSM Facilities

2

ADMINISTRATION AND SECURITY

Introduction

This chapter describes the concepts that underlie the administration of DSM on a Prime network. It explains how the administration of DSM on a network is divided between separate administrators, and how users' rights to DSM facilities are controlled by the administrator through user access definitions.

The chapter also introduces some of the factors you should consider when you are planning how to install and use DSM on your system or network. It describes DSM unsolicited message handling and message logging, and explains how the two systems combine to produce Prime's software event logging system.

Overview of DSM Administration and Security

DSM's administrative and security system allows you to partition the network for easier administration, and to define common policy for groups of machines.

To control access to its facilities on a Prime network, administrators can divide the network into groups of nodes under independent control. Group membership, and users' access to DSM commands and services within and without the group, is controlled by individual group administrators, while intergroup access is determined by cooperation between administrators. Groups of nodes under independent control are known as DSM **configuration groups**.

At installation, each node is a separate configuration group. To extend a configuration group to include more than one system you must configure DSM on the network. Configuring DSM is the process whereby you set up configuration groups, define users' access rights within groups, and distribute the new configuration to the group. It is performed using the DSM configurator commands.

Configuration data is held in a DSM configuration file that is replicated on all systems in a configuration group. DSM allows you to define an entire configuration just once, and then distribute it to all nodes in the configuration group simultaneously.

For details of the procedures you follow to define, distribute and activate a new configuration, see Chapter 4, Configuring DSM.

Users' access to DSM facilities within configuration groups is controlled by a security system that identifies users by their name and where they log in, and gives them access to specific facilities on specific nodes. An extension of this mechanism allows access across configuration group boundaries. The mechanism does not replace PRIMOS security on commands through Access Control Lists (ACLs) on DSM command runfiles, but rather provides an additional level of security that controls access to DSM facilities over the whole network.

Note

ACLs on DSM command runfiles override DSM security. If ACLs prevent you from running the command, you cannot invoke it even if you have access through DSM.

DSM security is flexible and allows you to configure DSM to suit your own requirements and network management. It allows you to define users' access to DSM applications in terms of individual DSM functions (commands or services), and the nodes where you can use these functions. You can use your own groupings of DSM commands, nodes and users, which you define for your own convenience. DSM security operates network-wide by identifying users and user groups uniquely throughout the network, and is independent of existing node-to-node trust established through Remote File Access (RFA).

DSM Configuration and Security

Security on DSM commands and facilities operates within groups of PRIMENET nodes known as configuration groups. Access control policy within each group is the responsibility of a single administrator, who sets up DSM user access definitions that define users' access to DSM commands.

Configuration Groups

A configuration group is a set of nodes that operate within the same security sphere, and which are therefore subject to the same administrative and security policies. All nodes in the group have a common view of group membership and users' access rights.

Configuration groups are established by distributing the same DSM configuration on all nodes in the group. Thereafter, the integrity of the group is maintained through a system of configuration identities, configuration revision numbers, and common views of group membership. For details of how the system works, see Configuration Group Integrity, later in this chapter.

A configuration group can be any convenient group of machines, from a single Prime system to a large interconnected network of machines. Group membership is not constrained by network topology, existing node-to-node security, geographical location, or CPU type (within the 50 Series). For single-system installations, the configuration group consists of the single machine.

As an example of how a configuration group might map onto a Prime installation, consider a Prime network of six systems organized as in Figure 2-1.

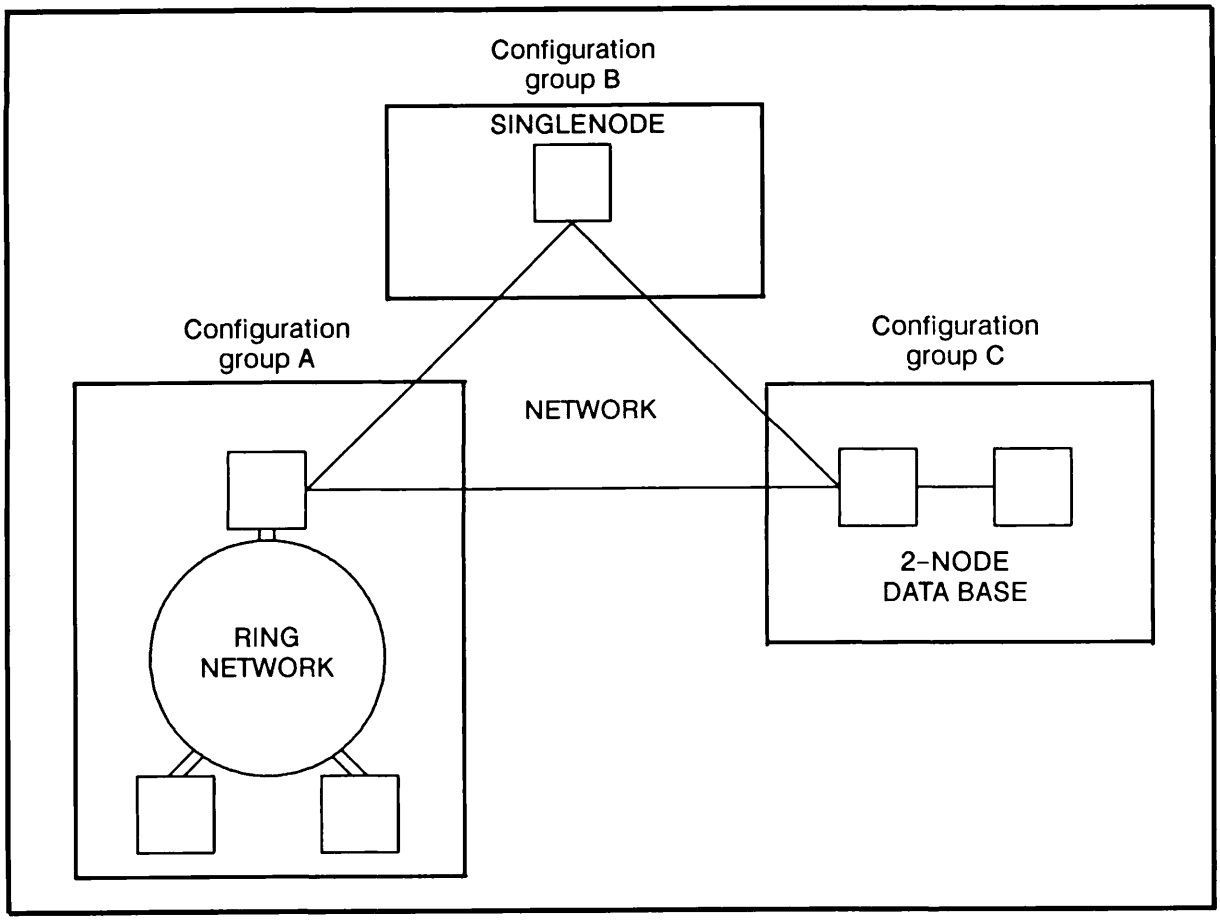

FIGURE 2-1 Distributing Control of DSM on a Network

The network is described below.

Configuration Group A: Three systems installed at a single site and connected in a ring network are administered collectively. One system on the ring acts as the gateway point for the rest of the systems on the network. Remote File Access is configured on all three machines in the ring.

Configuration Group B: A laboratory machine on the same site is connected into the ring through a full duplex line. It is under the independent control of a project director.

Configuration Group C: Two machines on another site contain a database that is accessible to users on the ring through a public service link. The administrator for the site is responsible for the two machines.

The network in this example contains three centers of administration; the three-node ring, the two-node database, and the single laboratory machine. This existing division into three well-defined administrative groupings could be mapped directly into three DSM configuration groups, each administered by separate administrators, and three separate configuration files.

The Configuration File

The DSM configuration file contains the data that establishes DSM administration and security policy on the network. It sets security on DSM commands and facilities, and defines group identity and intergroup access rights.

Data in the configuration file includes

- Configuration group membership
- Users' access definitions
- Contents of **node groups**
- Contents of **function groups**
- Details of the access allowed to systems and users outside the group
- Details of customer products

For details of user access definitions, node groups, function groups, and customer products, see the relevant sections below.

Collective Administration

Administering a configuration group can be the responsibility of one person, or it can be shared. If the responsibility is shared between several individuals, they must cooperate to produce an integrated set of administrative policies for the group, and define a single overall configuration.

Configuration Group Integrity

DSM ensures group integrity across configuration mismatches between nodes in the same configuration group. Mismatches can occur when nodes cannot be reached during the distribution of a new configuration, perhaps because of a communications failure, or because the node is not yet up on the network.

Where nodes in the same configuration group have different revisions of a DSM configuration file, they remain in the same configuration group, but access between them is restricted. The access allowed in these circumstances depends on which node has the more up-to-date revision.

Unsolicited messages are generated when access is denied between two nodes, and when a server detects a configuration file mismatch. You can log or display these messages at a terminal by configuring a UMH selection, so that you have an up-to-date record of the integrity of your configuration group.

For details of configuration file mismatch messages and their meanings, see Appendix D, and for details of how to configure an Unsolicited Message Handling (UMH) selection, see Chapter 5, UMH Configuration.

Intergroup Access

DSM security operates primarily to define users' access rights within the configuration group. To grant access to DSM commands across the configuration group boundary, you must do two things. First, you must specifically configure special access rights by naming those nodes which you, as administrator of the group, are prepared to trust. Second you must specify which functions to allow users from those nodes to invoke, on which nodes in your group. You do step one by defining the reserved node group .ALIEN_NODES$, and step two by completing the function part of the user access definition ALIEN$.

Note

All users from nodes defined in the alien nodes list acquire the access rights of the user access definition ALIEN$. The intergroup access mechanism does not distinguish between different users, only between different nodes.

Therefore, requests to invoke a DSM command from outside the configuration group must pass both local and remote security checks: a local check at the node where the user types the command, to ensure that the user has the correct user access definition, and two checks at the target node, which check whether

- The requesting node is in the alien node list .ALIEN_NODES$
- The function part of user access definition ALIEN$ allows the command to be invoked

As an example of intergroup access, consider the rights required by JOHN, a user who logs in on SYSA, to execute LIST_VCS on SYSB, a node in a different configuration group.

Firstly, at least one user access definition must exist in the configuration on SYSA to permit JOHN to use the LIST_VCS command on node SYSB; the user part of this user access definition must contain the following combination, either explicitly as user JOHN and SYSA, or implicitly through an ACL group of which JOHN is a member and a node group of which SYSA is a member:

(JOHN-from-SYSA)

and the function part must contain the combination:

(LIST_VCS-on-SYSB)

Secondly, the function part of ALIEN$ on SYSB must contain the combination:

(LIST_VCS-on-SYSB)

The Configurator Commands

DSM provides three commands that you use to configure DSM. CONFIG_DSM allows you to create a configuration file, DISTRIBUTE_DSM enables you to distribute the configuration, and STATUS_DSM allows you to determine configuration status. Details of the commands,together with a simple example of how to configure DSM are given in Chapter 4, Configuring DSM.

User Access Definitions

DSM security employs a series of access checks that determine which DSM commands users can invoke, and on which nodes. Access control data is in the form of DSM user access definitions that you define in the configuration file.

A user access definition links a user to a DSM function on a node where that function can be performed. In general terms, it maps a user to what that user can do, and where it can be done.

User access definitions consist of a user part and a function part. The user part of a user access definition contains one or more user names or ACL groups, each linked to nodes and node groups where the user can log in. Each combination of PRIMOS user name and node is unique and ensures that DSM security operates throughout the network. For further details, see User Identities later in this chapter.

The function part of a user access definition defines the commands and services that users can invoke, and the nodes where they can be invoked. It consists of individual combinations of functions or function groups with nodes or node groups. Functions and Function Groups are defined later in this chapter.

At its simplest, a user access definition is a single user name recognized on one node, linked to a single DSM function on another (or the same) node. More realistically, user access definitions usually contain several users or ACL groups recognized on several nodes or node groups, linked to multiple functions and function groups. There is no restriction on the number of users, nodes or functions in a user access definition.

Note

DSM access rights granted via user access definitions are accumulative. Users that are included in several access definitions have the access rights of all those definitions.

For example, in the user access definition OPSWORK illustrated in Figure 2-2, ARTHUR who logs in on SYSA, and all members of the ACL group .OPS who are recognized on all nodes in the configuration group, can invoke RESUS on node SYSB, and can invoke all of the SIM commands on nodes in the configuration group.

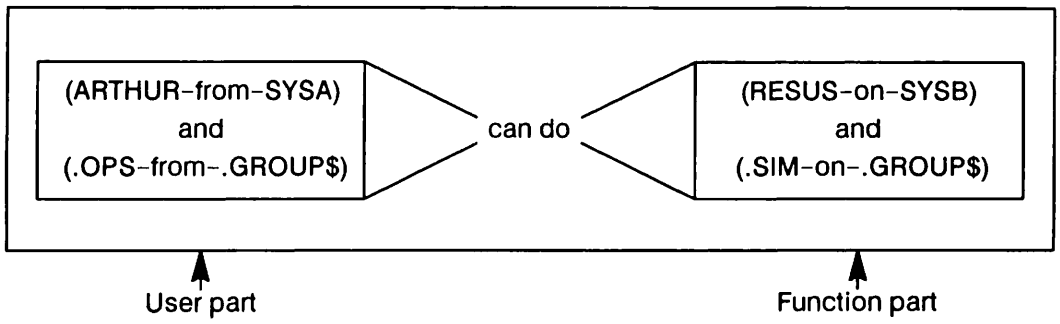

FIGURE 1-2 Essential Elements of a User Access Definition

User access definitions are activated, together with the rest of the configuration, when DSM starts up on a node. For details of how to create and modify user access definitions in the configuration, see Chapter 4, Configuring DSM.

The User's View of User Access Definitions

Users need have no knowledge of the user access definitions under which they operate. If they have no access to CONFIG_DSM in order read the loaded configuration file, they are only aware of which DSM commands they can execute, and on which nodes.

Typical Uses of User Access Definitions

The user access definition mechanism is flexible. It allows you to control access to DSM facilities by user ID, function, and location, in any combination.

For example, you can define user access definitions to reflect different job functions. You might set up an access definition called ADMINISTRATOR for administrative personnel which allows access to all DSM commands and facilities, including those which allow you to alter the configuration file and redistribute it. An access definition OPERATOR that gives access to RESUS and SIM commands might be appropriate for senior operators, and a default definition OTHER_USERS for normal time-share users, that gives access, say, to a limited set of SIM commands on the local node.

DSM provides you with the preset user access definitions DSM_ADMINISTRATOR$ and DSM_OPERATOR$ in the default configuration supplied with DSM. For a listing of the default configuration file, see Appendix A. These user access definitions anticipate the supervisory and operating functions of a typical Prime installation. To customize them for your own installation, simply include the real user IDs and node names that apply to your own system. Alternatively, define new user access definitions to cater for your own needs. Examples of both these methods of setting up access definitions can be found in Chapter 4, Configuring DSM.

User Identities

DSM security is based on existing PRIMOS user names and ACL groups that you define through the EDIT_PROFILE utility (for details see the *System Administrator's Guide, Vol. III, System Access and Security*). However, user names and ACL groups are only unique on the local system because EDIT_PROFILE is a system based utility, whereas DSM security must operate across the network. DSM, therefore, needs a mechanism that ensures IDs are uniquely identifiable throughout the network.

Duplicate user IDs are not a problem on networks that share data, cooperate fully in assigning user IDs, and permit Remote File Access (RFA). However, in networked systems where security between nodes is a strong concern and user IDs are assigned separately on each system, users may be able to access restricted files. The solution adopted in Remote File Access is to require that special remote IDs be passed between those nodes that enforce user validation, every time a remote file is accessed (see the PRIMENET *Planning and Configuration Guide*).

DSM adopts a different approach. Rather than insist that the user has to quote a remote ID to use the function on another node, DSM makes users uniquely identifiable over several nodes by qualifying user names and ACL groups with a **home node** identifier.

Consider the following example:

SYSA and SYSB are two nodes in the same DSM configuration group, and do not have RFA configured between them. There is a user ID ARTHUR on both systems, used by Arthur Dent, the senior operator on SYSA, and Denton J. Arthur, a salesman, who logs in on SYSB.

Both systems also recognize an ACL group .SYSTEM that covers administrators and operators.

System	*Login-ID*	*Person*
SYSA	ARTHUR	Arthur Dent, senior operator
SYSB	ARTHUR	Denton J. Arthur, salesman

Suppose you want to define a DSM user access definition OPERATOR so that Arthur Dent, the senior operator on SYSA, can use RESUS on his own machine. If the access definition were:

(ARTHUR) can do (RESUS-on-SYSA)

both individuals would acquire the right to invoke RESUS on SYSA, which is not intended.

DSM identifies users by combining a user ID with the node where they can log in. Using the example above, the user access definition would be:

(ARTHUR-from-SYSA) can do (RESUS-on-SYSA)

By adding the home node to his login ID, ARTHUR (the senior operator on SYSA) becomes known to DSM by the new network-unique ID. Denton J. Arthur, the salesman, cannot now impersonate Arthur Dent on SYSA because DSM cannot recognize ARTHUR, only ARTHUR-on-SYSA.

The home node and target node identifiers can also be node groups. For example, users in the group .SYSTEM can invoke RESUS on all machines in .SYS through the user access definition:

(.SYSTEM-from-.SYS) can do (RESUS-on-.SYS)

Functions and Function Groups

DSM **functions** are the key facilities and commands that are controlled by DSM security. DSM functions are fixed at installation and cannot be altered. For a list of all registered functions refer to any DSM configuration file listing.

Functions have no security significance until they are linked to a node or a node group in the function part of a user access definition. They cannot exist on their own.

The **function group** is a group of functions gathered together under a convenient name for easy reference. They provide you with a convenient shorthand for referring to many functions at once. An example is the predefined function group .SIM$ which contains all the SIM commands and private logger.

Functions and Commands

Each DSM command has a corresponding function or functions by which it is known to DSM security, and through which users' access to it is controlled. Functions can correspond to a specific command line (for example, the RESUS_STATUS function restricts a user to the command line RESUS -STATUS), or to a DSM-supplied service, such as logging, which is controlled by the PRIVATE_LOGGER and SYSTEM_LOGGER functions. For example, to use the DISPLAY_LOG and ADMIN_LOG commands and the -PRIVATE_LOG and -SYSTEM-LOG options on SIM commands, a user must have access to the functions PRIVATE_LOGGER and SYSTEM_LOGGER.

Table 2-1 lists DSM commands, and the corresponding DSM functions that control user access.

TABLE 2-1 DSM Commands and Their Corresponding Functions

Command	*Function(s)*
ADMIN_LOG	PRIVATE_LOGGER/SYSTEM_LOGGER
CONFIG_DSM	-
CONFIG_UM	CONFIG_UM
DISPLAY_LOG	PRIVATE_LOGGER/SYSTEM_LOGGER
DISTRIBUTE_DSM	DISTRIBUTE_DSM
LIST_ASSIGNED_DEVICES	LIST_ASSIGNED_DEVICES
LIST_ASYNC	LIST_ASYNC
LIST_COMM_CONTROLLERS	LIST_COMM_CONTROLLERS
LIST_CONFIG	LIST_CONFIG
LIST_DISKS	LIST_DISKS
LIST_LAN_NODES	LIST_LAN_NODES
LIST_MEMORY	LIST_MEMORY
LIST_PRIMENET_LINKS	LIST_PRIMENET_LINKS
LIST_PRIMENET_NODES	LIST_PRIMENET_NODES
LIST_PRIMENET_PORTS	LIST_PRIMENET_PORTS
LIST_PROCESS	LIST_PROCESS
LIST_SEMAPHORES	LIST_SEMAPHORES
LIST_SYNC	LIST_SYNC
LIST_UNITS	LIST_UNITS
LIST_VCS	LIST_VCS
RESUS	RESUS/RESUS_STATUS
START_DSM	-
STATUS_DSM	STATUS_DSM
STOP_DSM	-

START_DSM, STOP_DSM and CONFIG_DSM commands are not controlled by DSM security. START_DSM and STOP_DSM can only be invoked at the supervisor terminal and CONFIG_DSM is a PRIMOS operator command.

Other Functions

Other functions are also listed in the configuration file. These relate either to PRIMOS operator commands that use DSM networking and security services or facilities provided by Prime products that may be installed on your system.

For details of the PRIMOS commands, see the *PRIMOS Commands Reference Guide* and the *Operator's Guide to System Commands.*

For details of how specific Prime products use DSM, see the product documentation.

Nodes and Node Groups

DSM **nodes** are simply PRIMENET nodes in your network configuration.

A **node group** is a group of PRIMENET nodes that you define in order to address related nodes collectively. You can use node groups in user access definitions and in the -ON <node-ID> option permitted by some commands. Generally, you can use node groups in all situations where you can use single nodes.

Node groups can be a subset of nodes on the network. They are not constrained by the current network configuration or by the configuration group. They can be subsets or supersets of configuration groups, identical with them or contain mixtures of nodes from several configuration groups.

There is no restriction on the size of a node group but if you use large groups there may be implications for network performance. For further consideration of these issues, see section Configuration Planning Notes, in Chapter 4.

You can nest node groups within other node groups to any level, except where this would lead to recursion. The CONFIG_DSM utility prevents you from creating node groups that refer to themselves.

Node groups are unique entities; access to one does not imply access to others which just happen to be subsets of it. For example, if ABC contains the nodes A, B, and C, and AB contains nodes A and B, then access to group ABC does not imply access to groups AB.

Node groups have no inherent security significance. Until they are used in user access definitions they are simply a list of nodes you define on your own installation and for your own convenience.

Product Register

When you issue the START_DSM command, the identities of all Prime and customer products that use DSM services are passed to the DSM server. The customer product information is contained in the **product register**; this register is part of the standard DSM configuration file which you set up using the CONFIG_DSM command. The product names chosen must

conform to the PRIMOS standards for filenames. Details on setting up a Product Register are given in the section MODIFY the Configuration, Option 6, Definition of the PRODUCT Register, in Chapter 4.

The Prime product information is contained in the following file and cannot be modified:

DSM* > CONFIG_FILES > PRIME_REGISTER.CONFIG,

Unsolicited Message Handling

Unsolicited Message Handling (UMH) is the DSM facility that filters and routes event messages in a networked environment. It enables System Administrators to redirect event messages of particular types to local and remote destinations. Messages, identified by origin and severity, are directed to log files, users, and terminals on assigned lines. The UMH is primarily intended to deal with alarm and warning messages from software modules and subsystems, including PRIMOS, PRIMENET, and DSM.

The routing of all DSM unsolicited messages on a system is controlled by a database consisting of user-defined UMH **selections** that you define by using the CONFIG_UM command. Messages that are not routed through any selection are logged in the UMH Default Log.

DSM provides examples of how unsolicited message handling can be configured on a system, in the selections PRIMOS.LOG, NETWORK.LOG and CONSOLE, that are supplied on the Master Disk in order to log messages from PRIMOS and PRIMENET. They demonstrate how the UMH can be used and can be modified in any way that you wish.

For details of the CONFIG-UM command and how to use it to create and modify selections see Chapter 5, UMH Configuration.

Figure 2-3 shows the main components of DSM unsolicited message handling.

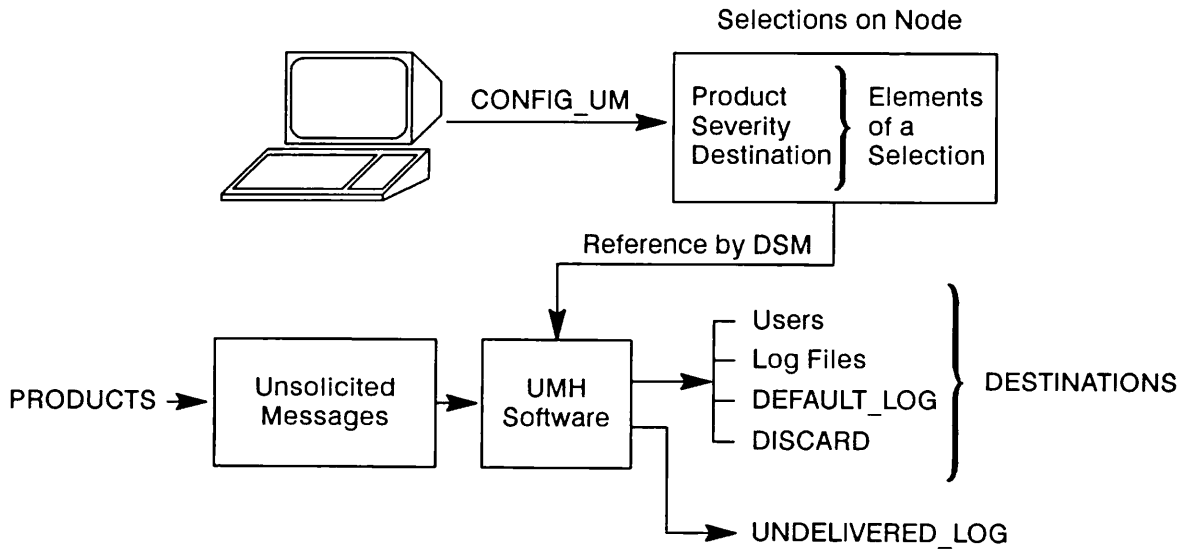

FIGURE 2-3 Unsolicited Message Handling

Selections

A UMH selection consists of a set of user-defined criteria that control the routing of specific messages to destinations such as log files, users and terminals. It consists of a list of products and message severities, linked to specific destinations. The selections that you configure on a system collectively form the database that determines where all unsolicited messages that are generated on that system will be sent.

Products are the registered senders of Unsolicited Messages, and can be any type of systems management software whether Prime or customer originated. A list of Prime registered products can be found in Appendix B. **Severities** are a set of keywords that indicate the importance of the event that caused the message to be sent. **Destinations** are the targets to which the selected messages are sent. DSM private and system logs, users, terminals on assigned lines, and the special destination called DISCARD, are all valid destinations.

For an example of how to set up a selection, see Chapter 5, UMH Configuration.

UMH Configuration

CONFIG_UM is the command that configures unsolicited message handling on a system. You can use it to create, modify, delete, and list selections on local and remote systems. For details of the CONFIG_UM command and how to use it, see Chapter 5, UMH Configuration.

The Destination DISCARD

The DISCARD destination in a selection forces a message to be discarded in that selection.

Note

Messages are often covered by more than one selection. For a message to be truly discarded from the system, *all* selections that apply must specify the DISCARD destination.

Messages With No Configured Destinations

Unsolicited messages for which there is no specified destination, and those that fail to be delivered, are written to special DSM system logs: the default log and the undelivered log. These logs are located in the system logging directory on the system where the message is generated.

The default log (pathname DSM* > LOGS > UMH > DEFAULT.LOG) records messages that have not been redirected to any destination. The undelivered log (pathname DSM* > LOGS > UMH > UNDELIVERED.LOG) records messages that could not be delivered because of a communications breakdown, or insufficient access rights.

The default and undelivered logs are local system logs. To purge them or modify their attributes use the ADMIN_LOG command, and to display them use the DISPLAY_LOG command. For details of both commands, see Chapter 6, Log Administration and Display.

Security and UMH Configuration

Access to the CONFIG_UM command is controlled by DSM security, through the corresponding DSM function CONFIG_UM. The command CONFIG_UM is primarily for administrators and operators, because it confers the power to redirect messages to logs and users throughout the configuration group, and to discard messages altogether. You should therefore restrict the CONFIG_UM command to administrative personnel only. There is no additional security; once a selection is configured on a system, it remains in force until you modify or delete it using the CONFIG_UM command.

System and Network Event Logging

From PRIMOS Rev. 21.0, software event logging on Prime systems is performed through DSM. System and network event messages are passed to the unsolicited message handling system via the DSM System Manager, from where it becomes the responsibility of the System Administrator to route messages to log files, users or assigned devices, using the CONFIG_UM command to set up UMH selections. For further details of the event logging mechanism, see the section Software Event Logging, later in this chapter.

Disk Error Messages

From PRIMOS Rev. 21.0, disk error messages, in common with all system event messages, are passed to DSM as unsolicited messages, and can be directed to log files or users in the normal way.

DSM provides an example of how you might handle disk errors, in the form of the example selection CONSOLE. For details, see later in this chapter.

Sending Unsolicited Messages from Customer Products

You can include customer products in the DSM configuration using the CONFIG_DSM command. You can then use the CONFIG_UM command to configure UMH selections which include these customer products. This command issues separate prompts for the names of either Prime or customer products. See Chapters 4 and 5 for details of registering customer products and using them in UMH selections.

The subroutine DS$SEND_CUSTOMER_UM can then be incorporated into these products, to allow them to send unsolicited messages. See Appendix C for details of this subroutine.

DSM Logging

DSM provides a logging service to the unsolicited message handling system and SIM commands. The service enables messages to be recorded in log files throughout the network. Logs are structured binary files that you create, administer, and display using DSM commands.

With SIM commands, you can store output displays in log files using the general SIM options -PRIVATE_LOG and -SYSTEM_LOG. For details of the logging options see Chapter 7, System Information/Metering.

With unsolicited message handling, you can specify private or system logs as destinations for unsolicited messages. This forms the basis of Prime's software event logging system.

Log Administration and Display

All event logs generated after Rev. 21.0 are DSM system logs, which you control, administer, and display using DSM commands. Two commands allow you to do this: ADMIN_LOG and DISPLAY_LOG.

ADMIN_LOG allows you to create DSM logs, define and modify them, and perform maintenance tasks such as message purging and file deletion. By modifying log file attributes you can

- Monitor log growth
- Control log growth
- Protect logs against quota and disk constraints
- Configure automatic log overflow handling

For further details, see later in this section.

DISPLAY_LOG allows you to list the contents of DSM logs at your terminal, or write them to disk file. Messages can be selected from logs by the product, user, and node that originated them, by their severity, and on their date/time stamp. Options allow you to display messages in summary, tabular, or full format. To print a log, you write the output from the DISPLAY_LOG command to disk file, and print the file.

For details of both commands, see Chapter 6, Log Administration and Display.

Private and System Logs

DSM logs are structured binary files and are of two types: private logs and system logs.

Private logs and system logs differ in the way users' access is controlled, and in how they are located within the file system. Access to system logs is controlled by the function SYSTEM_LOGGER, and access to private logs by the function PRIVATE_LOGGER.

To provide protection for sensitive information, you can record it in a system log and restrict access to it using DSM security. In addition, system logging uses a uniform directory structure on all nodes, and allows event logs to be administered more easily on a network.

Private logging allows users to have access to the logging facilities of DSM on their own directories.

Private Logs: Private logs can be created and maintained on any PRIMOS directory to which a user has access. The right to use a private log depends both on the ACLs on the directory, and on access to the PRIVATE_LOGGER function (see below). To create, modify and display their own private logs, users must also have access to the ADMIN_LOG and DISPLAY_LOG commands.

Note

User DSM_LOGGER (the DSM logging server) must have ALL access to all private logs on the system, and to the directory that contains them.

Private logs are specified in the same way as any PRIMOS file, using either a complete pathname, or a pathname relative to the current attach point. Thus, given the correct ACL rights, users have access to any private log on the system, and to logs that are visible to them through Remote File Access.

Private logs are created automatically if they do not already exist.

System Logs: System logs are also specified using a PRIMOS pathname. Because only one system logging directory is ever active on the system at one time, a disk partition name is not required and should not be supplied. On the logging partition that is active on a system, system logs can only exist as files or pathnames relative to DSM*>LOGS.

System logs must be created before use; unlike private logs, they are not created automatically when you specify the appropriate option.

System logs have a uniform directory structure throughout the network. This enables you to store the same system information in the same place, and in the same form, on every node, and makes it easy to collate and manipulate system information for a whole network.

Security on DSM Logs

All DSM logs, including system logs, can be protected by ACLs on the file or directory. DSM provides additional security on the logging facility itself, through the PRIVATE_LOGGER and SYSTEM_LOGGER functions.

To use private logging and system logging on a system, a user must have access to the functions PRIVATE_LOGGER and SYSTEM_LOGGER, through an appropriate DSM user access definition.

Caution

Users who have access to system logs on remote nodes through DSM security are not subject to normal network security through Remote File Access. For this reason, restrict the use of system logging to trusted personnel.

Only the DSM server (DSMSR) and the DSM logging server (DSM_LOGGER) need full access to DSM*>LOGS. This is a way of ensuring maximum security on system logs, because you can exclude all other users. If you grant only this minimum level of access to the

DSM server processes, users are denied access to the logs unless they have access to the SYSTEM_LOGGER function through an appropriate user access definition; access to the files by other routes, for example through PRIMOS commands, is denied.

Uses of Private and System Logs

For system information that needs to be kept in a common area, but protected against unauthorized access, use a system log. A good example is the use of system logs in software event logging.

Private logs are useful with SIM commands, to save a permanent record of the display for later examination. They are especially useful in combination with periodic execution, to gather and record data at regular intervals over a period of time.

Log File Attributes

All DSM logs are assigned a set of **attributes** that can be used to monitor and limit log growth. These are as follows:

- Maximum Size
- Minimum Size
- Warning Level
- Message Retention Time
- Purge Time
- Cyclic/Linear

Attributes can be specified using the ADMIN_LOG -CREATE command and altered using the ADMIN_LOG -MODIFY command. For details of the commands and default attributes, see Chapter 6, Log Administration and Display.

For details of how attributes can be used in log management and maintenance, see later in this section.

Backup and Recovery

Because DSM logs are PRIMOS files, they can be saved as part of your normal backup procedures. You may need to reset the concurrency locks on DSM logs after restoration from disk or tape (see below).

For extra security, you can make periodic dumps of log contents to disk using the DISPLAY_LOG write-to-file option. For details of this, see Chapter 6, Log Administration and Display.

Concurrency Locks on DSM Logs

The ADMIN_LOG command sets the read/write lock (RWLOCK) on DSM logs at creation to NONE, that is, the file can be read and written simultaneously by any number of users.

Caution

Commands such as COPY and the backup utilities may not preserve the concurrency lock on a log. If you use these or other PRIMOS commands to manipulate logs, you should reset RWLOCK to NONE before you use the DISPLAY_LOG and ADMIN_LOG commands. Only DSM commands guarantee to preserve a log's RWLOCK status.

Using FIX_DISK on Logging Directories

When you run FIX_DISK on a partition that contains DSM logs, it disables logging on the whole of that partition. If messages arrive for logging while FIX_DISK is active, they are recorded in the undelivered log at:

DSM* > LOGS > UMH > UNDELIVERED.LOG).

Notes

When FIX_DISK is run on the partition that contains DSM*, the undelivered log is itself unavailable. If you need to run FIX_DISK on this partition, first stop DSM, and then restart DSM when the fix is complete.

Selected essential event messages that arrive for logging when DSM is stopped are displayed instead at the supervisor terminal. Thus, although messages are not logged in the normal way, they are not discarded altogether.

Monitoring Log Growth

You can set a warning limit to inform you of approaching log saturation. This enables you to take appropriate action in advance of log overflow, such as to increase the maximum size limit, or purge the log of out-of-date messages.

When the warning limit is reached, a DSM unsolicited message with a severity of WARNING is generated. The message can be displayed at your terminal, or directed to a log file of your choice, using an appropriate UMH selection.

Note

You can only set warning limits on logs where a maximum size has already been set. This applies to all cyclic logs, for which you *must* specify a maximum size.

Controlling Log Growth

To prevent logs from growing indefinitely and consuming too much disk space set appropriate values for the following attributes:

- Maximum size
- Retention time

Maximum Size: This attribute sets a maximum size in disk records beyond which the log is not permitted to grow. Whether messages are discarded or old messages are overwritten when the limit is reached, depends on whether the log is cyclic or linear. If it is cyclic, new messages overwrite old messages on the log, and if it is linear, new messages are discarded and the log is closed (see Dealing With Log Overflow, below).

Retention Time: You can set a retention time for messages in a log to ensure that logs are purged automatically at the same time every day. To specify when the purge should take place, set an exact time of day using the -PURGE_TIME attribute.

You can also control log growth by deleting out-of-date messages using the ADMIN_LOG -PURGE command.

Note

Linear logs with maximum size set to *unlimited* and message retention time to *indefinite* should be purged regularly, or they will grow indefinitely.

Reserving Disk Space for Logs

Use the minimum size attribute to reserve an area on disk for logs that gather important information. This ensures that crucial information is recorded whatever the disk quota constraints, and whatever applications and subsystems are running.

For example, you might set a minimum size on logs that gather important information about how your system and network is behaving.

Dealing With Log Overflow

You can specify how log overflow is handled using the **cyclic** and **linear** log file attributes.

When cyclic logs reach their maximum size, new messages successively overwrite the oldest messages on the log, in first-in, first-out date order, so that you risk losing old messages at the expense of newer ones. It is therefore best to use cyclic logs to record information that has a limited lifetime.

When linear logs reach their maximum size new messages are discarded, the log is closed, and no more messages can be added until you make more space available by deleting existing messages, or by raising the maximum size limit. In linear logs therefore, existing messages are retained, and you risk losing the most recent. Use linear logs when you need to ensure that information is retained for any length of time, for example to record the behavior of a device over a period of time, and to store it for later analysis.

With both types of log, an unsolicited message is generated with a severity of ALARM when the log reaches saturation. The message can be displayed at your terminal, or directed to a log file of your choice, by defining an appropriate UMH selection. The message is repeated every 60 minutes, provided there is logging activity, until you purge the log.

You can also set a warning level on the log to notify you of approaching saturation. When the warning level is reached, an unsolicited message is generated with a severity of WARNING.

Software Event Logging

From PRIMOS Rev. 21.0, software event messages from PRIMOS and PRIMENET, formerly logged to LOGREC* and NETREC*, are logged to DSM as unsolicited messages. The mechanism works in the following way.

Messages are received from PRIMOS and PRIMENET by the DSM System Manager process. The System Manager translates messages from the internal format to standard DSM message format, and passes them on to DSM as unsolicited messages. At this point they become the responsibility of the System Administrator, to be directed to log files or users through the CONFIG_UM command.

DSM supplies some selections on the Master Disk, that you can use as templates for configuring message handling on your own system. These are no more than *advisory*, and Prime does not insist that you use them; you should treat them as examples and templates rather than as fixed parts of the system.

You can modify the example selections and their related logs in any way you wish. You can modify them in order to route messages to log files of your own creation, display them to users, or direct them to assigned lines. You can even delete them and create new ones to suit the practice at your own installation.

Example Selections

The selections that Prime supplies as examples are called PRIMOS.LOG, NETWORK.LOG, and CONSOLE. To list them at the terminal, use the CONFIG_UM -LIST command.

The PRIMOS.LOG and NETWORK.LOG selections route event messages from PRIMOS and PRIMENET respectively to system logs. PRIMOS messages are recorded in the file DSM* > LOGS > PRIMOS > PRIMOS.LOG and PRIMENET messages in the file DSM* > LOGS > NETWORKS > NETWORK.LOG. All other messages are routed to the default log, DSM* > LOGS > UMH > DEFAULT.LOG

Both files are created when DSM is installed on the system, and are assigned default values for all attributes. To view the files use the DISPLAY_LOG command, and to modify, delete and purge the files use the ADMIN_LOG command. For further details of log file attributes and the two commands, see Chapter 6, Log Administration and Display.

The CONSOLE selection displays all disk errors at the supervisor terminal, by routing them to User 1.

Shown on the next page are listings of the selections PRIMOS.LOG, NETWORK.LOG, and CONSOLE. For details of how to modify and create selections, and for descriptions of products, severities, destinations, and their meanings, see Chapter 5, UMH Configuration.

```
Selection Name: PRIMOS.LOG
Prime Product: LOG_COLD
Prime Product: LOG_SEG4
Prime Product: LOG_DISK
Prime Product: LOG_TAPE
Prime Product: LOG_MISC
Prime Product: LOG_UNKN
Prime Product: LOG_OVFL
Severity: -ANY
Destination: LOGGER DSM*>LOGS>PRIMOS>PRIMOS.LOG -SLOG

Selection Name: NETWORK.LOG
Prime Product: NPX
Prime Product: PRIMENET
Severity: -ANY
Destination: LOGGER DSM*>LOGS>NETWORKS>NETWORK.LOG -SLOG

Selection Name: CONSOLE
Prime Product: LOG_DISK
Severity: -ANY
Destination: DISPLAY -USER 1 -FMT FULL
```

Displaying and Printing Event Logs

To display event logs at your terminal, or write them to disk file, use the DISPLAY_LOG command. Options allow you to select messages for display by type, origin and severity, and to display them in different formats. To print an event log, simply write the output from the command DISPLAY_LOG to a file, and print the file.

For details of the DISPLAY_LOG command and examples of how to use it, see Chapter 6, Log Administration and Display.

Configuring Event Logging on Your System

The following sections describe briefly how to modify event logging to suit the needs of your system and network.

Rerouting Event Messages: To redirect event messages to other log files, users, and terminals on assigned lines, you can modify the example selections PRIMOS.LOG and NETWORK.LOG, or create new selections of your own, using the CONFIG_UM command.

For example, you could force all PRIMOS messages to be displayed at your terminal by adding the following destination to the selection PRIMOS.LOG:

DISPLAY -USER <your username/usernumber>

If you were interested in cold starts only, you could restrict the display to cold-start messages by creating a *new* selection to route messages from the Prime product LOG_COLD, of any (-ANY) severity, to the destination DISPLAY -USER *username/usernumber.*

Modifying Event Log Attributes: To control log growth, ensure adequate disk space, and deal with log overflow through the modification of log file attributes, use the ADMIN_LOG command.

For a description of how to control log growth and prevent message loss and overflow, see the section DSM Logging, earlier in this chapter. For a full description of the ADMIN_LOG command, see Chapter 6, Log Administration and Display.

3

STARTUP AND OPERATION

Introduction

This chapter describes DSM installation, subsystem operation, monitoring and maintenance, startup and shutdown, and the structure and contents of the DSM* directory.

Installing DSM

DSM is supplied on the PRIMOS Master Disk, but requires some additional installation tasks to be carried out once the Master Disk is mounted and PRIMOS is running. Before you start the installation, it may be necessary to set a priority ACL using the SPAC command, to ensure that you have sufficient access rights to the disk. You run the program SYSTEM>DSM.INSTALL.CPL to complete installation of DSM. This program installs the DSM configuration and data files, sets the correct ACLs throughout the directory tree, and amends the system subroutine search rules.

First-Time Startup

Before starting DSM on a new system, you must first run the install program (see above). If you now issue the START_DSM command, DSM starts up under certain configuration defaults, as follows:

- User access to commands, and the ability to invoke commands on remote systems, are configured according to the configuration file DSM*>CONFIG_FILES>DSM_DEFAULT.CONFIG. which is the DSM default. In this configuration:
  - DSM commands can be invoked only by the System Administrator.
  - DSM commands can be invoked only on the local system.
  - Reconfiguration from other nodes is not permitted.

- PRIMOS and PRIMENET event logging is controlled by the UMH selections PRIMOS.LOG and NETWORK.LOG. Messages are directed to SYSTEM logs:
  - DSM* > LOGS > PRIMOS > PRIMOS.LOG
  - DSM* > LOGS > NETWORKS > NETWORK.LOG.
- All other unsolicited messages are logged in DSM* > LOGS > UMH > DEFAULT.LOG, which is the UMH Default Log,

To view the default DSM configuration, use the LIST option within the CONFIG_DSM command environment.

To view the example selections, use the CONFIG_UM -LIST command.

The configuration defaults are adequate for the initial testing of DSM on the system, and during familiarization with the product. If your system is not part of a network, and you intend to restrict the availability of DSM commands to machine room staff, the default configuration may also be adequate for normal operation.

To allow commands to be invoked remotely, and to grant wider access to them, you must define a new configuration and distribute it on the network. When doing this for the first time, you must follow a special procedure.

For details of how to define a new configuration, and how to configure DSM on a network for the first time, see Chapter 4, Configuring DSM.

To modify event logging for your system use the CONFIG_UM and ADMIN_LOG commands to change example selections and system log files. For a discussion of the ways in which you can alter event logging, see the section Software Event Logging, in Chapter 2.

The DSM Subsystem

Server Processes

DSM is controlled by the following server processes:

- DSM server (user DSMSR)
- Logging Server (user DSM_LOGGER)
- System Manager (user SYSTEM_MANAGER)
- Application Servers (user DSMASR)

Users DSMSR, DSMASR, DSM_LOGGER, and SYSTEM_MANAGER are members of the ACL group .DSM$.

DSM Server: The DSM server on a node runs the core software of DSM, including networking to remote nodes and DSM security. By cooperating with DSM servers on other nodes, it invokes DSM commands remotely, controls user access, and ensures secure message exchange.

Logging Server: The logging server controls the reading, writing, administration and display of DSM logs.

Note

If no DSM commands are being invoked, the DSM server and the logging server are idle, and use a minimum of system resources.

System Manager: The System Manager controls the transfer of PRIMOS and PRIMENET event messages from the operating system to the DSM unsolicited message handling system.

If the System Manager is not running, event logging cannot take place. Messages are displayed instead at the supervisor terminal.

Application Servers: Application servers control the invocation of DSM commands and services. They are spawned by the DSM server as privileged phantom processes under the user name DSMASR. Application servers are started and stopped as required to invoke commands and service user requests. The number of application servers running on a system at any one time depends on the performance of your system, and how many DSM commands are being invoked.

Note

You should reserve enough phantom processes at cold start for the number of DSM commands you wish users to invoke simultaneously on your system. Each command requires one DSMASR, and each DSMASR requires a phantom process. The more phantoms you reserve, the more DSM commands can be executed simultaneously.

The DSM Text Database

Text for all DSM messages and displays is held in a central database. From Rev. 22.0, this database consists of language files in the directory DSM*>SIT_TEXT_DBS.

Language files have the general filename DSM_*language*.TDIMG, where *language* is the code for the language version in use. The default language is USA, for which the language file is DSM_USA.TDIMG.

The text database is a read-only file. In the unlikely event of the file becoming corrupted, you must restore it from backup store.

Starting DSM

To start DSM on the system, use the START_DSM command. START_DSM is a supervisor terminal command. The command and its options are described below.

▶ **START_DSM [options]**

The START_DSM command starts DSM on the system. It starts the server processes that control and run DSM, and initializes the DSM message text database.

Descriptions of the options follow.

Option	*Description*
{-RETAIN_ASRS / -ASRS} [nn]	Allows you to specify how many free (idle) DSM application servers remain logged in indefinitely on the system. *nn* is an integer number in the range 0 to 10 inclusive. The default value is 1. Any free DSMASR's in excess of the number *nn* will log out once the timeout period is exceeded. The optimum value for *nn* depends on how much DSM is used; the less it is used, the lower is the requirement for free ASR's. Further details on retaining application servers on the system are given in the section Retaining Application Servers, later in this chapter.
{-HELP / -H} [{-NO_WAIT / -NW}]	Explains how to use the command. This option cancels any other options on the command line. If you specify -NO_WAIT, the display is not paginated at your terminal. The same information is available through the PRIMOS HELP subsystem.
-USAGE	Gives you the command syntax in brief. This option cancels all others on the command line.

START_DSM is normally included in the system cold-start file PRIMOS.COMI, but it can also be issued at any time, for example when you restart DSM after fault finding or maintenance. In the PRIMOS.COMI file, START_DSM should *follow* the command that adds the local disks, so that the product directory is in place when the subsystem starts. It should also *precede* the START_NET and COMM_CONTROLLER commands, so that DSM is ready to log error messages from PRIMENET and the communications controllers should they occur.

For details of PRIMOS startup, and the composition of the PRIMOS.COMI template, see the *System Administrator's Guide, Vol. I, System Configuration* and the appropriate manual for your processor.

Startup Files

The START_DSM command normally loads the *restart* configuration file, pathname DSM*>CONFIG_FILES>DSM_RESTART.CONFIG. If this file is corrupt or out of date with respect to the configuration that was last loaded, the *default* configuration file, pathname

DSM* > CONFIG_FILES > DSM_DEFAULT.CONFIG is loaded instead. If the default configuration file is invalid, DSM cannot start.

The Startup Sequence

As DSM starts on the system, the following message is displayed at the supervisor terminal:

```
DSM initialization started.
```

The DSM server process (user DSMSR) is now being started on the system. Once this point is reached, DSM startup cannot be aborted using CONTROL-P.

When DSM initialization is complete, the following message is displayed:

```
DSM Server is now in steady state.
```

The DSM server is now running on the system. The configuration file has been loaded, and the configuration that it represents is active on the system.

The steady state message is also sent as an unsolicited message (product DSM, user DSMSR, severity INFORMATION) You can direct the message to a log, user, or terminal of your choice using the CONFIG_UM command (see Chapter 5, UMH Configuration).

Finally, the DSM logging server (user DSM_LOGGER) and the System Manager process (user SYSTEM_MANAGER) are started. This may take a few seconds to complete.

When the System Manager and logging server are both running, system event logging is fully active, and users can invoke DSM commands. The SYSTEM_MANAGER will continue running until the DSM_LOGGER process fails. You need only intervene if you want to reconfigure DSM on the network, change access rights, or modify event logging. For details of how to configure DSM and set access rights, see Chapter 4, Configuring DSM, and for a description of software event logging, see Chapter 2, Administration and Security.

Failure to Start

If DSM fails to start correctly, you are notified by a message at the supervisor terminal. Issue the STOP_DSM command to clear the system of DSM processes, and reissue the START_DSM command when all the processes have logged out.

Retaining Application Servers

Whenever a DSM command is executed, and there is no free DSMASR, a new one is created. The overhead in creating this DSMASR results in a slower response time. Thus, the DSM response time is improved if there is a free DSMASR available for use. By using the RETAIN_ASRS option when you issue the START_DSM command, you can increase the probability of there being a free DSMASR on the system when a DSM command is issued.

The number of free application servers you should retain depends on how much DSM is used on the system. If usage is low, the requirement for DSMASRs is reduced, and the timeout period before a free DSMASR logs out is longer. Having more free application servers available for use than are required does increase unnecessarily the number of processes on the system.

Note

Application servers must be created to service the first DSM commands executed after DSM is started, so the use of the RETAIN_ASRS option does not result in improved performance during the initial period after DSM startup.

Warm Start

A PRIMOS warm start eliminates all current network connections, including DSM connections to remote nodes. Commands that are being invoked on remote nodes are aborted, and are not recovered when PRIMOS restarts.

You do not need to restart DSM when PRIMOS is warm started.

Stopping DSM

To stop DSM on the system, use the STOP_DSM command. STOP_DSM is a supervisor terminal command.

The command and its options are described below.

▶ **STOP_DSM [options]**

The STOP_DSM command shuts down DSM on the system by logging out the DSM processes.

Descriptions of the options follow.

Option	*Description*
{-HELP / -H} [{-NO_WAIT / -NW}]	Explains how to use the command. This option cancels any other options on the command line. If you specify -NO_WAIT, the display is not paginated at your terminal. The same information is available through the PRIMOS HELP subsystem.
-USAGE	Gives you the command syntax in brief. This option cancels all others on the command line.

When you issue the STOP_DSM command, the following message is displayed at the supervisor terminal:

```
DSM shutdown is in progress
```

It may take a few minutes for DSM shutdown to complete, while files are closed. When these operations are complete, the DSM processes log out.

Notes

STOP_DSM terminates active DSM sessions. Any commands that are executing at the time are aborted.

STOP_DSM disables event logging. While DSM is stopped, some event messages are displayed at the supervisor terminal instead.

The Directory DSM*

DSM* is DSM's product directory. It is a top-level directory that contains:

- Runfiles for the DSM and application servers
- Directories for the applications software, databases for DSM and UMH configuration, DSM logs and journals, and the display format files for SIM command output

The structure of the DSM* directory is fixed at installation and should not be changed.

Figure 3-1 shows the structure of DSM*. Tables 3-1 and 3-2, describe the contents of DSM* and DSM*>LOGS, and indicate the minimum access rights for DSM server processes.

Minimum ACLs

Note

For DSM to work correctly, users SYSTEM, DSMSR, DSM_LOGGER, and DSMASR need at least Use (U) access to DSM*.

Resetting ACLs

Recommended ACLs are set on DSM* by the DSM install program that you run to install DSM on the system. If you need to reset them at any time, for example, if they have become corrupted, run the program SYSTEM>DSM.INSTALL_ACL.CPL.

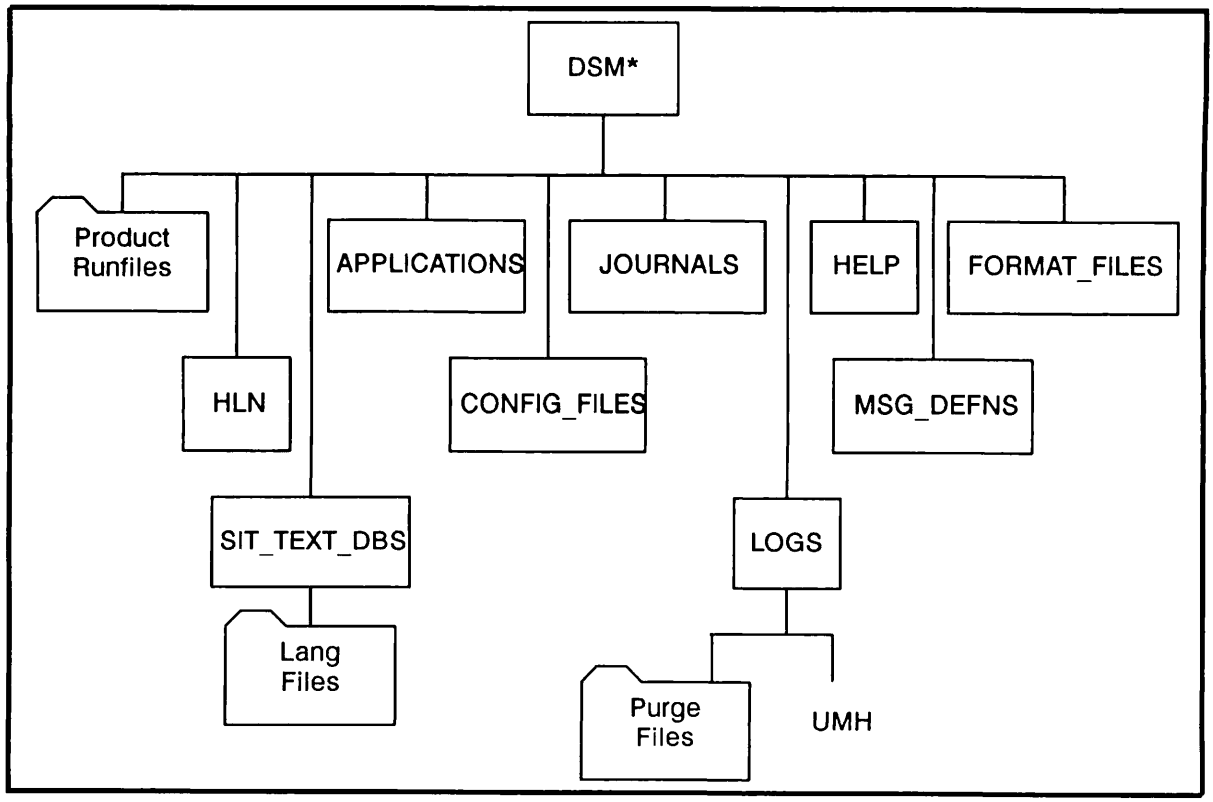

*FIGURE 3-1 Contents of the Directory DSM**

*TABLE 3-1 Files and Subdirectories in DSM**

File	*Contents*
DSMSR.CPL	The command runfile that invokes the DSM server. User SYSTEM and the DSM server need UR (read) access.
DSMSR.RUN	The DSM server runfile. User SYSTEM and the DSM server need UR access.
ASR.CPL	The command runfile that invokes the application server. The DSM and application servers need UR access.
ASR.RUN	The application server runfile. The DSM and application servers need UR access.
CONVERT_LOG.RUN	This utility is used by SYSTEM > DSM.INSTALL.CPL to ensure that system logs are of the latest format prior to starting DSM. Any other types of log which require reformatting are automatically converted by the system so you do not need to run this utility explicitly.
LOGGER_ASR.CPL	The logging server runfile that invokes the DSM logging server. The DSM and logging servers need UR access.

Subdirectory	*Contents*
SYSTEM_MANAGER.COMI	The command file that invokes the System Manager.
START_SYSTEM_MANAGER.RUN	The System Manager startup file.
HLN	The directory that is used by the DSM processes to communicate between each other. The contents should never be modified by the user.
SIT_TEXT_DBS	The directory that contains DSM's message text database. The database consists of language files used by DSM processes to display standard text and information to the user.
APPLICATIONS	The directory that contains the runfiles for all DSM controlled applications software. The DSM application server needs UR access.
CONFIG_FILES	The directory that contains the data files that define DSM Configurations and UMH Selections. DSM_DEFAULT.CONFIG - the Prime-supplied configuration file, that should never be modified. Authorized users of CONFIG_DSM, the DSMSR and DSMASR need UR (use and read) access. DSM_EMPTY.CONFIG - the empty configuration file template, also supplied by Prime. Authorized users of CONFIG_DSM need UR (use and read) access. DSM_LOADED.CONFIG - the configuration file that was loaded at the last startup and which defines the configuration under which DSM is currently running. The DSM server needs URW (use, read and write) access, and the application server needs UR (use and read) access. DSM_RESTART.CONFIG - the configuration file that is loaded at the next startup. The DSM and application servers need URW (use, read and write) access. DSM_UMH.CONFIG - the file that contains user-configured UMH Selection data. The System Manager process needs AURW (add, use, read, write) access. DSM_UMH_DEFAULT.CONFIG - the file that contains example UMH Selection data.

JOURNALS	The directory that contains the error/event journals generated by the DSM and application servers. The DSM and application servers need DAWPU (delete, add, write, protect, use) access to this directory.
HELP	The directory that contains the HELP files for DSM subsystems. Users with access to a subsystem need UR (use and read) access to the corresponding HELP file in DSM* > HELP.
FORMAT_FILES	The directory that contains the format definition files for the DISPLAY_LOG option -FORMAT.
MSG_DEFNS	The directory that contains DSM message structure definitions in binary form.
LOGS	The directory that contains the DSM log administration and purge information for the DSM logging service and sudirectories for the various subdivisions of DSM logs (see Figure 3-2, Files and Subdirectories in DSM* > LOGS). The DSM logging application server (DSM_LOGGER) needs all access to the directory.

TABLE 3-2 Files and Subdirectories in DSM > LOGS*

File	*Contents*
DSM_LG_PURGE_LIST$	This file contains the control and purge information (message retention and purge times) for all DSM log files on the system.
Subdirectory	*Contents*
UMH	This directory contains the default logs for DSM unsolicited message handling. DEFAULT.LOG records unsolicited messages that are not routed elsewhere. UNDELIVERED.LOG records unsolicited messages that could not be delivered because of system or communications failure.

Maintaining DSM*

In maintaining the DSM* directory you must

- Ensure adequate security on DSM command files, runfiles and configuration files.
- Monitor the system logging directory DSM* > LOGS and ensure that it does not consume excessive disk space.
- Restore corrupt configuration files and text database files.
- Reset ACLs on DSM* if they become corrupted.

Protecting Files: Protect the DSM* subdirectories and files against malice or misuse in the same way that you protect other systems.

Monitoring Logs: To ensure that system logs do not consume too much disk space set an appropriate retention time on the log. To delete unwanted messages use the ADMIN_LOG purge facility. For details see the section DSM Logging in Chapter 2 and refer to Chapter 6, Log Administration Display.

Restoring Corrupt Files: DSM configuration files and text database language files are specially protected against inadvertent or malicious misuse. If corruption does occur it is likely to be due to disk failure.

To restore configuration and database files

1. Stop DSM.
2. Logout all users to ensure that no files are open.
3. Restore the files from backup store.

Resetting ACLs: The recommended access rights for DSM server processes are set on DSM* and its subdirectories at installation. To reset ACLs to the recommended defaults run the program SYSTEM>DSM.INSTALL_ACL.CPL.

Minimum ACL settings for files and directories within DSM* are indicated in Table 3-1 and Table 3-2.

Using FIX_DISK on the DSM* Directory

Because FIX_DISK disables logging on a disk partition you should stop DSM before you run FIX_DISK on the partition that contains DSM* (usually the command partition disk 0); if you do not, messages may be lost when the system logging directory DSM*>LOGS is not available. When DSM is stopped, messages are displayed at the supervisor terminal. When FIX_DISK has finished, restart DSM and event logging resumes.

Monitoring and Diagnostic Errors

This section describes some of the tasks involved with monitoring and maintaining DSM on a system. It also describes what to do when there are problems.

The DSM Journals

The DSM journals are the comoutput files for the DSM processes DSMSR, DSM_LOGGER, SYSTEM_MANAGER and DSMASR. They log exceptions, internal errors, startups and shutdowns. DSM journals are kept on the directory DSM*>JOURNALS and are limited to fifty records in size. You can use the journals to monitor DSM's internal events, to track the development of impending problems, or to help in the analysis of faults after the event. They are intended as diagnostic and trace tools, and may require skilled interpretation.

The DSMSR, DSM_LOGGER and SYSTEM_MANAGER journals each consist of three files named after their respective user names. For example DSMR$.1, DSMR$.2, and DSMR$.3. DSM cycles round the three files in turn, overwriting the oldest file in the sequence each time DSM starts up, or when the existing file exceeds fifty records.

In this way DSM maintains a complete record of three invocations of the subsystem (the current and the two previous ones). If the record limit is exceeded, a new journal is opened, and fewer invocations are recorded.

A separate journal file is opened for each application server that is started on the system. This is closed when the system shuts down. Application server journals are prefixed by ASR$ and are allocated a random character string. Application server journals are deleted daily.

Saving Files

If there is a failure in any of the DSM servers you should save the entire contents of the following directories to disk or to tape:

DSM* > CONFIG_FILES
DSM* > JOURNALS
DSM* > LOGS

If possible, also make a note of which command was being invoked when the problem occurred.

Unexpected Errors

Unexpected errors result from inconsistencies in the software. The command aborts and an unsolicited message is generated that describes the error. These messages are normally recorded in the UMH default log pathname DSM* > LOGS > UMH > DEFAULT.LOG, but you can also redirect them to logs, users or terminals of your choice by using the CONFIG_UM command.

Trace and diagnostic information about the error can be found in the DSM and application server journals. To interpret the information you may need to consult your Prime representative.

4

CONFIGURING DSM

Introduction

This chapter describes the procedures that you use to configure DSM on a network. It explains how to define a DSM configuration, how to distribute it on the network, and how to determine configuration status. The chapter ends with a configuration example.

The Installed Configuration

When newly installed, DSM runs the **default** configuration that allows only user SYSTEM to invoke DSM commands, and on the local node only. This configuration is adequate for gaining familiarity with the product, and may be suitable as the permanent configuration on single machines. Only configure DSM if you wish to extend DSM access to include other users, and if you wish to invoke commands over the network.

To run the default configuration, do nothing. The configuration is automatically activated when DSM is first started on the system.

Overview of DSM Configuration

You configure DSM on a system or network by *editing* an existing **configuration file** using the CONFIG_DSM command, and *distributing* the configuration to a group of nodes. The new configuration is activated the next time DSM is started on each system. To distribute a configuration, you use the DISTRIBUTE_DSM command, or, when distributing the first configuration, the COPY or FTR commands.

Note

The Name Service uses the DSM Configuration Group as its Name Space. For further details of the Name Service, see the *System Administrator's Guide, Vol. 1,* and the *Networks Release Notes Rev. 23.*

The STATUS_DSM command allows you to determine configuration status on nodes and node groups.

Distributing the First Configuration

When distributing the first configuration, you must use the COPY command or the File Transfer Service (FTS), rather than DISTRIBUTE_DSM, to install it in the restart configuration file. For example,

```
COPY <LOCAL>WORK>NEW.CONFIG <REMOTE>DSM*>CONFIG_FILES>DSM_RESTART.CONFIG
```

Once the first configuration is in place, you can use DISTRIBUTE_DSM to distribute subsequent configurations.

The first configuration must allow at least one user on the network to invoke DISTRIBUTE_DSM on all nodes in the configuration group, from at least one other node in the group. This ensures that subsequent reconfigurations can be performed using DISTRIBUTE_DSM.

For details of the minimum access that is required in the first configuration, see The DISTRIBUTE_DSM Command, later in this chapter.

Security on the Configurator Commands

CONFIG_DSM: CONFIG_DSM is a regular PRIMOS command, and access to it is controlled in the normal way by ACLs on CMDNC0.

You should restrict access to CONFIG_DSM in the same way that you would control access to operator commands such as EDIT_PROFILE, that enable users to view system data.

Note

CONFIG_DSM is a configuration editing facility. It does not allow users to install a new configuration on the network, which is the function of the DISTRIBUTE_DSM command.

DISTRIBUTE_DSM/STATUS_DSM: Access to the DISTRIBUTE_DSM and STATUS_DSM commands can be controlled in two ways:

- By ACLs on the command runfiles
- By DSM security, using the functions DISTRIBUTE_DSM and STATUS_DSM

Configuration File Security

DSM **Configuration Files** are binary PRIMOS files that contain details of configuration group membership, users' access rights to DSM commands, and other configuration data.

This information should be protected in the same way that you protect all system information, using ACLs. You should ensure that user DSMASR (the application server) has LU access to any master configuration file intended for distribution.

File Maintenance

All DSM configuration files are PRIMOS files. You can use normal PRIMOS commands to copy, rename and delete them.

The CONFIG_DSM Command

CONFIG_DSM is the command you use to create, modify, list, check, and save a configuration.

The syntax of the command is as follows:

▶ **CONFIG_DSM [pathname] [options]**

pathname specifies the name of the configuration file you wish to edit. If none is specified, the system prompts you for the pathname of the required file.

The remaining command-line options are described in the following section.

Command-line Options

Command-line options allow you to set the terminal type so that each menu is displayed on a new screen, and to summon HELP and USAGE information for the command.

Descriptions of the options follow.

Option	*Description*
{-TERMINAL_TYPE / -TTP} **terminaltype**	Specify the *terminaltype* that you are using, so that the screen is cleared before each menu is displayed. Valid terminal types are TTY, PT45, PST100 and PT200. TTY (glass teletype mode) is the default. Supports the global variable .TERMINAL_TYPE$ when -TTP is not specified.
{-HELP / -H} [{-NO_WAIT / -NW}]	Explains how to use the command. This option cancels any other options on the command line. If you specify -NO_WAIT, the display is not paginated at your terminal. The same information is available through the PRIMOS HELP subsystem.
-USAGE	Gives you the command syntax in brief. This option cancels all others on the command line.

Invoking CONFIG_DSM

You invoke CONFIG_DSM from PRIMOS in the normal way. For example:

```
CONFIG_DSM DSM*>CONFIG_FILES>DSM_NEW.CONFIG -TTP PT200
```

If you do not specify a pathname for the configuration file in the command line, you are prompted to enter one. CONFIG_DSM uses the specified file as a template. You can use any valid DSM configuration file, but on installation only the Prime-supplied *empty* and *default* configuration files are available.

If you press the RETURN key when prompted for the configuration file pathname, the default configuration file is used.

When the template file has been read, its revision details are displayed, as in Figure 4-1.

```
Configuration file  : <filename>
Revision number     : <nn>
Last updated        : <date/time>
Updated by user     : <username>
Updated on node     : <nodename>
DSM revision number : <nn>
Comment             : <text>




--Press < RETURN > to continue :
```

FIGURE 4-1 Configuration File Revision Details

Configuration Templates

Prime supplies two configurations that you can use as templates when constructing a configuration, namely, the **empty** and **default** configurations. Subsequent configurations can be constructed from any validated configuration file.

The empty configuration template is represented by the file

DSM* > CONFIG_FILES > DSM_EMPTY.CONFIG

and the default configuration template is represented by the file

DSM* > CONFIG_FILES > DSM_DEFAULT.CONFIG

For listings of the template files, see Appendix A.

The Empty Configuration

The empty configuration is a blank configuration template. It contains only the fixed and reserved entries that are used by DSM security. Fixed entries cannot be modified or deleted. Reserved entries cannot be renamed or deleted, and can only be modified in a limited way. Fixed and reserved entries are present in all DSM configuration files.

Fixed entries are as follows:

- .ANY_NODE$ - represents all PRIMENET nodes.
- .ANY_FUNCTION$ - represents all registered DSM functions.
- .ANY_USER$ - represents all users on the system.

Reserved entries are:

- .GROUP$ - a node group that represents all nodes in the configuration group. Membership is only changed by adding or removing nodes.
- .ALIEN_NODES$ - a node group that represents all nodes from which remote users can invoke commands. Membership is only changed by adding or removing nodes.
- ALIEN$ - the DSM user access definition assigned to users from other configuration groups. Only the function part can be modified.

The Default Configuration

The default configuration defines a base level of user and internode access that you can modify for your own network. The configuration group contains only the local system, and only user SYSTEM can invoke DSM commands. Users outside the group are excluded.

The default configuration runs on any system, and is automatically installed as the running configuration when DSM is first started after installation.

In addition to the fixed and reserved entries, the default configuration contains predefined node groups, function groups, and user access definitions, that you can modify or delete to suit your own installation. These are described below.

Function Groups	*Description*
.RESUS$	Contains the functions RESUS and RESUS_STATUS.
.SIM$	Contains the SIM functions and PRIVATE_LOGGER.
User Access Definitions	*Description*
DSM_ADMINISTRATOR$	Gives the ACL group .SYSTEM_ADMINISTRATOR$ on any node access to ALL commands on any node in the configuration group.
DSM_OPERATOR$	Gives user SYSTEM on the local node access to all SIM commands, and RESUS, on all nodes in the configuration group.

Configuration Initial Menu

To display the configuration initial menu, press the RETURN key once the template configuration file revision details have been displayed.

The configuration initial menu introduces the first level of definition and modification options available with CONFIG_DSM. The menu is illustrated in Figure 4-2.

```
INITIAL menu

Which of the following do you wish to perform?

 (1) MODIFY the configuration.
 (2) CHECK the configuration for consistency.
 (3) SAVE the configuration.
 (4) LIST the configuration.
 (5) HELP.




Enter option number, or press RETURN to leave this menu:
```

FIGURE 4-2 CONFIG_DSM Initial Menu

The following sections describe some aspects of the CONFIG_DSM user interface, and how to interact with it.

Menus and Prompts

You conduct your dialog with CONFIG_DSM through screen menus. Selecting a menu option may produce a further submenu, or may display a prompt to which you should respond.

If you type QUIT (abbreviation Q, upper or lower case) or press the RETURN key on a menu, you return to the previous menu in the hierarchy. The same response to a prompt may display another prompt, or return you to the menu. If you want to use the character q as an identifier, you must enclose it in single quotes, as in 'q'.

Errors and Warnings

Error and warning messages are prefixed by `Error` and `Warning` respectively. In both cases you are returned to the previous menu or prompt.

Help

To summon HELP at any stage in your dialog with any of the three commands, select the HELP option that is present on all menus.

The BREAK Key

You can interrupt dialog with any of the configurator commands at any time by pressing the PRIMOS break key (CONTROL-P). This summons the BREAK Menu, which is illustrated in Figure 4-3.

```
BREAK menu.

The following BREAK options are available:

 (1) Continue.
 (2) Exit to INITIAL menu.
 (3) Exit from <command name>.
 (4) HELP.

Enter option number, or press RETURN to leave this menu:
```

FIGURE 4-3 BREAK Menu

Menu option (1) - `Continue.` - redisplays the menu or prompt that was interrupted when you pressed the BREAK key, and allows you to continue from that point.

Menu option (2) - `Exit to INITIAL menu.` - returns you to the initial menu of the command.

Menu option (3) - `Exit from <command name>.` - returns you to PRIMOS after allowing you to save any outstanding modifications to the file.

Note

If you press CONTROL-P before the template configuration file has been fully read in, you cannot return to the initial menu. In this case selecting, option (2), `Exit to INITIAL Menu` - returns you directly to PRIMOS.

You can quit from CONFIG_DSM at any time by typing QUIT or RETURN on the initial menu. If you do so without first saving your modifications to disk, you are given the opportunity to return to the initial menu where you can use the UPDATE option.

The Menu Hierarchy

CONFIG_DSM contains several levels of menus and submenus. To help trace your path to a particular function within the command, refer to the menu hierarchy in Figure 4-4.

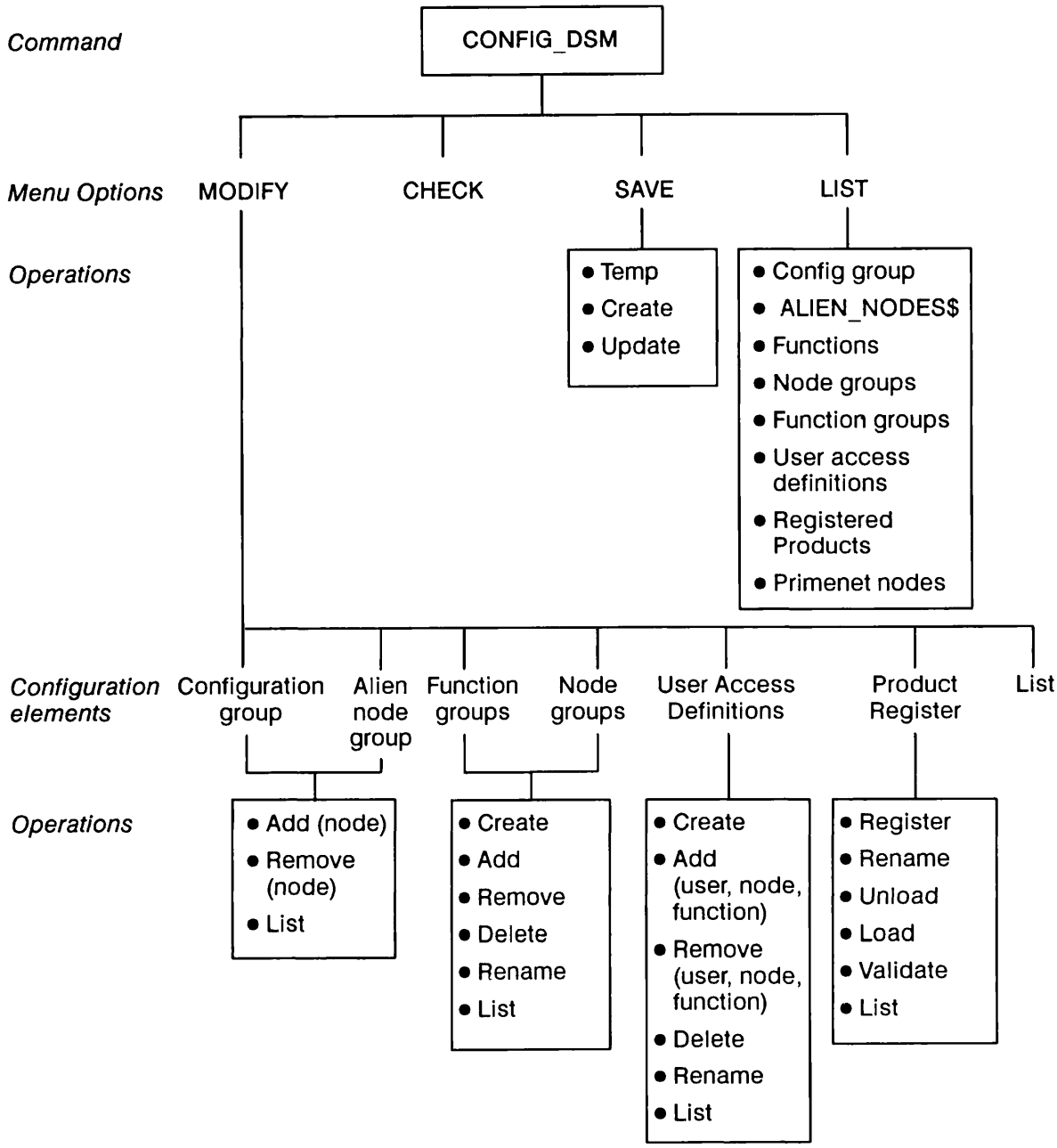

FIGURE 4-4 Menu Hierarchy for CONFIG_DSM

CONFIG_DSM Option (1) - MODIFY the Configuration

The MODIFY the configuration file option allows you to add, remove, modify and delete elements in the configuration.

When you select this option, the MODIFY configuration menu is displayed as shown in Figure 4-5.

```
MODIFY the configuration

Which of the following do you wish to MODIFY?

 (1) Membership of the CONFIGURATION GROUP.
 (2) Membership of the ALIEN NODE GROUP.
 (3) Definition of FUNCTION GROUPS.
 (4) Definition of NODE GROUPS.
 (5) USER ACCESS DEFINITIONS.
 (6) Definition of the PRODUCT REGISTER.
 (7) LIST the configuration.
 (8) HELP.

Enter option number, or press RETURN to leave this menu:
```

FIGURE 4-5 MODIFY the Configuration Menu

Note

The MODIFY the configuration option contains several sublevels of menus and prompts. Use the CONFIG_DSM menu hierarchy (Figure 4-4) to trace the path to a particular editing function.

MODIFY menu, option (1) - Membership of the CONFIGURATION GROUP. - allows you to add and remove nodes, and to display current membership of the group. Listing the configuration group is equivalent to listing the node group .GROUP$.

At installation the configuration group contains only the local node, identified by the reserved name LOCAL$. LOCAL$ is automatically removed if you add any other node to the configuration group. You can use LOCAL$ to stand in for the local node's PRIMENET node name.

All changes to the configuration group are automatically reflected in membership of the reserved node group .GROUP$.

MODIFY menu, option (2) - `Membership of the ALIEN NODE GROUP.` - allows you to create and modify the list of **alien** nodes. *Alien* nodes are those nodes outside your group from which you are prepared to accept requests to invoke DSM commands. Users from all alien nodes work under the special user access definition ALIEN$; users from other nodes outside the group have no access to DSM within your group.

Changes to the alien node list are automatically reflected in the reserved node group .ALIEN_NODES$.

MODIFY menu, option (3) - `Definition of FUNCTION GROUPS`, and menu option (4) - `Definition of NODE GROUPS` - allow you to define, delete and rename function groups and node groups, to add and remove elements, and to list their contents.

Node groups and function groups can be nested within each other to any level, but must not be recursive.

DSM node groups and function groups *must* begin with a period.

Notes

Because function groups and node groups are unique objects, rather than lists of names, they cannot be deleted simply by removing all elements in the list individually; they must be deleted explicitly by name.

The node groups .GROUP$, .ALIEN_NODES$, and .ANY_NODE$ are automatically updated when you add or remove nodes. You cannot alter them through the `Definition of NODE groups` option.

There is no mandatory limit on the size of node groups, but large groups may have implications for system and network performance.

MODIFY menu, option (5) - `USER ACCESS DEFINITIONS.` - allows you to define, rename, delete and list user access definitions, and to change user IDs and function details within the definitions. When you select this option, the `USER ACCESS DEFINITIONS` menu is displayed as shown in Figure 4-6.

```
MODIFY user access definitions and their contents.

USER ACCESS DEFINITIONS currently in the configuration are:
ALIEN$, DSM_ADMINISTRATOR$, DSM_OPERATOR$

 (1)  CREATE new user access definition.
 (2)  ADD user/ACL group to user access definition.
 (3)  REMOVE user/ACL group from user access definition.
 (4)  ADD node/node group that user/ACL group has access from.
 (5)  REMOVE node/node group that user/ACL group has access from.
 (6)  ADD function to user access definition.
 (7)  REMOVE function from user access definition.
 (8)  ADD node/node group that function has access on.
 (9)  REMOVE node/node group that function has access on.
 (10) RENAME user access definition.
 (11) DELETE user access definition.
 (12) LIST contents of user access definitions.
 (13) LIST the configuration.
 (14) HELP.

Enter option number, or press RETURN to leave this menu:
```

FIGURE 4-6. USER ACCESS DEFINITIONS Menu

USER ACCESS DEFINITIONS menu option (1) - CREATE new user access definition. - creates a new user access definition and prompts you for a user ID, a home node or node group, a function or function group, and a target node or node group.

USER ACCESS DEFINITIONS menu options (2) to (5) - allow you to modify the *user* part of a user access definition by adding and removing user names, ACL groups, or node names.

Notes

DSM identifies users by a combination of PRIMOS user name (or ACL group) and home node name. Therefore, a user name alone may not be sufficient to identify a user uniquely if systems on your network do not cooperate in creating user IDs.

When you add a new user to an established ACL group, remember that the user inherits any DSM access rights that are already defined for the group.

USER ACCESS DEFINITIONS menu options (6) to (9) allow you to define and modify the function part of the user access definition by specifying functions and function groups, and the nodes or node groups where they can be invoked.

USER ACCESS DEFINITIONS menu options (10), (11), and (12) allow you to rename, delete, and list existing user access definitions. For further details about user access definitions and how the mechanism works, see Chapter 2, Administration and Security.

USER ACCESS DEFINITIONS menu option (13) invokes the LIST the configuration menu.

USER ACCESS DEFINITIONS menu option (14) invokes the HELP menu.

MODIFY menu option (6) - Definition of the PRODUCT REGISTER. - allows you to make your own applications known to DSM for the purpose of generating, routing, and logging event messages. When you select this option, the menu is displayed as shown in Figure 4-7.

```
MODIFY the Product Register.

Which of the following do you wish to perform?
 (1)  REGISTER product
 (2)  RENAME product
 (3)  UNLOAD Product Register
 (4)  LOAD Product Register
 (5)  VALIDATE Product Register
 (6)  LIST registered products
 (7)  LIST the configuration
 (8)  HELP

Enter option number, or press RETURN to leave this menu:
```

FIGURE 4-7. The PRODUCT REGISTER Menu

PRODUCT REGISTER Menu, option (1) - REGISTER product - enter the name of the customer product that you wish to include in the Product Register. The name must conform to the PRIMOS standard for filenames. Once you have registered a product, you can subsequently rename it, but you cannot delete it from the Product Register.

PRODUCT REGISTER Menu, option (2) - RENAME product - enter the name of the product in the Product Register that you wish to rename, and then enter the new name for this product. The new name must conform to the PRIMOS standard for filenames. When you start DSM with the new configuration, the changed name is used when interpreting DSM log files.

PRODUCT REGISTER Menu, option (3) - UNLOAD Product Register - use this option to store to an ASCII file the list of product names you have entered using Options 1 and 2 above. Enter any valid PRIMOS pathname. If the file already exists, the system prompts you for confirmation before overwriting it. Existing files must not be password protected, and the specified pathname must be sufficient for the system to locate the file from your current attach point. If the file does not exist, a new file is created. If you enter a filename that is invalid or inaccessible, the system reprompts you for the filename.

You can use files created in this way to recreate a Product Register, by using the LOAD Product Register option described in the following paragraph. This facility is important at installations where several configuration groups exist, and it is necessary to keep the customer Product Register consistent across the groups.

You must not edit the unloaded file, as the edited file may not be accepted by the LOAD Product Register option.

PRODUCT REGISTER Menu, option (4) - `LOAD Product Register` - use this option to load an existing ASCII Product Register file, that you have previously created as described in option 3 above. The list of products specified in the file overwrites the contents of an existing Product Register in the current DSM configuration; you are prompted for confirmation before it is overwritten. The pathname you specify must be sufficient for the system to locate the file from your current attach point. If you enter a filename that is invalid or inaccessible, the system reprompts you for the filename.

Use this option to recreate a previously used Product Register, or to set up identical Product Registers in several configuration groups, in order to enable portability across configuration group boundaries.

PRODUCT REGISTER Menu, option (5) - `VALIDATE Product Register` – use this option to check the current configuration by comparing it with an existing ASCII Product Register file. The system reports whether or not the two are identical, but does not list any differences. The pathname you specify for the file must be sufficient for the system to locate it from your current attach point; the specified file must not be password protected. If you enter a filename that is invalid or inaccessible, the system reprompts you for the filename.

PRODUCT REGISTER Menu, option (6) - `LIST registered products` - use this option to list the customer products in the currently loaded Product Register.

PRODUCT REGISTER Menu, option (7) - `LIST the configuration` - invokes the LIST the configuration menu.

PRODUCT REGISTER Menu, option (8) - `HELP` - invokes the HELP menu.

CONFIG_DSM Option (2) - CHECK the Configuration

The CHECK the configuration option on the CONFIG_DSM initial menu, automatically checks the configuration for logic errors and internal consistency in the configuration. Once you have specified the name of the file to be checked, no further input is required on your part. The verification consists of checks for

- Internal consistency
- Consistency with the current PRIMENET configuration on the system

Internal Consistency Check

This is a sequence of verifications that check for

- Completeness: checks that there are no empty definitions of node groups, function groups or user access definitions. If there are, a warning is displayed.
- Incomplete user access definitions: checks that each user access definition has all the necessary elements, that is, a user ID, a node ID, a DSM function and a target node. If any elements are missing, a warning is displayed.
- Administrative user access definitions: checks that the configuration group contains at least one user access definition in which the configuration can be altered on all systems in the group. In practice this means that at least one user must be able to execute STATUS_DSM and DISTRIBUTE_DSM on all nodes in the configuration group.

The internal consistency checks form part of the mandatory validation of the configuration file. Failure to pass any of the internal consistency checks prevents the configuration file from being saved to disk as a valid configuration, and therefore prevents it from being distributed and activated on the network.

PRIMENET Configuration Check

This verifies that all nodes mentioned in the configuration, either as members of the configuration group, alien nodes list and node groups, or as the home node within user access definitions, are in the local PRIMENET configuration.

Failing the PRIMENET configuration check does not prevent you from saving the file as a valid configuration file, or from distributing it. The PRIMENET check is merely intended as a warning.

CONFIG_DSM Option (3) - SAVE the Configuration

The SAVE the configuration option allows you to

- Save an unfinished or unchecked configuration file temporarily to disk.
- Create a new configuration file and save it to disk.
- Save to disk the configuration file that you have defined, as the next revision of an existing configuration file.

When you select this option, the menu is displayed that is shown in Figure 4–8.

```
SAVE the configuration.

How do you wish to save the configuration?
 (1)  WRITE to temporary configuration.
 (2)  CREATE new configuration.
 (3)  UPDATE existing configuration.
 (4)  LIST the configuration.
 (5)  HELP.

Enter option number, or press RETURN to leave this menu:
```

FIGURE 4–8 SAVE the Configuration Menu

SAVE Menu, option (1) - `WRITE to temporary configuration.` - saves the configuration file to disk in a temporary, unchecked form. A temporary configuration file cannot be distributed. You might use this option to save an incomplete configuration, or a file that has failed one or more of the mandatory checks.

SAVE Menu, option (2) - `CREATE new configuration.` - creates a new configuration and saves it to disk. It assigns a unique ID to the configuration file, and sets its revision number to 1.

SAVE Menu, option (3) - `UPDATE existing configuration.` - saves the configuration to disk by overwriting an existing configuration file. The revision number is incremented by one. If you do not specify a pathname, the default action is to overwrite the template configuration file. If the template is a specially protected file, such as the default or restart configuration file, you must specify a pathname.

You cannot revise a previous version of the current *loaded* configuration file with this option. The only way to do this is to rebuild the entire configuration using the current loaded configuration file as the template, and use the option to save it to disk as the *next* revision of that configuration file.

Note

Only files created through the `CREATE new configuration`, and `UPDATE existing configuration` options are valid DSM configuration files.

Before you finally save the configuration file to disk, you can add a line of text to be included in the file header display. Typically, this will be a mnemonic to help identify the configuration, perhaps with some update history. The text must not exceed 160 characters.

CONFIG_DSM Option (4) - LIST the Configuration

The LIST the configuration option allows you to display all or part of the configuration you are currently working on. The list is displayed in a page-mode style. The complete listing can also be written to disk in a form suitable for spooling.

You can summon the LIST menu from all CONFIG_DSM submenus. This enables you to review any part of the configuration at any time.

When you select this option either from the initial menu, or from a submenu, the menu is displayed that shown in Figure 4-9.

```
LIST the configuration.

Which of the following do you wish to LIST?
 (1)  The configuration HEADER.
 (2)  Nodes in CONFIGURATION GROUP.
 (3)  Nodes in ALIEN NODE GROUP.
 (4)  FUNCTIONS.
 (5)  FUNCTION GROUPS.
 (6)  NODE GROUPS.
 (7)  USER ACCESS DEFINITIONS.
 (8)  Registered PRODUCTS
 (9)  COMPLETE listing of configuration.
 (10) User access definition associated with SPECIFIC user/ACL group.
 (11) PRIMENET node names.
 (12) HELP.

Enter option number, or press RETURN to leave this menu:
```

FIGURE 4-9 LIST the configuration Menu

LIST Menu, option (1) - The configuration HEADER. - displays details of the template configuration file, including its ID, revision number, and its recent updating history.

LIST Menu, options (2) to (8) - display subsets of the complete configuration file listing.

LIST Menu, option (2) - Nodes in CONFIGURATION GROUP. - displays all the contents of all nodes in the current configuration group.

LIST Menu, option (3) - Nodes in ALIEN NODE GROUP. - displays a list of all alien nodes.

LIST Menu, option (4) - FUNCTIONS. - displays the complete list of registered DSM functions.

LIST Menu, option (5) - FUNCTION GROUPS. - displays the contents of a named function group, or all function groups.

LIST Menu, option (6) - NODE GROUPS. - displays the contents of a named node group, or all node groups.

LIST Menu, option (7) - USER ACCESS DEFINITIONS. - displays the contents of a named user access definition, or all user access definitions.

LIST Menu, option (8) - Registered PRODUCTS. - displays a list of registered customer applications.

LIST Menu, option (9) - COMPLETE listing of configuration. - displays the complete configuration file at your terminal, or writes it to a disk file. For examples of the display, refer to Appendix A.

LIST Menu, option (10) - User access definition associated with SPECIFIC user/ACL group. - summarizes the DSM access rights of a particular user or ACL group, displaying all the DSM commands they can invoke, and the nodes on which they can invoke them. The access rights of .ANY_USER$ are displayed first, followed by the rights of the individual user, and of the ACL groups to which the user belongs.

Note

To display all the rights of a particular user, you must specify both the user name and *all* of the ACL groups of which that user is a member.

LIST Menu, option (11) - PRIMENET node names. - displays the names of all PRIMENET nodes known to the loaded configuration.

LIST Menu, option (12) - HELP - invokes the HELP menu.

The DISTRIBUTE_DSM Command

DISTRIBUTE_DSM copies a master configuration file to all nodes in a configuration group, or to a named node or node group. DISTRIBUTE_DSM also allows you to remove a node from the loaded configuration group, by distributing to it the default configuration.

The syntax of the command is as follows:

▶ **DISTRIBUTE_DSM [pathname] [options]**

The option *pathname* is used in the case of Options (1), (2), and (4) of the DISTRIBUTE_DSM menu, which is shown in Figure 4-10 It specifies the name of the configuration file you wish to distribute or list. If none is specified, the system prompts you for the pathname of the required file.

The remaining command-line options are described in the following section.

Command-line Options

Command-line options allow you to set the terminal type so that each menu is displayed on a new screen, and to summon HELP and USAGE information for the command.

Descriptions of the options follow.

Option	*Description*
{-TERMINAL_TYPE / -TTP} **terminaltype**	Specify the *terminaltype* you are using, so that the screen is cleared before each menu is displayed. Valid terminal types are TTY, PT45, PST100 and PT200. TTY (glass teletype mode) is the default. Supports the global variable of .TERMINAL_TYPE$ when -TTP is not specified.
{-HELP / -H} [{-NO_WAIT / -NW}]	Explains how to use the command. This option cancels any other options on the command line. If you specify -NO_WAIT, the display is not paginated at your terminal. The same information is available through the PRIMOS HELP subsystem.
-USAGE	Gives you the command syntax in brief. This option cancels all others on the command line.

Distributing the First Configuration

To distribute the first configuration, you must install the configuration in the restart configuration file using the COPY command or File Transfer Service (FTS).

To ensure that subsequent configurations can be performed in the normal way, your first configuration must define a certain minimum level of access, namely that DISTRIBUTE_DSM

can be invoked on all systems on the network from at least one other node. To define the minimum access, modify the default configuration file in the following way:

1. Add the function DISTRIBUTE_DSM to the function part of the user access definition ALIEN$, and specify that the command can be invoked on the local system. Specify the local system using the node's PRIMENET node name, or the keyword LOCAL$.
2. Ensure that node group .ALIEN_NODES$ contains at least one node from which DISTRIBUTE_DSM can be invoked.

To modify the default configuration file, use the CONFIG_DSM command and specify option (1) - MODIFY the configuration., on the Configuration Initial Menu.

For details see earlier in this chapter.

Security and Access

If you have access to DISTRIBUTE_DSM on your local node, you have the right to distribute a new configuration to all nodes in your configuration group.

For a configuration distribution to succeed, the DSM application server (user DSMASR) must have at least RU access to the configuration file that you wish to distribute.

Invoking DISTRIBUTE_DSM

If you invoke the DISTRIBUTE_DSM command without entering the pathname for the configuration file in the command line, the system prompts you for the pathname. If you press the RETURN key, the default configuration file is used. The menu is displayed as shown in Figure 4-10

```
INITIAL menu.

The following options are available:
 (1)  DISTRIBUTE to a SINGLE node
 (2)  DISTRIBUTE to ALL nodes in configuration group
 (3)  REMOVE node from LOADED configuration group
 (4)  LIST configuration group nodes in SPECIFIC configuration
 (5)  LIST configuration group nodes in LOADED configuration
 (6)  HELP.
Enter option number, or press RETURN to leave this menu:
```

FIGURE 4-10 DISTRIBUTE_DSM Menu

DISTRIBUTE_DSM Menu, option (1) - DISTRIBUTE to a SINGLE node - allows you to distribute the specified configuration to a single node. If you do not give a node name, the local node is assumed. For the command to be successfully executed on a node outside the configuration group, you must be recognized as an authorized alien user.

DISTRIBUTE_DSM Menu, option (2) - DISTRIBUTE to ALL nodes in configuration group - allows you to copy the specified configuration file to all nodes in the configuration group which are defined by that configuration.

DISTRIBUTE_DSM Menu, option (3) - REMOVE node from LOADED configuration group - removes a node from the currently active configuration group by distributing the default configuration to it. This forces the node to run as a single-node configuration group at the next startup.

Use this option when an old version of the configuration file has been left in place on a node after removal of the node from a configuration group.

DISTRIBUTE_DSM Menu, option (4) - LIST configuration group nodes in SPECIFIC configuration - displays the contents of the configuration group in the configuration file supplied on the command line or in response to the prompt.

DISTRIBUTE_DSM Menu, option (5) - LIST configuration group nodes in LOADED configuration - displays the contents of the currently active configuration group.

For an example of how to use DISTRIBUTE_DSM, see Example DSM Configuration, at the end of this chapter.

Recording the History of a Configuration

When you invoke DISTRIBUTE_DSM to distribute a new configuration, unsolicited messages are generated to show the origin of the configuration, and whether the distribution was successful. These messages may be useful in verifying the success of a configuration distribution on the network, and as diagnostic and trace data.

DISTRIBUTE_DSM messages can be routed to log files or terminals using the CONFIG_UM command. They are generated by the product DISTRIBUTE_DSM, of severity INFORMATION.

The STATUS_DSM Command

STATUS_DSM allows you to display details of the restart and loaded configuration files on a node, and compares their revision details with the current configuration on any other node. The syntax of the command is as follows:

▶ **STATUS_DSM [pathname] [options]**

The option *pathname* is only used in the case of options (3) and (4) of the STATUS_DSM menu, which is shown in Figure 4-11. It specifies the name of the specific configuration file you wish to inspect. The remaining command-line options are described in the following section.

Command-line Options

Command-line options allow you to set the terminal type so that each menu is displayed on a new screen, and to summon HELP and USAGE information.

Descriptions of the options follow.

Option	*Description*
{**-TERMINAL_TYPE** / **-TTP**} **terminaltype**	Specify the *terminaltype* you are using, so that the screen is cleared before each menu is displayed. Valid terminal types are TTY, PT45, PST100 and PT200. TTY (glass teletype mode) is the default. Supports the global variable of .TERMINAL_TYPE$ when -TTP is not specified.
{**-HELP** / **-H**} [{ **-NO_WAIT** / **-NW** }]	Explains how to use the command. This option cancels any other options on the command line. If you specify -NO_WAIT, the display is not paginated at your terminal. The same information is available through the PRIMOS HELP subsystem.
-USAGE	Gives you the command syntax in brief. This option cancels all others on the command line.

Invoking STATUS_DSM

When you invoke the STATUS_DSM command, the menu is displayed as shown in Figure 4-11.

```
INITIAL menu.

The following options are available:

 (1)  Status of SINGLE node or node group
 (2)  Status of ALL nodes in LOADED configuration group
 (3)  Status of ALL nodes in configuration group of a SPECIFIC configuration
 (4)  LIST configuration group nodes in SPECIFIC configuration
 (5)  LIST configuration group nodes in LOADED configuration
 (6)  HELP

Enter option number, or press RETURN to leave this menu:
```

FIGURE 4-11 STATUS_DSM Menu

STATUS_DSM Menu, option (1) - Status of SINGLE node or node group - allows you to obtain details of the loaded and restart DSM configurations on a node or node group. You are prompted to enter the node whose status you require. If you press <RETURN>, the local node is assumed. Nodes outside the configuration group can be interrogated only if you have the right to invoke STATUS_DSM on those nodes.

STATUS_DSM Menu, option (2) - Status of ALL nodes in LOADED configuration group - allows you to obtain details of the loaded and restart DSM configurations of all nodes in the loaded DSM configuration. It is equivalent to issuing STATUS_DSM on .GROUP$.

STATUS_DSM Menu, option (3) - Status of ALL nodes in configuration group of a SPECIFIC configuration - allows you to obtain the same information as in option (2), but in this case, the nodes are those defined in the configuration file whose name is specified in the STATUS_DSM command line. If you did not specify a file when issuing the command, the system prompts you for the filename.

STATUS_DSM Menu, options (4) and (5) - list the nodes in either the configuration file specified on the command line, or in the loaded DSM configuration, respectively. In the case of option (4), if you did not specify a file when issuing the command, the system prompts you for the filename.

For an example of the kind of display produced when you invoke STATUS_DSM, refer to the example configuration at the end of this chapter.

Strategies for Adding and Removing Nodes

Adding a Node

To add a node to a configuration group you must

1. Have a user access definition that allows you to invoke DISTRIBUTE_DSM on the node in question. As administrator of the group, this is under your control.

2. Ensure that the node from which you use DISTRIBUTE_DSM is in the list of alien nodes on the node you want to add.
3. Ensure that the user access definition ALIEN$ on the node you want to add allows you to invoke DISTRIBUTE_DSM.

Steps 2 and 3 are under the control of the target node. If you do not control the target node, you must elicit the cooperation of the target node's administrator.

Once these conditions are met, you can add the node to your group using the following steps:

1. Invoke CONFIG_DSM using your current *loaded* configuration file as a template, and add the target node to the configuration group.
2. Check the new configuration and save it to disk.
3. Use DISTRIBUTE_DSM to copy the new configuration to the configuration group.

The node becomes part of your group the next time DSM is started on those nodes.

Removing a Node

To remove a node from your configuration group using the following steps:

1. Remove the node from the group.
2. Check and save the new configuration.
3. Distribute it to all nodes in the group.

This leaves the node suspended; it is no longer recognized as part of the group of which it still believes it is a member. To avoid mismatches, the node should be reverted at the earliest opportunity to the default configuration, using option (3) - `REMOVE node from LOADED configuration group` of DISTRIBUTE_DSM. The node then reverts to the default configuration the next time DSM is started.

A node can also be removed from the configuration as a result of capture by another group.

Configuration Planning Notes

This section describes some of the factors that you should consider when planning a DSM configuration for your system.

User Security

DSM commands and services are intended for System Administrators and operators, and you may not consider them suitable for general release to time-share users on your system. It is your responsibility as System Administrator to determine how you make the commands available on your system; the decisions can only be made in the light of the security practice at your installation, and the level of experience of your user base.

Remember that facilities such as RESUS, system logging, CONFIG_UM, and the DSM configuration commands should be made available only to trusted personnel: you might also wish to restrict users' access to commands that display sensitive user information, such as LIST_PROCESS and LIST_UNITS.

In general, always take care when you define access to DSM commands and services, and be aware of the possible implications for security on your system.

Intergroup Security

Remember that users on nodes that are outside your configuration group have all the access rights of the user access definition ALIEN$ on your system. You rely on the administrators of these groups to grant access to trustworthy users, and so the granting of intergroup access must be a consultative procedure with other administrators. If cooperation is impossible because of geography or departmental division, you should restrict ALIEN$ to a bare minimum of DSM facilities on your system.

System and Network Resources

Unrestricted access to distributed facilities such as those of DSM could affect networking performance by preempting network resources. Further, DSM competes for network resources with other distributed products such as the **File Transfer Service** (FTS). As administrator, you should be careful to balance the needs of all distributed products on your system.

The Configuration Group

DSM places no constraints on membership of the configuration group. You are free to define configuration groups in any way you wish, and in a way most convenient for your network. Systems that are administered as single machines can each be in their own configuration group. Local ring networks can be controlled collectively as one configuration group, or can be split for easier administration. For small networks that consist of a few machines, whether locally or widely networked, a single configuration group is usually sufficient.

In deciding how to partition your network, first consider if your current pattern of administration should be mapped directly into a DSM configuration. Any degree of collective administration tends to imply a DSM configuration group. Other factors to be taken into account include the mix of CPU types and the physical topology of your network, the speed of the various node-to-node links, and existing security arrangements.

In summary:

- Nodes that are geographically isolated, or on slow communications lines may be unsuitable for inclusion in the same group, because response times would be too slow.
- Grouping fast and slow machines together could create bottlenecks. Fast machines may be better grouped together to maximize the benefits of increased CPU power on overall network performance.

- The larger the group the greater are the demands on the networking capacity of your system when you perform a group-wide operation. To minimize the possible impact on network performance you may decide on several small groups rather than a single large one.
- DSM security and Remote File Access (RFA) are independent. However, both systems implement security between nodes on the network, and you may feel it appropriate to ensure that they coincide on your system. It is worth reflecting that if there are good reasons why two nodes do not trust each other through RFA, then perhaps they should not trust each other through DSM security.

Size and Content of Node Groups

You can create node groups of any size, but remember that the ability of DSM to execute a command on many nodes depends on the demands made on network resources by other networked products. How large you make your node groups depends on the performance you expect from DSM in relation to other networked products on your system.

Node groups, once defined and activated in the configuration, can be used in all commands that support distributed execution. Nodes that are geographically distant, or linked by slow communications lines may be unsuitable for inclusion in the same node group, because the response time would be unacceptably slow.

Example DSM Configuration

This section shows how to construct and establish a DSM configuration on a three-node ring network. The network is linked to another Prime installation, and to the public network through one node on the ring that acts as a gateway.

The main features of the example ring network are summarized in Figure 4-12.

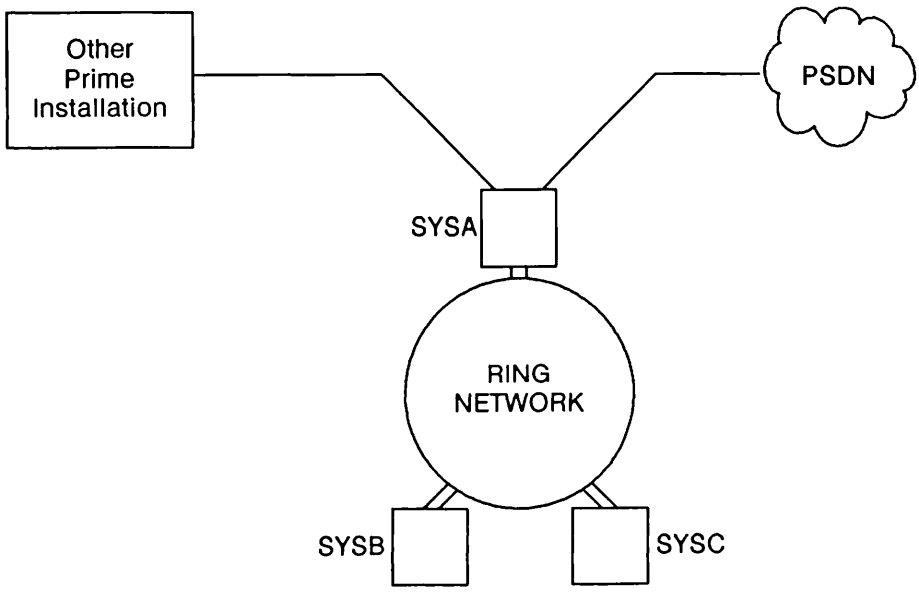

FIGURE 4-12 Example Prime Network Configuration

Example Configuration Environment

In the example, the three systems on the ring are known as SYSA, SYSB and SYSC. SYSA is the system that handles communication with the other Prime site, and with the Public Services Data Network (PSDN).

All three machines are controlled by a single System Administrator based at SYSA. Two operators in his staff are responsible for administering and monitoring network services on the ring and for general operational duties. The System Administrator and the two operators work under system-based user IDs, all of which are in the ACL group .SYSTEM. The ACL group .SYSTEM has access to all operator commands, system files, and system management utilities.

All users on the ring also have personal user IDs. The administrator's user ID is ARKWRIGHT.

A student employed on an industrial placement scheme is doing a project on PSDN usage on the ring. The student, who has the login ID AHACKER on SYSB, needs access to information about the network on SYSA, the PSDN gateway.

Two customer applications, LOGIN_MANAGER and MAIL, will use the Customer UM facility.

Imagine you are the System Administrator responsible for this Prime ring network. You decide on the following requirements for the administration of DSM on the ring:

- The existing ring network should form a single DSM configuration group, to reflect current administrative practice. You will remain personally responsible for all aspects of administering DSM, until there is more experience with the product.
- The operators should have rights to the DSM facilities that help with day-to-day monitoring and system operation, but will not be allowed to reconfigure DSM, or set access rights.
- The industrial student should have access only to information about the network resources of SYSA; for security purposes the student should have access to no other system information.
- For the time being, time-share users on the ring should have no access to DSM commands.
- There are two applications that will send UM's.

The Configuration Sequence

To create the example configuration, you need to

1. Define a configuration group that contains nodes SYSA, SYSB and SYSC.
2. Insert your own user name and those of your operators in the preset user access definitions DSM_ADMINISTRATOR$ and DSM_OPERATOR$ respectively.
3. Set up a special user access definition for the student employee to monitor network parameters on the PSDN gateway node SYSA.
4. Add the products LOGIN_MANAGER and MAIL.

In the following dialogs, pressing the RETURN key after user input is omitted for the sake of clarity.

Invoking the DSM Configurator

1. Invoke CONFIG_DSM from PRIMOS with the correct *terminaltype.*
2. Press the RETURN key to read in the default configuration file.
3. After the configuration file header details are displayed, press the RETURN key once again, to summon the CONFIG_DSM Initial menu (see Figure 4-2).

These steps are illustrated in the following example:

```
OK, CONFIG_DSM -TTP PT200
[CONFIG_DSM Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]

Give pathname for configuration file or Quit (default is
"DSM*>CONFIG_FILES>DSM_DEFAULT.CONFIG")
: Return

Configuration file   : DSM_DEFAULT.CONFIG
Revision number      : 1
Last updated         : 90/06/23 17:46:08
Updated by user      : SYSTEM
Updated on node      : PRIME
DSM revision number  : 1
Comment              : DEFAULT CONFIG FILE

--Press < RETURN > to continue: Return

   Which of the following do you wish to perform?

    (1)  MODIFY the configuration.
    (2)  CHECK the configuration for consistency.
    (3)  SAVE the configuration.
    (4)  LIST the configuration.
    (5)  HELP.

   Enter option number, or press RETURN to leave this menu:
```

Configuration Group Definition

To define the example configuration group, you would have to add nodes SYSA, SYSB and SYSC to the configuration group. The procedure you would follow is outlined below.

1. On the CONFIG_DSM Initial menu, select option (1) - `MODIFY the configuration`. See Figure 4-2.
2. On the MODIFY the configuration menu, select option (1) - `Membership of the CONFIGURATION` group. See Figure 4-5.
3. On the Membership of the CONFIGURATION group Menu, choose option (1) - `ADD node to configuration group` - and input the three node names.

Step 3 in this sequence is illustrated in the following example:

```
The configuration group (.GROUP$) contains:
 LOCAL$.

 (1)  ADD node to configuration group.
 (2)  REMOVE node from configuration group.
 (3)  LIST the configuration.
 (4)  HELP.

Enter option number, or press RETURN to leave this menu: 1

Enter node name: SYSA
Warning from DSM_ADMIN (DSM_admin-427):
 You have added a node to the configuration group.
 The local node (LOCAL$) has been automatically removed.

Enter node name: SYSB
Enter node name: SYSC
Enter node name: QUIT
```

When you type QUIT to the final prompt, you return to the MODIFY the membership of the configuration group menu, which in this example would now display the three nodes you have just added at the head of the option list.

This completes definition of the example configuration group. Type QUIT, or press the RETURN key, to display the MODIFY the configuration menu once again.

User Access Definition Modification Sequence

To modify the predefined user access definitions in this example to include your own user IDs, you would proceed as follows:

1. On the MODIFY the configuration menu (see Figure 4-5), select option (5) - USER ACCESS DEFINITIONS.
2. On the USER ACCESS DEFINITIONS Menu (see Figure 4-6), select option (2) - ADD user/ACL group to user access definition, name the user access definition you want to alter, specify the user ID to be added, and quit.

Step 2 in the user access definition modification sequence is illustrated in the following example:

```
User access definitions currently in the configuration are:
 ALIEN$, DSM_ADMINISTRATOR$, DSM_OPERATOR$
 (1)  CREATE new user access definition.
 (2)  ADD user/ACL group to user access definition.
 (3)  REMOVE user/ACL group from user access definition.
 (4)  ADD node/node group that user/ACL group has access from.
 (5)  REMOVE node/node group that user/ACL group has access from.
 (6)  ADD function to user access definition.
 (7)  REMOVE function from user access definition.
 (8)  ADD node/node group that function has access on.
 (9)  REMOVE node/node group that function has access on.
 (10) RENAME user access definition.
 (11) DELETE user access definition.
```

```
  (12) LIST contents of user access definitions.
  (13) LIST the configuration.
  (14) HELP.

Enter option number, or press RETURN to leave this menu: 2

Enter user access definition name: DSM_ADMINISTRATOR$
Enter user/ACL group name to add to user access definition: ARKWRIGHT
  Enter node/node group that user/ACL group has access FROM : .GROUP$
  Enter node/node group that user/ACL group has access FROM : QUIT
Enter user/ACL group name to add to user access definition: QUIT

Enter user access definition name: DSM_OPERATOR$
Enter user/ACL group name to add to user access definition: .SYSTEM
  Enter node/node group that user/ACL group has access FROM : .GROUP$
  Enter node/node group that user/ACL group has access FROM : QUIT
Enter user/ACL group name to add to user access definition: QUIT
```

Removing Unwanted Usernames: In the default configuration that you are using as a template in this example, DSM_ADMINISTRATOR$ and DSM_OPERATOR$ contain usernames that you may wish to delete. You could remove them in the following way:

1. On the USER ACCESS DEFINITIONS Menu, select option (3) - `REMOVE user/ACL group from user access definition`. See Figure 4-6.
2. Name the user access definition you want to alter, specify the user ID to be removed, and quit.

Step 2 is illustrated in the following example:

```
Enter user access definition name: DSM_ADMINISTRATOR$
Enter user/ACL group name to remove from user access definition: .SYSTEM_ADMINISTRATOR
Enter user/ACL group name to remove from user access definition: QUIT

Enter user access definition name: DSM_OPERATOR$
Enter user/ACL group name to remove from user access definition: SYSTEM
Enter user/ACL group name to remove from user access definition: QUIT
```

If you list the two user access definitions at your terminal using option (12) on the MODIFY user access definitions menu, shown in Figure 4-6, the following display is shown:

```
Do you want to list all the user access definitions ? NO
Enter user access definition name: DSM_ADMINISTRATOR$
User access definition DSM_ADMINISTRATOR$ is defined as:
 User/ACL group ARKWRIGHT from location(s): .GROUP$
 Function/function group: .ANY_FUNCTION$ is allowed on node/node groups: .ANY_NODE$
Enter user access definition name: DSM_OPERATOR$
User access definition DSM_OPERATOR$ is defined as:
 User/ACL group .SYSTEM from location(s):.GROUP$.
 Function/function group: .RESUS$ is allowed on node/node groups: .ANY_NODE$.
 Function/function group: .SIM$ is allowed on node/node groups: .ANY_NODE$.
```

User Access Definition for the Student Employee

In the example configuration, the student needs to use SIM commands that relate to the operation of the network, on the PSDN gateway SYSA.

You could define a function group called .NETWORK_STATUS that contains all the network-related SIM commands:

LIST_COMM_CONTROLLERS
LIST_LAN_NODES
LIST_PRIMENET_NODES
LIST_PRIMENET_LINKS
LIST_PRIMENET_PORTS
LIST_VCS

To make the PSDN function of SYSA clearer in the user access definition, you could define a node group called .PSDN_LINK, containing SYSA.

To give the student access to these commands and no others, you could define the following user access definition:

(AHACKER-from-SYSB) can do (.NETWORK_STATUS-on-.PSDN_LINK)

This user access definition would give AHACKER the right to use all the commands in .NETWORK_STATUS on nodes in the group .PSDN_LINK (= SYSA), from node SYSB. User AHACKER cannot log in at SYSA, nor use any DSM facilities there other than the commands in the node group .NETWORK_STATUS.

The function group, node group and user access definition sequences are described in the following subsections.

Function Group Definition Sequence

1. On the MODIFY the configuration menu, select option (3) - `Definition of FUNCTION GROUPS`. See Figure 4-5.
2. On the DEFINITION OF FUNCTION GROUPS Menu, select option (1) - `CREATE new function group`.
3. Name the function group, input its member functions one by one, and quit.

Steps 2 and 3 in this sequence are illustrated below.

```
Function groups which may be modified by this menu are:
   .ADMIN$, .RESUS$, .SIM$.

  (1)  CREATE new function group.
  (2)  ADD function to function group.
  (3)  REMOVE function from function group.
  (4)  DELETE function group.
  (5)  RENAME function group.
  (6)  LIST all functions.
```

```
(7)  LIST contents of function groups.
(8)  LIST the configuration.
(9)  HELP.


Enter option number, or press RETURN to leave this menu: 1

Create new function group: .NETWORK_STATUS

Enter function/function group name to add to .NETWORK_STATUS: LIST_COMM_CONTROLLERS
Enter function/function group name to add to .NETWORK_STATUS: LIST_LAN_NODES
Enter function/function group name to add to .NETWORK_STATUS: LIST_PRIMENET_NODES
Enter function/function group name to add to .NETWORK_STATUS: LIST_PRIMENET_LINKS
Enter function/function group name to add to .NETWORK_STATUS: LIST_PRIMENET_PORTS
Enter function/function group name to add to .NETWORK_STATUS: LIST_VCS
Enter function/function group name to add to .NETWORK_STATUS: QUIT
```

If you listed the function group .NETWORK_STATUS at your terminal, you would see the following display:

```
Do you want to list all the function groups? NO
Enter function group name: .NETWORK_STATUS
Function group .NETWORK_STATUS contains:
 LIST_COMM_CONTROLLERS, LIST_LAN_NODES, LIST_PRIMENET_LINKS,
 LIST_PRIMENET_NODES, LIST_PRIMENET_PORTS, LIST_VCS.
Enter function group name: QUIT
```

Node Group Definition Sequence

1. On the MODIFY the configuration menu, select option (4) - Definition of NODE GROUPS. See Figure 4-5.
2. On the DEFINITION OF NODE GROUPS Menu, select option (1) - CREATE new node group.
3. Input the new node group name, specify its member nodes, and quit.

Steps 2 and 3 in this sequence for the example configuration are illustrated below.

```
There are no node groups which may be modified by this menu.

 (1)  CREATE new node group.
 (2)  ADD node to node group.
 (3)  REMOVE node from node group.
 (4)  DELETE node group.
 (5)  RENAME node group.
 (6)  LIST contents of node groups.
 (7)  LIST the configuration.
 (8)  HELP.

Enter option number, or press RETURN to leave this menu: 1

Create New Node Group: .PSDN_LINK
Enter node/node group name to add to .PSDN_LINK: SYSA
Enter node/node group name to add to .PSDN_LINK: QUIT
```

If you listed the node group .PSDN_LINK at your terminal, you would see the following display:

```
Do you want to list all the node groups ? NO
Enter node group name: .PSDN_LINK
Node group .PSDN_LINK contains: SYSA.
Enter node group name: QUIT
```

User Access Definition Sequence

1. On the MODIFY the configuration menu, choose option (5) - USER ACCESS DEFINITIONS. See Figure 4-5.
2. On the USER ACCESS DEFINITIONS Menu, choose option (1) - CREATE new user access definition. See Figure 4-6.
3. Name the new user access definition, enter the components of the definition, and quit.

Steps 2 and 3 in this sequence are illustrated below.

```
User access definitions currently in the configuration are:
   ALIEN$, DSM_ADMINISTRATOR$, DSM_OPERATOR$

 (1)  CREATE new user access definition.
 (2)  ADD user/ACL group to user access definition.
 (3)  REMOVE user/ACL group from user access definition.
 (4)  ADD node/node group that user/ACL group has access from.
 (5)  REMOVE node/node group that user/ACL group has access from.
 (6)  ADD function to user access definition.
 (7)  REMOVE function from user access definition.
 (8)  ADD node/node group that function has access on.
 (9)  REMOVE node/node group that function has access on.
 (10) RENAME user access definition.
 (11) DELETE user access definition.
 (12) LIST contents of user access definitions.
 (13) LIST the configuration.
 (14) HELP.

Enter option number, or press RETURN to leave this menu: 1

CREATE new user access definition: PSDN_PROJECT

DEFINE user part of user access definition ...

Enter user/ACL group name to add to user access definition: AHACKER
  Enter node/node group that user/ACL group has access FROM: SYSB
  Enter node/node group that user/ACL group has access FROM: QUIT
Enter user/ACL group name to add to user access definition: QUIT

DEFINE function part of user access definition ...

Enter function/function group to add to user access definition: .NETWORK_STATUS
  Enter node/node group that function/function group has access ON: .PSDN_LINK
  Enter node/node group that function/function group has access ON: QUIT
Enter function/function group to add to user access definition: QUIT
```

If you were to list the contents of PSDN_PROJECT, you would see the following display:

```
Do you want to list all the user access definitions? NO
Enter user access definition name: PSDN_PROJECT
User access definition PSDN_PROJECT is defined as:
   User/ACL group AHACKER from location(s): SYSB.
   Function/function group: .NETWORK_STATUS is allowed on node/node groups: .PSDN_LINK.
Enter user access definition name: QUIT
```

Access Rights For All Other Users

The default configuration prevents all users other than those in the user access definitions DSM_ADMINISTRATOR$ and DSM_OPERATOR$ from executing DSM commands on the network. You need take no further action to prevent time-share users from executing DSM commands on the system.

Adding Customer Products

4. On the MODIFY the configuration menu, select option (6) - Definition of the PRODUCT REGISTER, see Figure 4-5.
5. On the PRODUCT REGISTER Menu, (see Figure 4-7) select option (1) and enter the names of the customer products you wish to be included in the configuration.

The screen dialog is shown below.

```
Enter product name: LOGIN_MANAGER
Enter product name: MAIL
Enter product name: Return
--Press <RETURN> to continue: Return
```

If you list the the registered products, using option (6) on the PRODUCT REGISTER Menu, the following display is shown:

```
Registered products are:
LOGIN_MANAGER, MAIL
--Press <RETURN> to continue:
```

Listing the Master Configuration File

To display the configuration or any part of it, select the LIST the configuration option on any menu and choose the required option.

For a complete listing of the master configuration file generated by this example, refer to Appendix A.

Checking the Master Configuration File

To check the configuration, select option (2) - CHECK the configuration for consistency - on the CONFIG_DSM Initial menu shown in Figure 4-2.

This automatically verifies the configuration and warns you of any inconsistencies or omissions. If there are any inconsistencies in the mandatory checks, you must reenter the MODIFY the configuration menu and make the necessary changes before you check the file once again. The configuration cannot be distributed until it has passed all the mandatory checks.

You may also wish to modify or delete any items that, although incomplete in some way, do not prevent the file being distributed.

The following is an example of the display you see when you check the example master configuration:

```
Warning: The following empty definitions were found:
 (CONFIG_DSM)

  Node group .ALIEN_NODES$.
--Press < RETURN > to continue: Return

The configuration file has PASSED the consistency checks.

--Press < RETURN > to continue: Return
```

Saving the Master Configuration File

To save the configuration, proceed as follows:

1. On the CONFIG_DSM Initial menu, select option (3) - SAVE the configuration. See Figure 4-2.
2. On the SAVE the configuration menu, select option (2) - CREATE new configuration. See Figure 4-8.
3. Give a suitable pathname, and write an explanatory comment on the file.

Steps 2 and 3 are illustrated in the following example:

```
How do you wish to save the configuration?

 (1)  WRITE to temporary file.
 (2)  CREATE new configuration.
 (3)  UPDATE existing configuration.
 (4)  LIST the configuration.
 (5)  HELP.

Enter option number, or press RETURN to leave this menu: 2

Enter pathname for configuration: ARKWRIGHT>DSM>CONFIG.1
Enter comment or Quit (default is "DEFAULT CONFIG FILE"): SYS RING CONFIG FILE
Configuration File <DISK1>ARKWRIGHT>DSM>CONFIG.1, revision 1 written.

--Press < RETURN > to continue: Return
```

Distributing the Master Configuration File

At this stage in the example you would have a valid master configuration file on disk under the pathname <DISK1>ARKWRIGHT>DSM>CONFIG.1. To distribute the configuration to the three systems on the ring, proceed as follows:

1. Invoke the DISTRIBUTE_DSM command on SYSA.
2. Select option (2) - DISTRIBUTE to ALL nodes in configuration group on the DISTRIBUTE_DSM menu, see Figure 4-10.

The configuration represented by the file CONFIG.1 would be activated the next time DSM is started on the three systems.

Distributing the configuration is illustrated in the following example:

```
OK, DISTRIBUTE_DSM
[DISTRIBUTE_DSM Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]

Enter pathname for configuration or Quit: <DISK1>ARKWRIGHT>DSM>CONFIG.1
(default is "DSM*>CONFIG_FILES>DSM_DEFAULT.CONFIG)

The following options are available:-

 (1)  DISTRIBUTE to a SINGLE node
 (2)  DISTRIBUTE to ALL nodes in configuration group
 (3)  REMOVE node from LOADED configuration group
 (4)  LIST configuration group nodes in SPECIFIC configuration
 (5)  LIST configuration group nodes in LOADED configuration
 (6)  HELP

Enter option number, or press RETURN to leave this menu: 2

The configuration being distributed is:-

Master configuration file  : <DISK1>ARKWRIGHT>DSM>CONFIG.1
Configuration file         : CONFIG.1
Revision number            : 1
```

```
Last updated                : 90/07/01 16:38:56
Updated by user             : ARKWRIGHT
Updated on node             : SYSA
DSM revision number         : 1

Function DISTRIBUTE_DSM being invoked on node:-  SYSA, SYSB, SYSC .

Node: SYSA
Restart configuration file successfully updated at 1 Jul 90 16:58:56 Friday.

Node: SYSB
Restart configuration file successfully updated at 1 Jul 90 16:59:35 Friday.

Node: SYSC
Restart configuration file successfully updated at 1 Jul 90 16:59:47 Friday.
OK,
```

Checking Configuration File Status

To check the integrity of the group, use the STATUS_DSM command to compare the loaded and restart configuration files on the three systems. In the example you would proceed in the following way.

3. Invoke STATUS_DSM on SYSA.
4. Select option (2) - Status of ALL nodes in LOADED configuration group on the STATUS_DSM menu as shown in see Figure 4-11.

Checking configuration status in the configuration group is illustrated in the following example:

```
OK, STATUS_DSM
[STATUS_DSM Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]

The following options are available:-

 (1)  Status of SINGLE node or node group
 (2)  Status of ALL nodes in LOADED configuration group
 (3)  Status of ALL nodes in configuration group of a SPECIFIC configuration
 (4)  LIST configuration group nodes in SPECIFIC configuration
 (5)  LIST configuration group nodes in LOADED configuration
 (6)  HELP.

Enter option number, or press RETURN to leave this menu: 2

Give name of reference node or Quit (default is LOCAL node): Return

Reference node:- SYSA

LOADED configuration  : CONFIG.1
Revision number       : 1
Last updated          : 90/07/01 16:38:56
Updated by user       : ARKWRIGHT
Updated on node       : SYSA
DSM revision number   : 1
Comment               :

RESTART configuration : CONFIG.1
```

```
Revision number       : 1
Last updated          : 90/07/01 16:38:56
Updated by user       : ARKWRIGHT
Updated on node       : SYSA
DSM revision number   : 1
Comment               :

Node: SYSC

LOADED configuration : Same as LOADED configuration on reference node

RESTART configuration: Same as RESTART configuration on reference node

Node: SYSB

LOADED configuration : Same as LOADED configuration on reference node

RESTART configuration: Same as RESTART configuration on reference node

Node: SYSA
Node is the reference node.

OK,
```

5

UMH CONFIGURATION

Introduction

This chapter describes how to configure DSM unsolicited message handling (UMH) on the system using the CONFIG_UM command. For an overview of the unsolicited message handling service, refer to Chapter 2, Administration and Security.

The chapter begins with an introduction to the command, followed by descriptions of the command options. The descriptions are in two parts. The first part briefly describes the main options -CREATE, -MODIFY, -DELETE, -LIST, -HELP and -USAGE. The second part describes in detail the -CREATE option that invokes the main selection definition subsystem.

Overview of Unsolicited Message Handling

DSM unsolicited message handling (UMH) is the user-configurable service that routes event messages generated on the system, to log files and users on the network. It allows you to control the logging and real-time display of event messages by selecting messages according to product and severity, and routing them to log files and users throughout the configuration group. Messages can be recorded in DSM private or system logs for storage and later retrieval, directed to users by name or number, or displayed on assigned lines.

The messages may include event messages from PRIMOS and PRIMENET, as well as unsolicited messages from customer defined products. For details on registering customer products, refer to the section, Defining the Product Register, in Chapter 4. For details of sending unsolicited messages from customer defined products, see Appendix C.

To configure the UMH facility on a system, you define message **selections** using the CONFIG_UM command. Selections are sets of criteria that govern the selection of messages on a system for routing to specific destinations. Collectively, they form the database on a system that controls the routing of all unsolicited messages.

Selections consist of a list of product names, message severities, and destinations. **Products** can be either Prime or customer originated and are the programs, subsystems, and devices that generate unsolicited messages. **Severities** are keywords that reflect the importance of

the event, and **destinations** are targets for the selected messages. Destinations can be private or system log files, users specified by name or number, or assigned devices and terminals identified by line number. The destination DISCARD allows messages to be discarded from the system.

UMH selections are held in the binary file DSM_UMH.CONFIG in the directory DSM*>CONFIG_FILES. This file should not be renamed, deleted, or altered in any way.

The UMH in Event Logging

System and network event logging is controlled by DSM. The DSM System Manager process supervises the transfer of event messages from both Prime products and customer registered products, to the UMH, from where they can be routed to logs or users of your choice using the CONFIG_UM command.

▶ CONFIG_UM [selection name] subcommand

CONFIG_UM is the command that configures unsolicited message handling on a system through the definition of message **selections**. Options allow you to

- Create new selections.
- Modify existing selections.
- Delete selections.
- List selections at your terminal.
- Display Help or Usage information.

You must specify one and only one subcommand when you invoke the CONFIG_UM command.

With the main subcommand options (-CREATE, -MODIFY and -DELETE), you must specify a selection name. If you do not give a name on the command line, you must do so in reply to the subsequent `Selection Name:` prompt.

Descriptions of the subcommand options follow.

Subcommand	*Description*
{**-CREATE** / **-CR**} **[-ON node]**	Creates a selection on the specified *node*. A maximum of twelve selections is allowed per system. If you do not specify a node, the local node is assumed. You can exit from the -CREATE command by entering QUIT or Q at any one of the prompts that are displayed by the -CREATE subsystem. For details of the -CREATE subsystem, see below.
{**-MODIFY** / **-MOD**} **[-ON node]**	Allows you to modify a selection. Displays the selection name and each item in the product, severity and destination lists in turn, and allows you to modify them using normal PRIMOS command-line editing. You can also add new items at the end of any of the lists, in response to the input prompt. When you modify an item, or add a new one, it is immediately redisplayed to you for checking.

When you have completed your modifications, quit the editing sequence by typing YES to the query prompt, and the modified selection is immediately configured on the system. You can exit from the -MODIFY command by entering QUIT or Q at any one of the prompts that are displayed by the -MODIFY subsystem.

-DELETE [-ON node] Deletes a selection from the system.

-LIST [-ON node] {-NO_WAIT / -NW} Displays a selection at your terminal. If you do not specify a selection name, all selections currently in force on the local node are displayed as well as the count of currently configured selections. Prime products will be listed first followed by the customer products.

{-HELP / -H} [{-NO_WAIT / -NW}] Explains how to use the command. This option cancels all others on the command line. If you specify -NO_WAIT, the display is not paginated at your terminal. The same information is available through the PRIMOS HELP subsystem.

-USAGE Gives you the command syntax in brief. This option cancels all others on the command line.

The -CREATE [-ON node] Option

The -CREATE option allows you to define a new selection. It invokes a simple subsystem environment in which you specify the elements of a selection. You can configure up to twelve selections on a system.

Selection Name

Selection names can be 1 through 32 characters long and must start with an alphabetic character. They can contain only alphanumeric characters, and the period (.), dollar ($) and underscore (_) symbols. The dollar symbol ($) is normally reserved for Prime's use.

If you do not give a selection name on the command line, give one in response to the `Selection Name:` prompt. If you do not specify a node name, the local node is assumed.

Subsystem Environment

Once you have entered the -CREATE subsystem, you are prompted in turn for

- Prime products
- Customer products
- Severities
- Destinations

You must specify at least one product, severity and destination in each selection. Two destinations are allowed per selection.

To specify a product, severity, or destination, type the name or keyword after the appropriate prompt and press the RETURN key.

To correct any errors, use PRIMOS command-line editing. Either backspace over part of the line with the erase key, and overtype, or delete the entire line with the kill key and retype it.

To quit from an input prompt and pass to the next stage of input, press the RETURN key.

To quit from the -CREATE subsystem at any time, type QUIT, or Q. This returns you immediately to PRIMOS, and discards the selection you were editing.

For brief online information on products, severities and destinations, type HELP when you are in the subsystem environment and a valid list of products, severities or destinations will be displayed.

Products

Products can be either Prime products or customer products. Applications and products that generate unsolicited messages are known by product names that are registered with DSM. For the list of Prime product names that you can use, with brief descriptions of the products to which they refer, see Appendix B, DSM Product Names. For details on registering customer products, refer to the section, Defining the Product Register, in Chapter 4, and for details on sending unsolicited messages from customer products, refer to Appendix C, Sending Customer Unsolicited Messages.

If you specify -ANY at the prompt `Prime Product`, all Prime product names are included in the selection. If you specify -ANY at the prompt `Customer Product`, all registered customer product names are included in the selection. The hyphen character is part of the syntax of this response and must be included.

Type HELP at the prompt `Prime Product:` to display the list of valid Prime Products. Type HELP at the prompt `Customer Product:` to display the list of valid Customer Products. You can also type HELP *product* or H *product* at either of these prompts in order to display the Help file for the product specified. If no Help file for the product exists, the system displays the message `Detailed help for <product> not available.`

Note

Help text can be added for customer products by placing text files in DSM*>HELP. The format for the filename is DS$UM_HELP_<product_name>.HELP; you should abbreviate <product_name>, if necessary, so that the length of the filename does not exceed 32 characters.

You must specify at least one product in each selection; this may be a Prime product or a customer product. The maximum number of products that you can configure is 12; these may be any combination of Prime and customer products.

Severities

The message severity is an indication of the importance to system integrity of the event that generated the message.

Type HELP at the prompt `Severity:` to display the list of valid severity levels. You can also type HELP *severity* or H *severity* at this prompt in order to display the Help file for the severity specified. If no Help file for the specified severity exists, the system displays the message `Detailed help for <severity> not available.`

Severities, their meanings, and the level of action required, are described below.

Severity	*Meaning*
SECURITY	An attempt to breach system or file security has been detected. This requires immediate investigation.
ALARM	A system, subsystem, program or device resource limit has been exceeded, and requires immediate attention.
WARNING	A system, subsystem, program or device resource limit is approaching, and serves as advance warning of a possible ALARM condition. Prompt attention is required.
INFORMATION	An event that does not require intervention and may be used for informative messages.
FAILURE	A subsystem, program or device has failed or crashed. This may be preceded by messages of lower severity such as information, warning, and diagnostic.
DIAGNOSTIC	Information about past or impending failures. This may be useful for predicting faults, and for analysing them after the event.
ACCOUNTING	Chargeable resource usage.
STATISTIC	Other resource usage.
-ANY	Shorthand for *all* severity categories.

Destinations

Destinations can be log files, users, or assigned lines on any node within the *loaded* configuration group.

You can specify up to two destinations in each selection.

Note

Use *remote* destinations with care. They can be expensive in network resources.

Standard destinations are

LOGGER <logfile>
DISPLAY <user/assigned line>
DISCARD
DEFAULT_LOG

Type HELP at the prompt `Destination:` to display the list of valid message destinations. You can also type HELP *destination* or H *destination* at this prompt in order to display the Help file for the destination specified; this file contains the syntax for the specified destination in addition to associated useful information, for example, the fact that you use the command ADMIN_LOG to create a log. If no Help file for the specified destination exists, the system displays the message `Detailed help for <destination> not available.`

To log messages in a specific log, give the keyword LOGGER followed by a filename. Give the keyword DEFAULT_LOG to log messages in the default log.

To send messages to users and display them at terminals, use the DISPLAY keyword followed by a user name, user number, or line number.

To ignore messages, specify the DISCARD keyword.

The full syntax of the LOGGER and DISPLAY destinations is described later in this chapter.

Other Destinations

Other destinations may be available on your system, if you have other system management products installed. For details of the syntax for other destinations, refer to the documentation for those products.

The standard UMH destinations are described in the following sections.

LOGGER logfile

To log messages, use the keyword LOGGER followed by a logfile filename. Logs can be private or system.

To specify the logfile, use the following syntax:

pathname [{**-PRIVATE_LOG** | **-PLOG**}] [{**-SYSTEM_LOG** | **-SLOG**} **[node]**]

If you do not specify -PRIVATE_LOG, -SYSTEM_LOG is assumed.

If you specify a system log, it should already have been created on the system, using the ADMIN_LOG -CREATE command. If it does not exist, messages cannot be directed to it, and are recorded instead in the UMH undelivered log (pathname DSM* > LOGS > UMH > UNDELIVERED_LOG).

Specify private logs using the -PRIVATE_LOG option and a normal pathname. If the log does not already exist, it is created for you. If the log is on a remote disk, the disk should be added to the system on which you are defining the selection.

Specify system logs using a pathname beginning with DSM*>LOGS (-SYSTEM_LOG is optional; a system log is assumed unless you specify -PRIVATE_LOG). The disk partition name is not required and should not be supplied. To direct messages to a system log on a remote node, specify the system's PRIMENET node name. If you do not specify a node, the local node is assumed.

DISPLAY target [options]: To send messages to users or display them at terminals, use the DISPLAY facility. This allows you to route messages for display to any local or remote user within the configuration group, by specifying user name, user number, or line number.

Target can be either of the following:

Target	*Description*
USER {**name** / **number**}	Allows you to specify a particular user by user *name* or process *number*. The message is displayed in the same format as the PRIMOS MESSAGE command. If PRIMOS user names are not unique on your network, or if you wish messages to be directed to users whose login IDs are the same on several nodes, you should specify the node using the -ON node option.
{**-ASSIGNED_LINE number** / **-ASLN**}	Allows you to direct messages to a device on an assigned line, by specifying the line *number* in octal.

Options to DISPLAY allow you to specify the node on which to display the message, and the display format. The descriptions of the options follow.

Option	*Description*
-ON [node]	Allows you to direct display to a particular *node*. If the option is omitted, the local node is assumed.
{**-FORMAT** / **-FMT**} {**BRIEF** / **FULL**}	Allows you to choose the display format. BRIEF format displays the message's origin and severity, and tells you when it was logged. FULL displays this information plus any descriptive text that accompanies it. The default format is FULL.

DISCARD: To ignore messages, specify the keyword DISCARD.

DISCARD allows you to force messages to be ignored. When you are defining a selection and you specify DISCARD as a destination, any previously defined destinations in that selection are ignored, and the system automatically terminates the CONFIG_UM session for that selection definition.

Note

For a message to be truly discarded, *all* selections that cover the message must specify the destination DISCARD. Messages are often the subject of more than a single selection, and may be logged or displayed elsewhere. Where there are no alternative selections, the message is discarded and cannot be recovered.

DEFAULT_LOG: Messages whose destination is not specified in any selection are sent to the DEFAULT_LOG destination. You can also force messages to be sent to DEFAULT_LOG by specifying this as the destination in a selection. It is the system log with the pathname DSM* > LOGS > UMH > DEFAULT.LOG.

When you have completed a selection definition, you are asked whether you would like to review it before it is activated. To review the selection, step through it line by line using the RETURN key, and correct any typing errors, modify existing parameters, or add new lines, using PRIMOS command-line editing.

If you choose not to review the selection, it is immediately configured on the system. It then remains in force across system failures and cold starts until it is modified or canceled.

Example Selection

This section contains the dialog of a CONFIG_UM session in which a simple UMH selection is defined on a system that acts as a PSDN gateway.

In this dialog, a network administrator routes all ALARM and WARNING messages from PRIMENET, Name_server, and the customer product LOGIN_MANAGER, to his terminal, and to a local system log. The local log DSM* > LOGS > NETWORKS > ALARMS already exists.

The system's name is SYSA, and the administrator works under the user name SYSOPR.

```
OK, CONFIG_UM NETWORK_ALARMS -CR -ON SYSA
[CONFIG_UM Rev. 23.0.0 Copyright (c) 1990, Prime Computer, Inc.]
Prime Product: H
Prime product name must be the name of a Prime application
registered with DSM or -ANY, the applications available are:
ADMIN_LOG        LOGGER           RESUS
ASYNC             LOG_COLD         SCREEN_HANDLER
BATCH             LOG_DISK         SIM
CONFIG_DSM        LOG_MISC         SPOOLER
CONFIG_UM         LOG_OVFL         START_DSM
CONTROLLER_DLL    LOG_SEG4         STATUS_DSM
CONTROLLER_ULD    LOG_UNKN         STOP_DSM
DASHBOARD         LTP              SYSTEM_MANAGER
DISPLAY_LOG       NAME_SERVER      SYSTEM_RESOURCE_MONITOR
DISTRIBUTE_DSM    NMSR             TCP/IP
DRM               NPX              THRESHOLD_MONITOR
DSM               NSA              UMH
FTS               OSINM            ICS
PRIMENET          PRIMOS           PROGRAMMED_ACTION
Prime Product: PRIMENET
Prime Product: NMSR
Prime Product: <RETURN>
Customer Product: H
Customer product name must be the name of a customer application
registered with DSM or -ANY, the applications available are:
LOGIN_MANAGER, MAIL
Customer Product: LOGIN_MANAGER
Severity: H
Valid severities are:-
SECURITY
ALARM
WARNING
INFORMATION
FAILURE
DIAGNOSTIC
ACCOUNTING
STATISTIC
Severity: ALARM
Severity: <RETURN>
Severity: WARNING
Severity: <RETURN>
Destination: H
Valid destinations are:-
DISCARD
DEFAULT_LOG
LOGGER
DISPLAY
ACTION (Chargeable product)
DASHBOARD (Chargeable product)
Destination: DISPLAY -USER SYSOPR -ON SYSA
Destination: LOGGER DSM*>LOGS>NETWORKS>ALARMS -SLOG SYSA
Do you wish to edit this selection ? Y
Selection Name: NETWORK_ALARMS <RETURN>
Prime Product: PRIMENET <RETURN>
Prime Product: NMSR <RETURN>
Prime Product: <RETURN>
Customer Product: LOGIN_MANAGER <RETURN>
Customer Product: <RETURN>
Severity: ALARM <RETURN>
Severity: WARNING <RETURN>
Severity: <RETURN>
Destination: DISPLAY -USER SYSOPR -ON SYSA <RETURN>
```

```
Destination: LOGGER DSM*>LOGS>NETWORKS>ALARMS -SLOG SYSA<RETURN>
Do you wish to edit this selection ? NO
Configuring NETWORK_ALARMS on SYSA
Completed OK
OK, CONFIG_UM NETWORK_ALARMS -LIST
[CONFIG_UM Rev. 23.0.0 Copyright (c) 1990, Prime Computer, Inc.]
Selection Name: NETWORK_ALARMS
Prime Product: PRIMENET
Prime Product: NMSR
Customer Product: LOGIN_MANAGER
Severity: ALARM
Severity: WARNING
Destination: DISPLAY -USER SYSOPR -ON SYSA
Destination: LOGGER DSM*>LOGS>NETWORKS>ALARMS -SLOG SYSA
OK,
```

6

LOG ADMINISTRATION AND DISPLAY

Introduction

This chapter describes the log administration and display commands ADMIN_LOG and DISPLAY_LOG. For a general description of DSM logging, see Chapter 2, Administration and Security.

The ADMIN_LOG Command

ADMIN_LOG is the command that you use to create and administer DSM logs. Command-line options allow you to

- Create DSM logs, and specify their attributes.
- Modify the attributes of existing logs.
- List the attributes of existing logs.
- Purge logs of unwanted messages.
- Delete logs.

The syntax of the command follows.

▶ **ADMIN_LOG filename [logtype] subcommand [attributes]**

A filename is required with all options except -HELP and -USAGE.

logtype is optional. If you do not specify a log type, a system log is assumed. You must specify one, and only one, subcommand.

Descriptions of all the parameters and attributes, follow.

Option	*Description*
filename	A PRIMOS filename. To specify a private log, use the-PRIVATE_LOG option and give any pathname except one beginning with DSM* > LOGS. To specify a system log, give a pathname beginning with DSM* > LOGS. Either give a full pathname, or attach to DSM* > LOGS and give a relative pathname. When specifying a full pathname, the disk partition is not required and should not be supplied.
Type of Log	*Description*
{**-PRIVATE_LOG** | **-PLOG**}	Specifies a private log. To access a private log you *must* specify -PRIVATE_LOG. If you do not, a system log is assumed. To administer a private log, you must have access to the DSM function PRIVATE_LOGGER, on the node where the file resides. For details of DSM security, see Chapter 2, Administration and Security.
{**-SYSTEM_LOG** | **-SLOG**} [{**node** | **nodegroup**}]	Specifies a system log. To reference system logs on remote nodes, specify *node* or *nodegroup.* -SYSTEM_LOG is the default. To administer system logs, you must have access to the DSM function SYSTEM_LOGGER on the node where the files reside. For details of DSM security, see Chapter 2, Administration and Security.
Subcommand	*Description*
{**-CREATE** | **-CR**} **attributes**	Creates a log with the specified *attributes.* Attributes that are not explicitly defined, are set to defaults. For a description of log file attributes and their defaults, see later in this chapter. **Note** You can only create system logs on the directory DSM* > LOGS or any subdirectory of it. Private logs can be created anywhere you have access, *except* under DSM* > LOGS.
{**-MODIFY** | **-MOD**} **attributes**	Changes the *attributes* of a log. Give new values for any or all of the attributes on the command line. This option does not alter the cyclic/linear attribute, which is fixed for the lifetime of the log when it is created.

-PURGE { **age** / **ALL** }

Immediately purges a log of messages that are at least *age* days old, whatever purge time is set. For example, if you specify an age of 1 day, all messages that are 24 hours or more old are deleted.

Permitted arguments to -PURGE are ALL, and integers in the range 1-365. If you specify ALL, all messages are deleted. If you give no argument, all messages older than the current retention time are deleted. If the retention time is infinite, no messages are deleted, and an error message is displayed.

-DELETE

Deletes a log. Use in preference to the DELETE command.

-LIST

Displays the attributes of a log, its current size in disk records, and the age of its oldest message.

{ **-HELP** / **-H** } [{ **-NO_WAIT** / **-NW** }]

Explains how to use the command. This option cancels any others on the command line. If -NO_WAIT is specified, display is not paginated at your terminal. Similar help information is available using the PRIMOS HELP subsystem.

-USAGE

Gives you the command syntax in brief. This option cancels all others on the command line.

Descriptions of the log attribute options follow.

Attribute	*Description*
{ **-MAXIMUM_SIZE** / **-MXSZ** } **records**	Sets the maximum size of the log in disk records (2 Kbytes). Permitted values for *records* are zero and 1-32767. A value of zero is interpreted as unlimited maximum size. The default is 50 records.
{ **-MINIMUM_SIZE** / **-MNSZ** } **records**	Sets the minimum size of the log, in disk *records* (2 Kbytes). Permitted values are 1-32767. A value of zero is invalid. The default is one record.
{ **-WARNING_LEVEL** / **-WL** } **percent**	Defines a level of occupancy at which messages are generated to warn you that the log is approaching its maximum size. *Percent* is a percentage of the maximum size in disk records. A warning level can only be set where a maximum size has already been defined. The default is to set no warning level. A UM will be sent at 60 minute intervals if the warning level is exceeded but remains below the log full condition, and messages are still being written to the log. After a successful manual or automatic purge or when the maximum size of the log is increased the time counter is reset to zero.

{-CYCLIC / -CYC} — Defines the log as cyclic.

Note
Cyclic logs cannot be assigned a maximum size of zero.

{-LINEAR / -LIN} — Defines the log as linear. For a discussion of log types and how to use them, refer to Chapter 2, Administration and Security.

{-RETAIN / -RET} days — Defines how many days messages are to be held in the log before being deleted, where *days* is an integer in the range 1–365. If you specify no argument, messages are retained indefinitely, that is, until the log is deleted, purged using the -PURGE option, or, for cyclic logs, until messages are overwritten. The default is to retain messages indefinitely.

{-PURGE_TIME / -PTIM} hh:mm — Specifies the time of day when the log is purged. This option is only honored if a retention time has been set (see above). The default purge time is 01:00 (1 a.m.).

hh:mm must be in 24-hr format.

Default Log File Attributes

Unless you specify otherwise, log files are created with the following default attributes:

Maximum Size	50 Records
Minimum Size	1 Record
Warning Level	Undefined
Cyclic/Linear	Cyclic
Retention Time	Infinite
Purge Time	1 a.m.

The DISPLAY_LOG Command

DISPLAY_LOG allows you to select and display messages from private and system logs throughout the network. You can select messages by origin, severity message type and date/time recorded, display them at your terminal in different formats, or write them to disk.

Notes

The DISPLAY_LOG command can be used to read logs on your local system even when DSM is not started on the system. This enables you to consult the system event logs for diagnostic purposes if the service fails, or cannot be started.

To prevent unauthorized access to system logs when DSM is not started on the system, you should set appropriate ACLs on DSM*>LOGS.

From Rev. 21.0, you must use the DISPLAY_LOG command to display and print system and network event logs. PRINT_SYSLOG and PRINT_NETLOG can only be used on logs created prior to Rev. 21.0.

Options to DISPLAY_LOG allow you to

- Specify the log file to be displayed.
- Specify display parameters.
- Write the log, or messages selected from it, to a disk file.
- Select specific messages or categories of messages from the log. Parameters on which you can select messages are:
  - The *node* on which they were generated.
  - The *user* that generated them.
  - The *products* that generated them; these may be *Prime products*, or *customer products*, or a combination of both types of product.
  - The message *severity.*
  - The *date/time* logged.
  - A DSM *message ID.*

The syntax of the command follows.

DISPLAY_LOG { **filename [logtype]** / **-DEFAULT** / **-UNDELIVERED** } **[options]**

filename is a PRIMOS filename. Specify private logs using the -PRIVATE_LOG option and a normal pathname, and system logs using a full pathname beginning with DSM*>LOGS (or attach to DSM*>LOGS and specify a relative pathname). When specifying a full pathname for system logs, the disk partition is not required and should not be supplied.

When specifying the -DEFAULT or -UNDELIVERED options, a filename is not required and should not be supplied.

Descriptions of the options follow, in three functional groups: log options, message selection options, and formatting and other options.

Log Options

Option	*Description*
{**-PRIVATE_LOG** | **-PLOG**}	Defines the log as a private log. If you do not specify this option, the log is assumed to be a system log.
{**-SYSTEM_LOG** | **-SLOG**} [{**node** | **nodegroup**}]	Defines the log as a system log, which is also the default. If you do not specify a *node* or *nodegroup*, the local node is assumed.

Message Selection Options

The message selection options allow you to extract messages of particular types, origin, and severities from a log.

Note

In order to select the messages that you require, DSM reads the log in its entirety. For large logs, the read time may be extended.

Option	*Description*
-NODE nodenames	Allows you to specify a list of PRIMENET *nodenames*. The default is to display messages from *all* nodes.
-USER usernames	Allows you to specify a list of *usernames*. Remember that PRIMOS user names are not necessarily unique on the network; if you want to retrieve messages you must specify the user name and PRIMENET node for that user. The default is to display messages from *all* users.
{**-SEVERITY** | **-SEV**} **severities**	Allows you to specify a list of *severities*. For example, you might use this option to select all ALARM and WARNING messages from a subsystem. Valid severities are: ALARM, WARNING, INFORMATION, SECURITY, FAILURE, DIAGNOSTIC, ACCOUNTING, STATISTIC, DATA. The default is to display messages of *all* severities.

{-LOGGED_AFTER / -LAF} date/time

Allows you to select messages logged after a specific *date/time*. The format for *date/time* can be either ISO:

(YY-MM-DD.HH:MM:SS)

USA:

(MM/DD/YY.HH:MM:SS)

or Visual:

(DD MM YY HH:MM:SS)

Notes

If you specify neither -LAF or -LBF, *all* messages are displayed.

Options -LAF and -LBF select messages on the date/time they were logged, rather than when they were generated. These times may differ because of the transmission time over the network, especially if messages are logged on distant nodes. Where messages are directed to nodes in different time zones, the date/time reflects these differences.

{-LOGGED_BEFORE / -LBF} date/time

Allows you to select messages logged before a specific *date/time*. Acceptable formats for *date/time* are the same as those for the -LOGGED_AFTER option. For notes on the use of -LBF and -LAF, see above.

{-CUSTOMER_PRODUCT / -CPROD} products

Allows you to specify a list of customer product names. You will be warned if a product name is not a customer product

{-PRIME_PRODUCT / -PPROD} products

Allows you to specify a list of Prime product names. You will be warned if a product name is not a Prime product.

{-PRODUCT / -PROD} products

Allows you to specify a list of both Prime and customer product names. You will be warned if a product name is not registered. The default is to display messages from all DSM-registered *products*.

For information about the products and the kinds of messages they generate, see Appendix B.

{-MESSAGE_ID / -MSGID} message IDs

Allows you to specify a list of *message IDs*. Some DSM messages are assigned a message ID that identifies the message type. For example, SIM output messages are identified by message IDs that are identical to the corresponding SIM command, and PRIMOS and network events are identified by system codes.

The following is a list of DSM message IDs that you can use as arguments to the -MESSAGE_ID option:

BADENT	LIST_ASSIGNED_DEVICES
LIST_ASYNC	LIST_COMM_CONTROLLERS
LIST_CONFIG	LIST_DISKS
LIST_LAN_NODES	LIST_MEMORY
LIST_PRIMENET_LINKS	LIST_PRIMENET_NODES
LIST_PRIMENET_PORTS	LIST_PROCESS
LIST_SEMAPHORES	LIST_SYNC
LIST_UNITS	LIST_VCS
NETWORK_BADSEQ	NETWORK_COLD
NETWORK_DIAPKT	NETWORK_HDXBRS
NETWORK_HOSTDN	NETWORK_ICS_00
NETWORK_ICS_01	NETWORK_ICS_02
NETWORK_ICS_03	NETWORK_ICS_04
NETWORK_ICS_05	NETWORK_ICS_06
NETWORK_ICS_07	NETWORK_ICS_08
NETWORK_ICS_09	NETWORK_ICS_20
NETWORK_ICS_21	NETWORK_ICS_22
NETWORK_ICS_23	NETWORK_ICS_24
NETWORK_ICS_25	NETWORK_ICS_26
NETWORK_ICS_36	NETWORK_ICS_37
NETWORK_LCFAIL	NETWORK_LPE
NETWORK_NETDMP	NETWORK_NORCVB
NETWORK_NPXCLR	NETWORK_NPXCON
NETWORK_NPXETR	NETWORK_NPXPUA
NETWORK_NPXRCV	NETWORK_NPXRLS
NETWORK_NPXSEQ	NETWORK_NPXTHR
NETWORK_OVERFL	NETWORK_PKTFLT
NETWORK_RESET	NETWORK_RING1
NETWORK_RING2	NETWORK_RING3
NETWORK_RNGHRD	NETWORK_RNGRCV
NETWORK_RNGRES	NETWORK_RNGTMT
NETWORK_SYNC1	NETWORK_SYNC2
NETWORK_SYNC3	NETWORK_SYNC4
NETWORK_SYNC5	NETWORK_SYNC6
SYSTEM_CHECK	SYSTEM_COLD
SYSTEM_DISKER	SYSTEM_DSKNAM
SYSTEM_ECCULO	SYSTEM_ERRCHK
SYSTEM_FORCDN	SYSTEM_OVERFL
SYSTEM_PACL	SYSTEM_QUIET
SYSTEM_SENSOR	SYSTEM_SETIME
SYSTEM_TYPE10	SYSTEM_TYPE11
SYSTEM_TYPE12	SYSTEM_TYPE13
SYSTEM_TYPE14	SYSTEM_TYPE15
POWERF	REMARK
SHUTDN	WARM

Other Options

Option	*Description*
{-FORMAT / -FMT} {BRIEF / FULL / format-name}	Allows you to choose one of several display formats:

BRIEF gives you the message data in summary format, and is most suitable for unsolicited messages. For messages that contain considerable information, such as SIM output messages, use FULL or *format-name*.

FULL displays the contents of all fields and records in each message. The format reflects the internal structure of the message and may require skilled interpretation.

format-name allows you choose a tabulated format for SIM output messages. There is a format for each SIM command, and some additional formats for detailed displays. If you specify one of these formats, only messages of the appropriate type are displayed.

Choose the appropriate format for the SIM messages you wish to display from the following list:

LIST_ASSIGNED_DEVICES	LIST_ASYNC
LIST_ASYNC_DETAIL	LIST_COMM_CONTROLLERS
LIST_CONFIG	LIST_DISKS
LIST_LAN_NODES	LIST_LAN_NODES_DETAIL
LIST_MEMORY	LIST_PRIMENET_LINKS
LIST_PRIMENET_NODES	LIST_PRIMENET_PORTS
LIST_PROCESS	LIST_PROCESS_DETAIL
LIST_SEMAPHORES	LIST_SEMAPHORES_DETAIL
LIST_SYNC	LIST_UNITS
LIST_UNITS_DETAIL	LIST_VCS
LIST_VCS_DETAIL	

The default format is BRIEF. Examples of BRIEF, FULL and tabular formats can be found at the end of this chapter.

-NOHEADER Suppresses display of all the message header information. The text of the message is unaffected. Useful for simulating pre-Rev. 21.0 event log displays. The default is to display full header information.

-CENSUS [**Product** | **Node** | **Severity** | **Rev21**]

Lists a count of messages under the parameter specified. If no parameter is specified the default is Product. The Rev. 21 parameter will report LOGREC/NETREC messages and is compatible with a node running pre-Rev. 23 DSM. The other parameters are compatible with nodes running Rev. 23 DSM.

-REMARK [comment]

Allows you to add a comment to the file, of maximum length 160 characters. All characters typed after the keyword -REMARK, are entered onto the file, so that -REMARK must be the last or only option on the command line.

filename [{**-NO_QUERY** | **-NQ**}]

The write-to-file option. Allows you to write output to a named disk file. If you specify -NO_QUERY, files that already exist are overwritten with no warning.

{**-NO_WAIT** | **-NW**}

Allows you to suppress screen pagination at the terminal. If you specify -NO_WAIT, messages are presented in a continuous stream that you can suspend and resume with PRIMOS XON/XOFF.

{**-HELP** | **-H**} [{**-NO_WAIT** | **-NW**}]

Explains how to use the command. This option cancels any other options on the command line. If you specify -NO_WAIT, the display is not paginated at your terminal. The same information is available through the PRIMOS HELP subsystem.

-USAGE

Gives you the command syntax in brief. This option cancels all others on the command line.

DISPLAY_LOG Examples

Displaying a Log

To display a log, simply type DISPLAY_LOG followed by a filename. Each message in the log is displayed complete with the message header, as in the following example:

```
OK, DISPLAY_LOG DSM*>LOGS>PRIMOS>PRIMOS.LOG
[DISPLAY_LOG Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]

*** Message from product LOG_COLD, generated by SYSTEM_MANAGER on SYS1
    (Severity Information, occurred at 15 Jun 90 08:59:32 Wednesday)
COLD START PRIMOS <REV.No.>  CPU TYPE = 9955
MICROCODE REV = 13
PROCESSOR ID = 000000 000022 000010 000015 000000 000000 000000 (OCT)

*** Message from product DSM, generated by SYSTEM_MANAGER on SYS1
    (Severity Information, occurred at 15 Jun 90 08:59:28 Wednesday)
DSM Server is now in steady state.
```

```
2 messages retrieved from log
OK,
```

Displaying Message Text Only

To suppress the message header, and display the text of the message only, use the option -NOHEADER, as in the following example:

```
OK, DISPLAY_LOG DSM*>LOGS>PRIMOS>PRIMOS.LOG -NOHEADER
[DISPLAY_LOG Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]

COLD START PRIMOS <REV.No.> CPU TYPE = 9955
MICROCODE REV = 13
PROCESSOR ID = 000000 000022 000010 000015 000000 000000 000000 (OCT)

DSM Server is now in steady state.

2 messages retrieved from log
OK,
```

Displaying a Summary of Messages

To produce a summary of the log's contents, use the -CENSUS option, as in the following example:

```
OK, DISPLAY_LOG DSM*>LOGS>PRIMOS>PRIMOS.LOG -CENSUS
[DISPLAY_LOG Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]

Prime product name              Count

   LOG_COLD                         1
   UNKNOWN                          1

2 messages retrieved from log
OK,
```

Selecting Messages of Specific Types

Most system logs will contain many more messages than there are in the above example. To select specific messages and categories of messages, use the message selection options.

To display only system cold start messages, use the -MESSAGE_ID SYSTEM_COLD option, as in following example:

```
OK, DISPLAY_LOG DSM*>LOGS>PRIMOS>PRIMOS.LOG -MSGID SYSTEM_COLD
[DISPLAY_LOG Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]

*** Message from product LOG_COLD, generated by SYSTEM_MANAGER on SYS1
    (Severity Information, occurred at 15 Jun 90 08:59:32 Wednesday)
COLD START PRIMOS <REV.No.> CPU TYPE = 9955
MICROCODE REV = 13
PROCESSOR ID = 000000 000022 000010 000015 000000 000000 000000 (OCT)
```

```
1 messages retrieved from log
OK,
```

FULL Format

The following example illustrates the FULL format for DSM message display.

```
OK, DISPLAY_LOG DSM*>LOGS>PRIMOS>PRIMOS.LOG -FMT FULL
[DISPLAY_LOG Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]

Occurred at: 15 Jun 90 08:59:32 Wednesday
Message Header:
   Sending User: SYSTEM_MANAGER
   Sending Node: SYS1
   Severity: Information
   Product Id: LOG_COLD
Message Body:
INTERNATIONALISED_MESSAGE =
COLD START PRIMOS <REV.No.> CPU TYPE = 9955
MICROCODE REV = 13
PROCESSOR ID = 000000 000022 000010 000015 000000 000000 000000 00000 (OCT)

Occurred at: 15 Jun 90 08:59:28 Wednesday
Message Header:
   Sending User: SYSTEM_MANAGER
   Sending Node: SYS1
   Severity: Information
   Product Id: DSM
Message Body:
INTERNATIONALISED_MESSAGE =
DSM Server is now in steady state.

2 messages retrieved from log
OK,
```

SIM Messages

Output from SIM commands can be displayed in BRIEF, FULL or tabulated formats. The following examples illustrate each of these types of display, using logged output from the LIST_ASSIGNED_DEVICES command shown below:

```
LIST_ASSIGNED_DEVICES SMLC@ -ON SYS2 -PLOG <filename>
```

BRIEF Format

```
OK, DISPLAY_LOG <filename> -PLOG -FMT BRIEF
[DISPLAY_LOG Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]

*** Message from product SIM, generated by DSMASR on SYS2
    (Severity Data, occurred at 16 Jun 90 13:36:44 Thursday)
SMLC00
```

```
50
server
NETMAN

1 messages retrieved from log
OK,
```

FULL Format

```
OK, DISPLAY_LOG <filename> -PLOG -FMT FULL
[DISPLAY_LOG Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]

Occurred at: 16 Jun 90 13:36:44 Thursday
Message Header:
   Sending User: DSMASR
   Sending Node: SYS2
   Severity: Data
   Product Id: SIM
Message Body:
LIST_ASSIGNED_DEVICES
[Private 511] Sequence
   CharString = SMLC00
   [Private 502] Sequence
      ShortInteger = 50
      DSM Internationalised Message = server
      CharString = NETMAN

1 messages retrieved from log
OK,
```

TABULATED Format

```
OK, DISPLAY_LOG <filename> -PLOG -FMT LIST_ASSIGNED_DEVICES
[DISPLAY_LOG Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]

DATE-TIME LOGGED: 90-06-16.13:36:44.Thu
DATA FROM NODE:   SYS2

Device        User    User       User
Name          Number  Type       Name

SMLC00        50      server     NETMAN
```

Recovery of Corrupt Logs

Because of the nature of DSM log files, there are certain circumstances that can cause the file to become corrupted: a machine crash during a write operation, for instance, or extraneous data being transmitted to the storage device. At PRIMOS Rev. 22.0 and all subsequent revisions, the logfile is structured so that DSM can recognise and recover corrupt logfiles.

This recovery action may involve adjusting internal pointers to point to valid data, or skipping records which contain corrupted data. In all circumstances, details of corruption encountered and recovery action taken are written to the DSM_LOGGER journals in DSM*>JOURNALS; these files should be checked periodically.

Usually, any action taken will be permanent, and as files wrap round (in the case of CYCLIC logs), or are purged, either manually or automatically, any corrupted data is removed. However it is advisable to delete, using ADMIN_LOG -DELETE, and recreate, using ADMIN_LOG -CREATE, any files which seem to suffer from frequent corruption.

7

SYSTEM INFORMATION/METERING

Introduction

This chapter describes the SYSTEM INFORMATION/METERING (SIM) commands and options. The first section describes the PRIMOS command line user interface to SIM and gives detailed descriptions of the general SIM options. This is followed by the main part of the chapter, which is a detailed description of each of the SIM commands and their options.

System Information/Metering (SIM) Commands and Options

The System Information and Metering (SIM) commands allow system operations staff, such as operators, system programmers, and experienced end users, to obtain information about the state and performance of a network of computer systems. These commands provide system control data for all nodes on the network simultaneously, and offer administrative staff a view of the network as a whole, rather than as a set of loosely associated systems.

In general, SIM offers a mechanism that collects and presents system information. A number of the commands provide access to information not previously available, while others overlap, but do not replace, areas currently covered by the system-monitoring STATUS command.

SIM presents information in a concise and compact fashion convenient for the system specialist, and therefore assumes a degree of technical knowledge and expertise. No attempt is made to interpret data.

There are fifteen SIM commands:

LIST_ASSIGNED_DEVICES	List assigned devices
LIST_ASYNC	List asynchronous terminals
LIST_COMM_CONTROLLERS	List comms controller configurations
LIST_CONFIG	List PRIMOS configuration directives
LIST_DISKS	List logical disks (partitions)
LIST_LAN_NODES	List local area networks
LIST_MEMORY	List physical memory usage
LIST_PRIMENET_LINKS	List PRIMENET status
LIST_PRIMENET_NODES	List PRIMENET configured nodes
LIST_PRIMENET_PORTS	List assigned PRIMENET ports
LIST_PROCESS	List processes
LIST_SEMAPHORES	List semaphores in use
LIST_SYNC	List synchronous line configurations
LIST_UNITS	List users' open file units
LIST_VCS	List active virtual circuits

Command/User Interface

SIM commands are like special-purpose PRIMOS commands, that you use to determine system status. They exist in the CMDNC0 directory, and access to them can be controlled in the normal way using ACLs. In addition, DSM security can be used to afford additional protection over the network. You can use SIM commands on the local node to obtain local system information, on remote nodes to give a wider view of the network, and on several nodes at once.

Display Formats

SIM information is displayed in a concise way, the exact format depending on the command and your choice of options. Most displays are in the form of tabulated lists or formatted screen pages.

Some commands use two levels of display, one brief and one detailed. Detailed displays appear when you request information about specific items, such as disks, and when you specify the -DETAIL option. The brief display is usually the default if you do not specify any options.

Where you do not request information about specific items, the display normally consists of a list of all items in the group, with a brief summary or subset of the available information. The summary display can be used initially to determine names, numbers, and IDs, before selecting items for more detailed display, or can be used simply as a summary of status.

Where displays extend over more than one screen page (23 lines), the display pauses between each page, and the system prompts:

```
-- More --
```

To display the next 23 lines of a target node's data you can respond with:

```
YES, Y, OK, RETURN
```

To end the current target node's response, and skip to the next target node's data, you can respond with:

```
SKIP
```

To end the display for the current command execution, you can type:

```
NO, N, QUIT, or Q
```

If you have specified command repetition options, the display resumes on the next command execution.

To cancel a repeated command and return to PRIMOS, you can respond with:

```
ABORT
```

When you invoke a SIM command on several nodes, it is directed to the target nodes, and the resulting output is displayed for each node in turn. The sequence in which the node's outputs are displayed depends on the sequence in which each responds to the command; this in turn depends on a node's status at the time a command is initiated. If a target node fails to respond, an exception message is displayed.

Parameter Lists

Arguments to SIM commands, and arguments to command options, are limited to a maximum of 10 on the command line.

If you exceed the parameter limit for command options, the extra arguments are treated as command arguments. This may cause the command to abort because of incorrect syntax. To avoid this, use wildcarding on arguments. A wildcarded argument is treated as a single parameter and can be used to extend the number of items that can be specified in a parameter list.

Integer Ranges

Where indicated, integer ranges are accepted in place of numerical arguments. To specify integer ranges, use the syntax:

```
n:m
```

where *n* is the start of the range and *m* is the end of the range. If you specify the start of a range without the end of the range, or vice versa, the range is assumed to

extend indefinitely. In practice, the range are limited by the range of integers that the command accepts.

For example:,

- the range *:3* specifies all integers, up to and including 3, that the command accepts.
- the range *3:* specifies all integers from 3 to the largest integer that the command accepts.

Note

You cannot use the colon alone as shorthand for *all* integers.

In a parameter list, integer ranges and single integers can be freely intermixed with one another, up to the command-line parameter limit.

Inter-Rev. Compatibility

SIM commands can be invoked between systems that are running different major revisions of PRIMOS. However, options that are introduced at later revisions may not be available on earlier revisions.

If you attempt to invoke a new option on a system that does not support it, the command aborts with incorrect syntax, and an error message is displayed.

General and Specific Options

All SIM commands support a set of general SIM options that can be used with any of the commands; these are described in the next section General SIM Options. Many commands also support specific options and/or arguments; these are described in the subsequent sections that deal with each command.

General SIM options support:

- Simultaneous invocation of a command on several nodes.
- Logging of output to private or system logs.
- Periodic invocation of commands.

Descriptions of the general SIM options follow.

General SIM Options

Option	*Description*
-ON { node / nodegroup }	Allows you to specify the *node* or *nodegroup* to which the commandis to be directed. The default is to direct the command to the node on which the command is invoked.
{ -PRIVATE_LOG / -PLOG } pathname [-NTTY]	Allows you to record SIM output in a DSM private log. To use private logging, you must have access to the PRIVATE_LOGGER function and user DSM_LOGGER should have *all* access to the directory that contains the log. If the log does not already exist, it is created for you.
{ -SYSTEM_LOG / -SLOG } pathname [-NTTY]	Allows you to record SIM output in a local system log. Specify a *pathname* starting with the prefix DSM* > LOGS, and do not give a disk partition. The log must already exist on the system. To use system logging, you must have access to the SYSTEM_LOGGER function. For further information about DSM logs and logging, see Chapter 2, Administration and Security. -NTTY can be used with the -PRIVATE_LOG and -SYSTEM_LOG options, and indicates that no data is to be displayed to the user. **Note** The -NTTY option starts a phantom under your user name. Errors are logged in a comoutput file on your login directory, so you must have write (W) access there.
-FREQ [seconds]	Provides periodic execution of the command. The interval you specify is the interval between two successive executions of a command, and not the interval between completion of the command's display and the next execution. Intervals are corrected to the nearest multiple of four seconds below the specified interval. If FREQ 0 is specified, the command is reexecuted immediately the previous execution is complete. If the interval elapses before the previous display is complete, the next execution is delayed until the display is complete. This option is used in conjunction with the -TIMES, -START, and -STOP options, to implement periodic execution of a command.

-TIMES [number]

Use in association with the -FREQ option, to set a limit on the *number* of times that a command is to be executed. Use in conjunction with -START, and -STOP options, to implement periodic execution of a command.

-START [date/time]

Sets the *date/time* that execution starts. Use in conjunction with -TIMES, and -STOP options, to implement periodic execution of a command. The format can be in either ISO standard as follows:

(YY-MM-DD.HH:MM:SS)

or USA standard

(MM/DD/YY.HH:MM:SS)

The default is to start immediately.

-STOP [date/time]

Sets the *date/time* execution stops; format and defaults are the same as for -START. Use in conjunction with -TIMES, and -START options to implement periodic execution of a command.

In the absence of any of these four options, the command is executed once, and immediately.

In the presence of any of these four options, the defaults applied to the unspecified options are

-FREQ immediate reexecution
-TIMES infinite
-START now
-STOP never

{-NO_WAIT / -NW}

Indicates that you are not to be prompted or queried during the command output display.

If this option is not used, you are prompted between every 23 lines (1 screen page) of output display.

{-HELP / -H} [{-NO_WAIT / -NW}]

Explains how to use the command. This option cancels any other options on the command line. If you specify -NO_WAIT, the display is not paginated at your terminal. The same information is available through the PRIMOS HELP subsystem.

-USAGE

Gives you the command syntax in brief. This option cancels all others on the command line.

SIM Commands and Command-line Options

This section describes each of the SIM commands in detail. The command syntax is given and a brief description of the command. This is followed by a description of the command-line options.

The LIST_ASSIGNED_DEVICES Command

▶ **LIST_ASSIGNED_DEVICES [options]**

The LIST_ASSIGNED_DEVICES command displays all the devices that have been assigned on a system through the ASSIGN command (see *PRIMOS Commands Reference Guide*).

The command options include both the general SIM options described earlier in this chapter, and command-specific options which are described below.

There are two command-specific options to this command. These options allow you to determine the subset of the information displayed. You can use them singly, or in combination to make the subset more specific.

Descriptions of the options follow.

Option	*Description*
device names	Allows you to specify a list of assignable device names. Only assigned devices specified in the list are displayed. The default is *all* devices that are currently assigned on the system. Wildcarding can be used. Some assignable devices follow. For a full list of assignable device names, refer to the *PRIMOS Commands Reference Guide*, ASSIGN command.

Device Code	*Meaning*
ASYn	Asynchronous communications line (0≤n≤2047).
CARDR	MPC parallel card reader or CRn (0≤n≤1) reader/punch.
DISKpdisk	Physical partition: *pdisk* is a partition (volume) number, specified in octal; there should be no space between the keyword DISK and the number.
GS0 - GS3	Vector General graphics display terminal.
MG0 - MG3	Megatek graphics display terminal.
MTn (0≤n≤7)	Magnetic tape unit.
PRn (0≤n≤3)	Line printer.
PTR	Paper tape reader.

PUNCH	Paper tape punch.
LOT	Printer/plotter.
SYNCn	Synchronous communications line (00≤n≤07). Line numbers are in decimal.

Note

ASY and SYNC are logical devices. Physical device names such as MDLC, HSSMLC, and ICS2 are not permitted.

-USER | **names** | **numbers** |

This option allows you to specify a list of users, by name or by number. Only devices assigned to the listed users are displayed. Wildcarding can be used on user names, and ranges of user numbers can be specified.

The default is to display devices assigned to *all* users.

▶ LIST_ASYNC [options]

The LIST_ASYNC command displays the status and configuration of any or all of the system's asynchronous lines. Asynchronous lines can be in one of three modes:

Mode	*Meaning*
LOGIN	The line is available for login.
ASSIGNED	The line is assigned to a user.
FREE	The line is available for assignment.

This command also displays terminals attached to the Local Area Network (LAN). For further information on assigned lines, see the AMLC section in the *System Administrator's Guide, Vol. II, Communications Lines and Controllers.*

The command options include both the general SIM options described earlier in this chapter, and command-specific options which are described below.

Three command-specific options determine the subset of the information displayed, and allow you to select detailed information. They can be used singly, or in combination, to make the subset more specific.

Descriptions of the options follow.

Option	*Description*
line numbers	Allows you to specify a list of asynchronous line numbers, as decimal integers. Ranges of line numbers can be specified. The command accepts integers in the range 0–32767. For line numbers on your system, consult your System Administrator. The default is to display information about logged in and assigned lines only.
-USER { **names** | **numbers** }	Allows you to specify a list of user *names* and *numbers*. Wildcarding can be used on user names, and ranges of user numbers can be specified. The default is to display *all* users.
{ **-DETAIL** | **-DET** }	Displays detailed information about the asynchronous line configuration. The default is to display a list of line numbers, with brief configuration data, and user assignments.

▶ LIST_COMM_CONTROLLERS [options]

The LIST_COMM_CONTROLLERS command displays information on communications controllers present in a system, including the LAN300 Host Controller (LHC300), but excluding the Prime Node Controller (PNC). Information is given for each controller and includes: controller name, its type, its device address, the number of synchronous lines attached, and the number of asynchronous lines attached.

Refer to the *System Administrator's Guide Vol. II, Communication Lines and Controllers* for details of Prime communication controllers.

The command options are the general SIM options described earlier in this chapter. There are no command-specific options.

▶ LIST_CONFIG [options]

The LIST_CONFIG command displays the cold-start values, default values, and current values of those system variables that can can be set by configuration directives at cold start.

The cold-start values are as specified in the configuration file, usually named CONFIG. Default values are those set by PRIMOS when there is no cold-start value. Current values may differ from both the cold-start and default values; this difference can either be because PRIMOS allows the cold-start and default values to be modified subsequent to cold start, or because the specified cold-start value was illegal, and PRIMOS has used an alternative upper or lower boundary value, which is not the default value.

The command selects the directives it displays. It does not return values set by the AMLBUF, SYNC, ICS, or LHC directives because these directives are set on a per line, per controller basis, rather than on a system basis, and may in any case be determined by other LIST commands, such as LIST_ASYNC and LIST_SYNC. Further, the command does not return

the values of directives that are only significant at cold start, such as VPSD, TYPOUT or WIRMEM.

The command options include both the general SIM options described earlier in this chapter, and one command-specific option which is described below. This option determines a subset of the information that is to be displayed.

A description of the option follows.

Option	*Description*
directive names	Allows you to specify a list of *directive names*, and displays the cold-start values, default values, and current values of those system variables that can be set by the configuration directives listed; directives are not displayed if they are not specified on the list. Wildcarding can be used. The default is *all* directives. For more detailed information on directives, refer to the *System Administrator's Guide, Vol. I, System Configuration.*

▶ LIST_DISKS [options]

The LIST_DISKS command displays information about local and remote disks that are added to the system, including partition names, numbers and size, record availability and partition type.

Using the command-specific options you can display information about users of disk partitions, select information about local and remote disks, and select a detailed display.

The command options include both the general SIM options described earlier in this chapter, and command-specific options which are described below.

There are five command-specific options to the LIST_DISKS command, each of which selects a subset of information to be displayed. They can be used singly, or in combination, to make the subset more specific.

Descriptions of the options follow.

Option	*Description*
disknames **ldev numbers**	Allows you to specify a list of local or remote disks by *diskname* or *ldev number* (logical device number). *ldev number* must be specified in *octal*. Wildcarding can be used on disk names, and ranges of ldev numbers can be specified. For remote disks, the system name, logical device number and locally logged-in users of the disks are displayed. The default is to display brief information on *all* disks.

-LOCAL — Selects local disks only. If you do not specify any disk names, brief information is displayed for *all* local disks.

-REMOTE [nodenames] — Selects remote disks only. To select disks on specific nodes, specify a PRIMENET node name. The default if you do not specify a node name is to display brief information about *all* remote disks.

Note

These options give you information about local and remote disks that are added on the system where you invoke the command, not about disks added on remote systems. To obtain information about added disks on remote systems, use the general SIM option *-ON node*.

-USERS — Displays detailed information about users on the specified disks. For local disks, all users are displayed; for remote disks, only locally logged-in users of the remote disks are displayed. If you do not give a disk name, detailed information is displayed about *all* disk users.

{-DETAIL / -DET} — Allows you to request detailed information. The default is an overview display.

▶ LIST_LAN_NODES [options]

The LIST_LAN_NODES command displays information about the configured local area networks. The command options include both the general SIM options described earlier in this chapter, and command-specific options which are described below. There are three command-specific options to the LIST_LAN_NODES command. These options determine the subset of the information displayed. They can be used singly, or the first can be used in combination with either the second or third, but not both, to make the subset more specific. Descriptions of the options follow.

Option — *Description*

lan names — Allows you to specify a list of *lan names*. *lan names* are the names of the LAN networks to which the node is connected. Wildcarding can be used.

The default is *all* LAN names.

-HOST — Allows you to display information about LAN *hosts*.

-LTS — Allows you to display information about LTSs.

For details of LAN hosts and LTSs, see the *NTS User's Guide*.

To display all available information about LAN networks, specify both -HOST and -LTS.

▶ LIST_MEMORY [options]

The LIST_MEMORY command displays current memory usage. It displays the number of segments, resident pages, and wired pages per user process; users are identified by name and number.

The command options include both the general SIM options described earlier in this chapter, and command-specific options which are described below.

There are two command-specific options to LIST_MEMORY. These options determine the subset of the information displayed. They can be used singly, or in combination, to make the subset more specific.

Descriptions of the options follow.

Option	*Description*
{**usernames** | **usernumbers**}	Allows you to specify a list of *usernames* or *usernumbers*. Wildcarding can be used on user names, and ranges of user numbers are accepted. The default is *all* logged-in users.
-TYPE usertypes	Allows you to specify a list of *usertypes*. Valid user types are terminal remote slave server batch child phantom The default is to display *all* user types.

▶ LIST_PRIMENET_LINKS [options]

The LIST_PRIMENET_LINKS command displays the status of PRIMENET links, where a link can be a PRIMENET configured SYNC line, a PRIMENET configured node on a ring, or a LAN network. For each link, the command displays the node or public data network to which it is connected, the number of active virtual circuits on the link, and the availability of the link for traffic routing.

The command options include both the general SIM options described earlier in this chapter, and command-specific options which are described below.

Two command-specific options determine the subset of the information displayed. They can be used singly, or in combination, to make the subset more specific.

Descriptions of the options follow.

Option	*Description*
node names | **PDN names**	Allows you to specify a list of *nodenames* or public data network PDN *names*. Only links that connect to the listed nodes and networks are displayed. Wildcarding can be used. The default is to display all PRIMENET nodes and subnetworks that are directly connected; nodes that are accessible over a PDN or by route-through are not directly connected, and do not constitute PRIMENET links. For further information about route-through, consult the *Operator's Guide to Prime Networks.*
-LINK link devices	Allows you to specify a list of *link devices*. Information is displayed only for links supported by the listed devices. Wildcarding can be used. There are three types of device: SYNCn PNC00 LHCn where *n* is the device number. The default is *all* link devices. For further information on PRIMENET links refer to the *Overview of Prime Networks*, and to the *System Administrator's Guide, Vol. II, Communication Lines and Controllers.* **Notes** SYNC and PNC are logical devices. Physical device names such as MDLC, HSSMLC, and ICS2 are not permitted. A system can only connect to one Prime ring network, and can therefore have only one PNC. PNC00 is the only permitted PNC device name.

▶ LIST_PRIMENET_NODES [options]

The LIST_PRIMENET_NODES command displays all PRIMENET-configured remote nodes, the paths to those nodes, and the permitted access to those paths; several paths can exist to the same node. Possible access modes to a path are *remote login* and *RFA (Remote File Access)*

The command options include both the general SIM options described earlier in this chapter, and command-specific options which are described below.

Seven command-specific options determine the subset of the information displayed. They can be used singly, or in combination, to make the subset more specific.

Descriptions of the options follow.

Option	*Description*
nodenames	Allows you to specify a list of remote *nodenames*. Only information for the listed nodes is displayed. Wildcarding can be used. The default is *all* PRIMENET-configured remote nodes.
-LINK link devices	Allows you to specify a list of *link devices*. Only paths that are routed on the listed link devices are displayed. Wildcarding can be used. There are three types of device: SYNCn PNC00 LHCn where *n* is the device number. The default is *all* link devices. For further information on links, refer to the *Overview of Prime Networks*, and the *System Administrator's Guide, Vol. II, Communication Lines and Controllers.* **Notes** SYNC, PNC, and LHC are logical devices. Physical device names such as MDLC, HSSMLC, and ICS2 are not permitted. A system can only connect to one Prime ring network, so that PNC00 is the only permitted PNC device.
-ADDRESS X25 addresses	Allows you to select nodes by their *X25 addresses*. For information about X25 addresses, consult the *Programmer's Guide to Prime Networks*. Wildcarding can be used.
-GATEWAY nodenames	Allows you to select nodes linked through particular GATEWAY (route-through) nodes. For further information about route-through, consult the *Operator's Guide to Prime Networks*. Wildcarding can be used.
-ACCESS access type	Allows you to specify the *access type*. Access types are *remote login* *RFA (Remote File Access)* The quotation marks are part of the syntax and must be supplied.
{**-VALIDATION** | **-VLD**}	Allows you to select nodes that require user validation from your node.

{**-NO_VALIDATION** | **-NVLD**}	Allows you to display nodes that do not require user validation from your node.

▶ LIST_PRIMENET_PORTS [options]

The LIST_PRIMENET_PORTS command displays a system's **port assignments**. Processes must assign ports in order to receive incoming PRIMENET calls.

You can obtain the following information about specific port assignments using the LIST_PRIMENET_PORTS command:

- Assign count
- Process number
- Process type
- User name

Notes

Where ports are not specifically assigned by number, LIST_PRIMENET_PORTS displays the user data (UDATA) information associated with the port, in hexadecimal. For more details about user data, see the *PRIMENET Guide*.

Slave processes that are not yet assigned appear as *not logged in*. When these slave processes are being used by remote users, they appear under the remote user name. Unassigned slave processes never appear as logged in.

The command options include both the general SIM options described earlier in this chapter, and command-specific options which are described below.

Two command-specific options determine the subset of the information displayed. They can be used singly, or in combination, to make the subset more specific.

Descriptions of the options follow.

Option	*Description*
port numbers	Allows you to specify a list of *port numbers*, as decimal integers. Ranges of port numbers can be specified. The command accepts integers in the range 0–32767. For port numbers on your system, refer to the *Overview of Prime Networks*, or consult your System Administrator. The default is *all* port numbers.
-USER | **names** | **numbers** |	Allows you to specify a list of user *names* or *numbers*. Only ports that are assigned to the users specified in the list are displayed. Wildcarding can be used on user names, and ranges of user numbers can be specified. The default is *all* users.

▶ LIST_PROCESS [options]

The LIST_PROCESS command displays current user processes on the system, including user numbers, names, types, and project IDs. Using the command-specific options, you can display the environment of specific processes in detail, including: attach points, abbreviation file, active COMI and COMO files, connect, CPU and I/O times and limits, users' ACL groups, and all active remote identities.

You can obtain other information about a process' environment by using other commands in the SIM set:

Information Needed	*SIM Command*
Asynchronous line status	LIST_ASYNC
List of assigned devices	LIST_ASSIGNED_DEVICES
Port Assignments	LIST_PRIMENET_PORTS
Semaphore values	LIST_SEMAPHORES
Identity of open file units	LIST_UNITS
List of active virtual circuits	LIST_VCS
Current memory usage	LIST_MEMORY

The command options include both the general SIM options described earlier in this chapter, and command-specific options which are described below.

Four command-specific options determine the subset of the information displayed. They can be used singly, or in combination, to make the subset more specific. Descriptions of the options follow.

Option	*Description*
|usernames| |usernumbers|	Allows you to specify a list of *usernames* or *usernumbers*. Only user processes specified in this list are displayed. Wildcarding can be used on user names, and ranges of user numbers can be specified. The default is to display *all* user processes.
{-PROJECT -PROJ} project groups	Allows you to specify a list of *project groups*. Only user processes that are logged in under one of these project identities are displayed. Wildcarding can be used. The default is *all* project identities.
-TYPE process types	Allows you to specify a list of *process types*. Only users who constitute one of these types are displayed.

Valid types are
terminal
remote
slave
server
batch
child
phantom

The default is to display all *user* process types.

{-DETAIL / -DET}

Allows you to specify whether detailed information must be returned for each user ID displayed.

The default is to display brief information only, namely
user number
user name
user type
user's project ID.

▶ **LIST_SEMAPHORES [options]**

The LIST_SEMAPHORES command displays the values of all semaphores in use on the system. The effect of the command is similar to that invoked by the command STAT SEMAPHORES; for further details, see the *PRIMOS Commands Reference Guide.*

For detailed information on semaphores and how they work, see the *Subroutines Reference Guide.*

Semaphore Security

Access to semaphores can be controlled by setting ACLs on files in the NUMSEM* directory. Semaphore security is activated by issuing the NUMSEMACL -ON command.

If semaphore security is active on the system, users can only display those semaphores to which they have access.

Note

If semaphore security is used, user DSMASR (the DSM application server) must also be given the appropriate access in the NUMSEM* directory, so that DSM can retrieve and display semaphore data.

For details of how to use semaphore security, see the *System Administrator's Guide, Vol. III, System Access and Security.*

The command options include both the general SIM options described earlier in this chapter, and command-specific options which are described below.

Four command-specific options determine the subset of the information displayed. They can be used singly, or in combination, to make the subset more specific.

Descriptions of the options follow.

Option	*Description*
semaphore numbers	Allows you to specify a list of *semaphore numbers*. The command accepts integers in the range -32 through 32767. Ranges of numbers can also be specified. Numbers 1 through 64 are user-assigned semaphores. Negative semaphores are assigned to the system and are only displayed by invoking the command at the supervisor terminal, or through RESUS. **Note** To quote a negative number in a range specification, enclose the entire range in single quote marks. For example: *'-32:5'* For semaphore numbers on your system, see the *Subroutines Reference Guide*, or consult your System Administrator. The default is to display *all* semaphores.
-USER { **names** | **numbers** }	Allows you to specify a list of user *names* or *numbers*. Wildcarding can be used on user names, and ranges of user numbers can be specified.
-TYPE { **NAMED** | **NUMBERED** }	Allows you to specify that only NAMED or NUMBERED semaphores are to be displayed. The default is to display both named and numbered semaphores.
{ **-DETAIL** | **-DET** }	Displays detailed information about semaphores. The default is to display brief information about all semaphores, including type, value, and number of users.

▶ LIST_SYNC [options]

The LIST_SYNC command displays configuration and controller data for all enabled synchronous lines.

The command does not return the current status of the line. This information is controlled by the individual software subsystems that control the line. Subsystems typically configured on synchronous lines are PRIMENET, RJE, and DPTX.

For a detailed explanation of synchronous lines, refer to the section on SYNC directives in the *System Administrator's Guide, Vol. II, Communication Lines and Controllers*, and the section on synchronous controllers in the *Subroutines Reference Guide*.

The command options include both the general SIM options described earlier in this chapter, and one command-specific option which is described below.

The command-specific option allows you to select a subset of the information for display. A description of the option follows.

Option	*Description*
line numbers	Allows you to list the lines by their logical numbers, and displays the configuration of those lines only. Specify *line numbers* as *octal* integers. Ranges of line numbers can also be specified. The command accepts integers in the range 0 through 77777. For synchronous line numbers on your system, consult your System Administrator.

▶ LIST_UNITS [options]

LIST_UNITS displays open file units. It can be used in three ways:

- To display the open file units for any system user
- To display the ID of all users with either a particular file open, or any file open in a particular directory
- To display the current attach points of all users on the system

The command options include both the general SIM options described earlier in this chapter, and command-specific options which are described below.

Four command-specific options determine the subset of the information displayed. They can be used singly, or in combination, to make the subset more specific.

Descriptions of the options follow.

Option	*Description*
usernames **usernumbers**	Allows you to specify a list of *usernames* and *usernumbers*. Only units open for users specified in this list are displayed. Wildcarding can be used on user names, and ranges of user numbers can be specified. The default is *all* users.

-PATHNAME pathname [{**-WALK_FROM** | **-WLKFM**} [level]] [{**-WALK_TO** | **-WLKTO**} [level]]

Allows you to display open file units and user attach points under a specified pathname. *pathname* can be a pathname that includes the disk partition, a pathname beginning with the name of a top-level directory, or a pathname relative to your current attach point. Wildcarding can be used on all elements of the pathname, including the disk partition.

If you specify a relative pathname or a pathname that includes a top-level directory, only the local node's disk table is searched. If you specify the disk partition, the entire pathname is passed to the target node, where it is interpreted according to that node's disk table. Therefore, to list open file units on a remote node, you should specify the disk name, or use wildcarding on the disk partition.

Wildcarding on the disk partition can be used to list file units on several nodes at once.

To walk a directory, use the -WALK_FROM and -WALK_TO options. Specify *level* as a decimal integer. Defaults are -WALK_FROM *2* and -WALK_TO *bottom-of-tree.*

-FILETYPE filetype

Allows you to select a file type.

File types are:

SAM
DAM
CAM
SAMSEG
DAMSEG
ACAT
UFD

{**-DETAIL** | **-DET**}

Displays detailed information on users' open file units. The default is to display a count of open units, and users' attach points.

▶ **LIST_VCS [options]**

The LIST_VCS command displays the state of virtual circuits. Used without any options, it displays all active virtual circuits on the system.

The command options include both the general SIM options described earlier in this chapter, and command-specific options which are described below.

Six command-specific options determine the subset of the information displayed. They can be used singly, or in combination, to make the subset more specific. Descriptions of the options follow.

Option	*Description*
VC ID numbers	Allows you to specify a list of virtual circuit ID numbers. Specify *VC ID numbers* as decimal integers. The command accepts integers in the range 1–32767. For VC ID numbers on your system, consult your System Administrator. The default is to display *all* active virtual circuits.
-USER {**names** | **numbers**}	Allows you to specify a list of user *names* or *numbers*. Wildcarding can be used on user names, and ranges of user numbers can be specified. The default is to display *all* system users.
-NODE nodenames	Allows you to specify a list of the *nodenames* of remote nodes to which the system is connected through virtual circuits. Only virtual circuits that connect to one of the listed nodes are displayed. Wildcarding can be used. **Note** Do not confuse this option with the general SIM option -ON node, which allows you to invoke the command on a remote node. The default is to display *all* nodes.
-LINK link devices	Allows you to specify a list of *link devices*. Only virtual circuits supported on the listed devices are displayed. Wildcarding can be used. There are three types of device: SYNCn PNC00 LHCn where *n* is the device number. The default is *all* link devices. **Notes** SYNC and PNC are logical devices. Physical device names such as MDLC, HSSMLC, and ICS2 are not permitted. A system can only connect to one Prime ring network, so that PNC00 is the only permitted PNC device.

-PORT port numbers

Allows you to specify a list of *port numbers*, as decimal integers.

The command accepts integers in the range 0 through 32767. For port numbers on your system, consult your System Administrator.

The default is to display VCs on *all* ports.

{**-DETAIL** / **-DET**}

Displays detailed information about VCs. The default is to display a summary of each VC's activity.

8

REMOTE SYSTEM USER (RESUS)

Introduction

This chapter describes the Remote System User facility (RESUS). The chapter begins with an overview of RESUS and describes the RESUS environment. The next section explains how access to RESUS is controlled, and outlines its implications for system security. The main part of the chapter is a detailed description of the RESUS command and its options. The chapter concludes with an example RESUS session.

Overview of RESUS

The Remote System User facility (RESUS) allows you to control machines from any point on the network. It gives you remote access to system and operator commands on any machine, under the security umbrella of DSM access control. Through RESUS, systems administrators and operators can add disks, shut down devices and share segments, and do other similar tasks, from any terminal on any node in the configuration group. You can use RESUS to issue control commands on a remote machine, or to control the local machine from a convenient local terminal.

RESUS gives operations staff working flexibility, by allowing day-to-day operations on a network of machines to be coordinated from any site, and from any terminal on that site.

The RESUS Environment

RESUS gives you access to the same command privileges at your terminal that you would have at the supervisor terminal. Your terminal is assigned to the User-1 process and replaces the User-1 functions of the supervisor terminal. In effect your terminal becomes the *logical* supervisor terminal, while the real or *physical* supervisor terminal merely echoes what you type, and the system's responses. A consequence of this is that at any one time only **one** user on a node can use RESUS.

To the RESUS user, an active RESUS session looks like a privileged NETLINK call; one in which it is possible to control a local or remote machine from a normal user terminal.

RESUS does not give remote access to control panel (CP) mode on the console, which remains under local control through the standard ESCAPE-ESCAPE sequence. During a RESUS session, the commands you type at the terminal, and the system's responses are echoed at the machine's supervisor terminal and at your terminal. This gives you a record of the RESUS session from which it is possible to reconstruct the complete context of a session if there is an unexpected failure such as loss of the terminal line.

Notes

RESUS can only operate at the speed of the supervisor terminal on the system. If your supervisor terminal is a slow device such as a teletype, display at the terminal will be correspondingly slow. To lessen the problem, you can increase the User-1 buffer size using the CAB command (see *System Administrator's Guide Vol. II, Communication Lines and Controllers*).

Take care with products that employ specific terminal characteristics. RESUS sessions are echoed at the supervisor terminal, and products such as EMACS may lock the keyboard.

System Security and Access Control

RESUS does not compromise system security in any way. Before any machine can be controlled through RESUS, it must first be enabled locally on the machine, at the supervisor terminal. Primary security is therefore provided by the physical security of the machine room, just as with standard arrangements. Only by breaking the security arrangements at your installation can users enable RESUS without permission.

Systems Administrators therefore have two choices; to allow or disallow access to RESUS facilities on their machines, by enabling or disabling RESUS locally. Keeping RESUS disabled locks out all RESUS users, both local and remote, and ensures that the machine can be controlled only from the local supervisor terminal.

A second level of security is provided by DSM security. User access to RESUS, as with all DSM facilities, is controlled throughout the network by the DSM security mechanism. Even when RESUS is enabled at a node, the only users who can use RESUS are those who have been given correct DSM access by the administrator. Specifically, only users that have been granted access to the function RESUS linked to the target node can control that node through RESUS.

A separate function, RESUS_STATUS, allows less trusted users to determine the RESUS enable/disable status of local and remote machines.

For further details of DSM security and how to use and set up user access definitions, see Chapter 2, Administration and Security, and Chapter 4, Configuring DSM.

Note

Once you have established a RESUS session to a node, full User-1 privileges, including commands such as SHUTDN, are available to the local or remote user. Choose carefully who you allow to use the RESUS command.

The RESUS Command and its Options

RESUS generates unsolicited messages when it is started, stopped, enabled, and disabled on a system. You can log these messages in a file, or display them at a terminal, by defining an appropriate UMH selection.

▶ RESUS subcommand

The RESUS command gives you access to the supervisor terminal on any machine on your network, from any terminal.

Descriptions of the subcommands follow.

Subcommand	*Description*
-ENABLE	The -ENABLE option enables RESUS at a node. Once RESUS is enabled at the supervisor terminal, any authorized local or remote user can gain control of the machine. -ENABLE is restricted to the real supervisor terminal. It allows operators to exercise local master control over the availability of RESUS on the local system. Once RESUS is enabled, users can only control the machines from a local or remote terminal, except where the console can be used as a normal terminal through MODE USER. The console subsequently ignores all input except the commands RESUS -DISABLE and RESUS -DISABLE -FORCE. The system and error prompts change to *nodename*.RESUS_OK>* *nodename*.RESUS_ER>*
-DISABLE	Disables RESUS facilities at a node. It is valid only at the supervisor terminal. Disabling RESUS at a node has no effect on the ability of users on that node to gain control of other nodes where RESUS is enabled. -DISABLE is restricted to the real supervisor terminal. It allows operators to exercise local master control over the availability of RESUS at each node.

-DISABLE is not honored if another RESUS user is already in control of the node. In these circumstances, you must use -DISABLE -FORCE to disable RESUS and reestablish local control.

-DISABLE -FORCE

Forcibly disables RESUS at a node, even if another user is already in control of the machine through RESUS. The user is ejected, and normal supervisor terminal activity is reestablished.

RESUS -DISABLE -FORCE bypasses normal operating system routines, and reestablishes local control of a machine independently of PRIMOS.

-DISABLE -FORCE is valid only when RESUS is enabled and is only honored at the real supervisor terminal.

Notes

When you force disable RESUS, the User-1 process remains in the most recently entered subsystem. To return the supervisor terminal to monitor level, simply quit the subsystem in the normal way. To identify the subsystem, refer to the supervisor terminal record.

There may be a short delay between typing the RESUS -DISABLE -FORCE command at the supervisor terminal, and its execution. The RESUS command allows type-ahead.

-START [-ON node]

Connects you to the supervisor terminal on the specified *node*. If you do not specify a node name, the local node is assumed. RESUS must be enabled on that node.

-START is not available at the supervisor terminal, or at a terminal where RESUS is already in use.

You cannot control more than one machine at a time through RESUS, and only one user can be in control of a machine at any time.

For an example of how to establish a RESUS session, with examples of the messages displayed, see the end of this chapter.

-STOP

Terminates the RESUS session and returns you to PRIMOS at the node where you are logged in. When the disconnection is complete, you receive a sign-off message at your terminal, and the machine is then available to other RESUS users. For an example of the messages displayed when a session terminates, see the example at the end of this chapter.

-STATUS [**-ON** {**node** / **nodegroup**}] — Allows you to determine the enable/disable status or current users of RESUS on a *node* or *nodegroup*. If you do not specify a node or node group, the local node is assumed.

The display is a simple table that gives you the enable/disable status of RESUS on the relevant nodes, along with current users, if any. Where the requested information cannot be retrieved, an explanatory message is displayed. For an example of the display, see the example at the end of this chapter.

{**-HELP** / **-H**} [{**-NO_WAIT** / **-NW**}] — Explains how to use the command. This option cancels any other options on the command line. If you specify -NO_WAIT, the display is not paginated at your terminal. The same information is available through the PRIMOS HELP subsystem.

-USAGE — Gives you the command syntax in brief. This option cancels all others on the command line.

Using RESUS in MODE USER

On 2250, 2350, 2450, 2550, 9650, 9750, 9950 and 9955 machines, you can deassign the supervisor terminal to work as a normal terminal, by issuing the command MODE USER from CP mode. You can use RESUS from the supervisor terminal on these machines, with the following restrictions.

If you use RESUS from USER mode, first issue the CP command SYSOUT IGNORE to disable output to the physical supervisor terminal. If you do not issue SYSOUT IGNORE, output is directed to the User-1 display buffer and characters may be lost. Remember that SYSOUT IGNORE forces the supervisor terminal to ignore display output, so there is no record of your dialog.

Do not use the CP command SYSOUT INTRLF, or screen output is hopelessly jumbled.

Precautions On Some PRIMOS Commands and Prime Products

RESUS is a special environment. It is a privileged machine control facility that operates through the networking software, and you should exercise caution when you use the following commands in a RESUS session.

Command	*Restriction*
STOP_DSM/LOGOUT	Do not issue the STOP_DSM command, or logout the DSM server, while you are using RESUS. The operation of RESUS itself depends on DSM running on the system.
NETLINK	If you invoke NETLINK from RESUS, the dialog is switched to the supervisor terminal buffer, and is not displayed at your terminal. To recover from this, disable RESUS at the supervisor terminal, and quit the NETLINK session from there.

Command	*Restriction*
EMACS	Take care with terminal-specific subsystems such as EMACS, that are specific for terminal type. The session is echoed at the supervisor terminal, and may lock the supervisor terminal keyboard.
TERM	Remote system users, like local system users, are free to customize their operating environment with the PRIMOS command TERM. Such changes remain in force on the supervisor terminal when the node returns to local control. Because others will use the supervisor terminal after you, it is good practice not to alter its environment in any way, either when you operate the machine from the supervisor terminal, or from a terminal through RESUS.
AMLC	When you use RESUS to control the local machine from a local terminal, it is possible to deassign the line to the terminal. You can regain control only by disabling RESUS at the supervisor terminal, and reconfiguring the line.
STOP_NET	Do not issue the STOP_NET command on a remote machine, from a RESUS session. It eliminates the communication link that RESUS is using, and aborts the session.
ICE	The ICE command reinitializes your command environment to the original login state. In the process, it can reset terminal prompts to the PRIMOS defaults. If you use ICE in a RESUS session, the special RESUS prompts may be lost for the remainder of the session, and are only restored when RESUS is next enabled.
USRASR	Do not issue the USRASR command from RESUS. It hangs the supervisor terminal and requires special procedures to recover normal operation.
MIRROR_ON/MIRROR_OFF	Do not use the MIRROR_ON and MIRROR_OFF commands from RESUS. They demand input from the supervisor terminal, and the RESUS session becomes suspended. To restore normal operation, disable RESUS at the supervisor terminal. Control is returned to the supervisor terminal, from where you can continue your dialogue with the MIRROR command if you wish.

For further details of these commands, see the *PRIMOS Commands Reference Guide* and the *Operator's Guide To System Commands.*

An Example RESUS Session

At the user's terminal:

```
OK, RESUS -START
[RESUS Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]
RESUS Connecting to : SYS1
Error: RESUS start request rejected
       RESUS is not enabled  (RESUS)
ER! RESUS -STOP
[RESUS Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]
Error: RESUS is not in use by this terminal (RESUS)

ER! RESUS -USAGE
[RESUS Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]

Usage:  RESUS -STATUS  [ -ON <node group>]
              -START   [ -ON <node name>]
              -STOP
              -ENABLE
              -DISABLE [ -FORCE]
              -Help
              -USAGE
OK, RESUS -STATUS
[RESUS Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]

                          RESUS STATUS REPORT

Source node:  SYS1

Invoked at:   10 Jun 90 16:54:12 Friday

 Target node                    Status
      SYS1 | RESUS is currently disabled
OK, RESUS -ENABLE
[RESUS Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]
Error: Enable option only available from physical system console (RESUS)

OK, RESUS -START
[RESUS Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]
RESUS Connecting to : SYS1

*** DSMASR (user 115 on SYS1) at 16:55
10 Jun 90 : RESUS currently in use by SYSOPR (User 34 on node SYS1)
SYS1.RESUS_OK> ADDISK COMND2 -ON SYS2
SYS1.RESUS_OK> RESUS -STATUS
[RESUS Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]

                              RESUS STATUS REPORT

Source node:  SYS1

Invoked at:   10 Jun 90 16:56:40 Friday

  Target node                                Status
      SYS1 | RESUS  in use by SYSOPR, user 34 on node SYS1
SYS1.RESUS_OK> RESUS -START
[RESUS Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]
Error: Start option not available to system console user (RESUS)
SYS1.RESUS_ER> RESUS -STOP
RESUS Session terminated
OK,
```

At the supervisor terminal:

```
OK, RESUS -ENABLE
[RESUS Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]
RESUS Enabled on SYS1
OK,
*** DSMASR (user 115 on SYS1) at 16:55
10 Jun 90 : RESUS currently in use by SYSOPR (User 34 on node SYS1)
SYS1.RESUS_OK> ADDISK COMND2 -ON SYS2

SYS1.RESUS_OK> RESUS -STATUS
[RESUS Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]

                              RESUS STATUS REPORT

Source node:  SYS1

Invoked at:   10 Jun 90 16:56:40 Friday

 Target node                    Status
      SYS1  | RESUS  in use by SYSOPR, user 34 on node SYS1

SYS1.RESUS_OK> RESUS -START
[RESUS Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]
Error: Start option not available to system console user (RESUS)

SYS1.RESUS_ER> RESUS -STOP
[RESUS Rev. 23.0 Copyright (c) 1990, Prime Computer, Inc.]
10 Jun 90 16:58:52 Friday: RESUS facilities no longer in use
OK,
```

APPENDICES

A

DSM CONFIGURATION FILES

This appendix contains listings of

- The empty configuration file, DSM* > CONFIG_FILES > DSM_EMPTY.CONFIG
- The default configuration file, DSM* > CONFIG_FILES > DSM_DEFAULT.CONFIG
- The configuration file generated in the example configuration (see Chapter 4).

The Empty Configuration File

```
Configuration       : DSM_EMPTY.CONFIG
Revision number     : 1
Last updated        : 89/02/02 18:16:22
Updated by user     : SYSTEM
Updated on node     : PRIME
DSM revision number : 1
Comment             : EMPTY CONFIG FILE

Nodes in the configuration group are:
   LOCAL$

DSM function names are:
   ADMIN_SNAD$, ADMIN_X400$, CHANGE_ASYNC_BUFFER$, CONFIG_THRESHOLD$,
   CONFIG_UM, CONTROL_DRM$, CONTROL_PA$, CONTROL_SRM$, DASHBOARD$,
   DASHBOARD_UM$, DISTRIBUTE_DSM, LIST_ASSIGNED_DEVICES, LIST_ASYNC,
   LIST_ASYNC_BUFFER$, LIST_COMM_CONTROLLERS, LIST_CONFIG, LIST_DISKS,
   LIST_LAN_NODES, LIST_MEMORY, LIST_PRIMENET_LINKS, LIST_PRIMENET_NODES,
   LIST_PRIMENET_PORTS, LIST_PROCESS, LIST_SEMAPHORES, LIST_SYNC, LIST_UNITS,
   LIST_VCS, PRIVATE_LOGGER, PROGRAMMED_ACTION$, RESUS, RESUS_STATUS,
   SCREEN_HANDLER, STATUS_DSM, SYSTEM_LOGGER

Function group .ANY_FUNCTION$ contains:
   Any valid function name.

Node group .ANY_NODE$ contains:
   Any valid node name.
Node group .ALIEN_NODES$ is empty.
Node group .GROUP$ contains:
   LOCAL$

User access definition ALIEN$ is:
   User/ACL group .ANY_USER$ from location(s):
     .ALIEN_NODES$
   Function/function group: STATUS_DSM is allowed on node/node groups:
     .GROUP$

Product Register details.

There are no registered products.
```

The Default Configuration File

```
Configuration       : DSM_DEFAULT.CONFIG
Revision number     : 1
Last updated        : 89/02/02 10:21:03
Updated by user     : SYSTEM
Updated on node     : PRIME
DSM revision number : 1
Comment             : DEFAULT CONFIG FILE

Nodes in the configuration group are:
   LOCAL$

DSM function names are:
   ADMIN_SNAD$, ADMIN_X400$, CHANGE_ASYNC_BUFFER$, CONFIG_THRESHOLD$,
   CONFIG_UM, CONTROL_DRM$, CONTROL_PA$, CONTROL_SRM$, DASHBOARD$,
   DASHBOARD_UM$, DISTRIBUTE_DSM, LIST_ASSIGNED_DEVICES, LIST_ASYNC,
   LIST_ASYNC_BUFFER$, LIST_COMM_CONTROLLERS, LIST_CONFIG, LIST_DISKS,
   LIST_LAN_NODES, LIST_MEMORY, LIST_PRIMENET_LINKS, LIST_PRIMENET_NODES,
   LIST_PRIMENET_PORTS, LIST_PROCESS, LIST_SEMAPHORES, LIST_SYNC, LIST_UNITS,
   LIST_VCS, PRIVATE_LOGGER, PROGRAMMED_ACTION$, RESUS, RESUS_STATUS,
   SCREEN_HANDLER, STATUS_DSM, SYSTEM_LOGGER

Function group .ANY_FUNCTION$ contains:
   Any valid function name.
Function group .RESUS$ contains:
   RESUS, RESUS_STATUS
Function group .SIM$ contains:
   LIST_ASSIGNED_DEVICES, LIST_ASYNC, LIST_COMM_CONTROLLERS, LIST_CONFIG,
   LIST_DISKS, LIST_LAN_NODES, LIST_MEMORY, LIST_PRIMENET_LINKS,
   LIST_PRIMENET_NODES, LIST_PRIMENET_PORTS, LIST_PROCESS, LIST_SEMAPHORES,
   LIST_SYNC, LIST_UNITS, LIST_VCS, PRIVATE_LOGGER

Node group .ANY_NODE$ contains:
   Any valid node name.
Node group .ALIEN_NODES$ is empty.
Node group .GROUP$ contains:
   LOCAL$

User access definition ALIEN$ is:
   User/ACL group .ANY_USER$ from location(s):
     .ALIEN_NODES$
   Function/function group: STATUS_DSM is allowed on node/node groups:
     .GROUP$
User access definition DSM_ADMINISTRATOR$ is:
   User/ACL group .SYSTEM_ADMINISTRATOR$ from location(s):
     .ANY_NODE$
   Function/function group: .ANY_FUNCTION$ is allowed on node/node groups:
     .ANY_NODE$
User access definition DSM_OPERATOR$ is:
   User/ACL group SYSTEM from location(s):
     LOCAL$
   Function/function group: .RESUS$ is allowed on node/node groups:
     .ANY_NODE$
   Function/function group: .SIM$ is allowed on node/node groups:
     .ANY_NODE$

Product Register details.

There are no registered products.
```

An Example Configuration

```
Configuration       : CONFIG.1
Revision number     : 1
Last updated        : 89/11/01 14:06:51
Updated by user     : ARKWRIGHT
Updated on node     : SYSA
DSM revision number : 1
Comment             : SYS RING CONFIG_FILE

Nodes in the configuration group are:
                SYSA, SYSB, SYSC

DSM function names are:
   ADMIN_SNAD$, ADMIN_X400$, CHANGE_ASYNC_BUFFER$, CONFIG_THRESHOLD$,
   CONFIG_UM, CONTROL_DRM$, CONTROL_PA$, CONTROL_SRM$, DASHBOARD$,
   DASHBOARD_UM$, DISTRIBUTE_DSM, LIST_ASSIGNED_DEVICES, LIST_ASYNC,
   LIST_ASYNC_BUFFER$, LIST_COMM_CONTROLLERS, LIST_CONFIG, LIST_DISKS,
   LIST_LAN_NODES, LIST_MEMORY, LIST_PRIMENET_LINKS, LIST_PRIMENET_NODES,
   LIST_PRIMENET_PORTS, LIST_PROCESS, LIST_SEMAPHORES, LIST_SYNC, LIST_UNITS,
   LIST_VCS, PRIVATE_LOGGER, PROGRAMMED_ACTION$, RESUS, RESUS_STATUS,
   SCREEN_HANDLER, STATUS_DSM, SYSTEM_LOGGER

Function group .ANY_FUNCTION$ contains:
   Any valid function name.
Function group .NETWORK_STATUS contains:
   LIST_COMM_CONTROLLERS, LIST_LAN_NODES, LIST_PRIMENET_LINKS,
   LIST_PRIMENET_NODES, LIST_PRIMENET_PORTS, LIST_VCS
Function group .RESUS$ contains:
   RESUS, RESUS_STATUS
Function group .SIM$ contains:
   LIST_ASSIGNED_DEVICES, LIST_ASYNC, LIST_COMM_CONTROLLERS, LIST_CONFIG,
   LIST_DISKS, LIST_LAN_NODES, LIST_MEMORY, LIST_PRIMENET_LINKS,
   LIST_PRIMENET_NODES, LIST_PRIMENET_PORTS, LIST_PROCESS, LIST_SEMAPHORES,
   LIST_SYNC, LIST_UNITS, LIST_VCS, PRIVATE_LOGGER

Node group .ANY_NODE$ contains:
   Any valid node name.
Node group .ALIEN_NODES$ is empty.
Node group .GROUP$ contains:
   SYSA, SYSB, SYSC
Node group .PSDN_LINK contains:
   SYSA

User access definition ALIEN$ is:
   User/ACL group .ANY_USER$ from location(s):
     .ALIEN_NODES$
   Function/function group: STATUS_DSM is allowed on node/node groups:
     .GROUP$
User access definition DSM_ADMINISTRATOR$ is:
   User/ACL group ARKWRIGHT from location(s):
     .GROUP$
   Function/function group: .ANY_FUNCTION$ is allowed on node/node groups:
     .ANY_NODE$

User access definition DSM_OPERATOR$ is:
   User/ACL group .SYSTEM from location(s):
     .GROUP$
   Function/function group: .RESUS$ is allowed on node/node groups:
     .ANY_NODE$
   Function/function group: .SIM$ is allowed on node/node groups:
```

```
     .ANY_NODE$
User access definition PSDN_PROJECT is:
   User/ACL group AHACKER from location(s):
     SYSB
   Function/function group: .NETWORK_STATUS is allowed on node/node groups:
     .PSDN_LINK

Product Register details.

Registered products are:
                 LOGIN_MANAGER, MAIL
```

B

DSM PRODUCT NAMES

This appendix lists the Prime product names that are registered with DSM as senders of unsolicited messages. They can be used as

- Product names that you use when you define UMH selections
- Arguments to the DISPLAY_LOG -PRODUCT option

You can generate an up-to-date list of all DSM products on your system by issuing the CONFIG_UM command and entering HELP or H at the prompt `Prime product:`. See Chapter 5 for further details.

Product Name	*Description*
ADMIN_LOG	The ADMIN_LOG command. A message is generated when there is a software failure.
ASYNC	Messages from the CAB and LAB commands. For details see the *System Administrator's Guide Vol. II, Communication Lines and Controllers.*
BATCH	Users can generate threshold UMs for various Batch resources via the Distributed Resource Monitor (DRM) product.
CONFIG_DSM	The CONFIG_DSM command. A message is generated when there is a software failure.
CONFIG_UM	The CONFIG_UM command. A message is generated when there is a software failure.
CONTROLLER_DLL	LAN300 downline load with the COMM_CONTROLLER command. For more information refer to the *NTS User's Guide.*
CONTROLLER_ULD	LAN300 upline dump with the COMM_CONTROLLER command. For more information refer to the *NTS User's Guide.*
DASHBOARD	This is part of Prime's Distributed Resource Monitor (DRM) product, and does not generate UMs.

DISPLAY_LOG	The DISPLAY_LOG command. A message is generated when there is a software failure.
DISTRIBUTE_DSM	The DSM configuration distribution service. A message is generated each time the restart configuration file is updated on a node.
DRM	This is the product name for the Distributed Resource Monitor product; it does not generate UMs.
DSM	The DSM server. Messages are generated when DSM starts and when a configuration mismatch is detected between nodes.
FTS	Users can generate threshold UMs for various FTS resources via the Distributed Resource Monitor (DRM) product.
ICS	ICS controllers. For more information refer to the *ICS User's Guide.*
LOG_COLD	PRIMOS cold-start message. DSM message ID: SYSTEM_COLD.
LOG_DISK	PRIMOS disk error messages. DSM Message ID: SYSTEM_DISKER.
LOG_MISC	Miscellaneous PRIMOS messages. DSM message ID: SYSTEM_ERRCHK SYSTEM_PACL SYSTEM_OVERFL SYSTEM_SHUTDN SYSTEM_DSKNAM SYSTEM_FORCDN
LOG_OVFL	PRIMOS log buffer overflow messages. DSM message ID: SYSTEM_OVERFL.
LOG_SEG4	PRIMOS machine check, warm start and sensor messages. DSM message ID: SYSTEM_CHECK1 SYSTEM_CHECK2 POWERF SYSTEM_SENSOR SYSTEM_ECCULO.
LOG_TAPE	PRIMOS tape controller errors.

LOG_UNKN

Other PRIMOS messages.
DSM message ID: SYSTEM_SETIME
SYSTEM_QUIET
REMARK
SYSTEM_TYPE10
SYSTEM_TYPE11
SYSTEM_TYPE12
SYSTEM_TYPE13
SYSTEM_TYPE14
SYSTEM_TYPE15.

LOGGER

The DSM logging service. Messages are generated when log files become full or exceed a record limit.

LTP

Light Transfer Protocol, which runs on the FDDI lan.

NAME_SERVER

The Name Server provides the ability to have a collection of machines share a common file system namespace. This is accomplished by having the Name Server replicate the Primos root-directory. Messages generated from the Name Server will be related to either problems achieving the replication, or general errors encountered by the Name Server.

NMSR

LAN300 network manager server. For more information see the *NTS User's Guide.*

NPX

NPX errors for all network media.

OSINM

Messages generated by MAP/TOP and FTAM products.

PRIMENET

All PRIMENET-related events. Users can also generate threshold UMs for various PRIMENET resources via the Distributed Resource Monitor (DRM) product. For more information see the *PRIMENET Planning and Configuration Guide.*

PRIMOS

Miscellaneous Primos messages. Users can also generate threshold UMs for various Primos resources via the Distributed Resource Monitor (DRM) product.

PROGRAMMED_ACTION

This is part of Prime's Distributed Resource Monitor (DRM) product, and does not generate UMs.

RESUS

The product RESUS. Messages are generated when resus is started, stopped, enabled or disabled. Users can also generate threshold UMs for various Resus resources via the Distributed Resource Monitor (DRM) product.

SCREEN_HANDLER

The DSM screen display function. A message is generated when there is a software failure.

SIM	All SIM commands. A message is generated when there is a software failure.
SNMP	Messages generated by the Simple Network Management Protocol product.
SPOOLER	The spooler subsystem. Messages are generated by the despooler software, mainly to signal PROP operations such as removing jobs from the queue. Other messages warn of impending subsystem failure. For further information see the *Operator's Guide to the Spooler Subsystem.*
START_DSM	The START_DSM command. A message is generated when there is a software failure.
STATUS_DSM	The STATUS_DSM command. A message is generated when there is a software failure.
STOP_DSM	The STOP_DSM command. A message is generated when there is a software failure.
SYSTEM_MANAGER	The DSM system manager that controls event logging.
TCP/IP	Prime's implementation of the Transport Control and Internet protocols, that support file transfer and remote login.
THRESHOLD_MONITOR	This is part of Prime's Distributed Resource Monitor (DRM) product, and generates an Unsolicited Message when a threshold triggers while it is being modified.
UMH	The Unsolicited Message Handler, part of the SYSTEM_MANAGER.

C

SENDING CUSTOMER UNSOLICITED MESSAGES

This appendix describes the subroutine that you use to send unsolicited messages from customer products registered with DSM.

Format of Call Statement

The call statement is shown below:

CALL DS$SEND_CUSTOMER_UM (text, severity, product_name, reserved, return_code)

The parameters in the call statement are described below.

Subroutine Parameters

Input Parameters

Parameter	*Description*
text	Contains the message text. You can use any alphanumeric character; the maximum number of characters is 1024.
severity	Specifies the severity level of the message. This must be one of the severities contained in the insert file SYSCOM>DS$SEVERITY_KEYS.INS.PL1. For further details, refer to the section, Severities, in Chapter 5.
product_name	Specifies the name of the customer product, that you use when you register the product using CONFIG_DSM. This is also the name that you use when you create UM selections using CONFIG_UM. If the product is registered, but no UM selections have been set up, all UM's are sent to the DSM default log.
reserved	This parameter is reserved for future use. You must set it to 0.

Output Parameters

Parameter	*Description*
return_code	This parameter contains the return status. The settings for the return status are given in the insert file SYSCOM>DS$ERROR_KEYS.INS.PL1, and are as follows:

DS$OK	Successful call.
DS$ER_UNKNOWN_CUST_PROD	The product specified is not registered with DSM as a customer product.
DS$ER_TEXT_TOO_LONG	Message text length exceeds 1024 characters.
DS$ER_BAD_TEXT_LENGTH	Message text length is less than 0 characters.
DS$ER_BAD_SEVERITY	The specified severity parameter specified is not valid.
DS$ER_DSM_UNAVAILABLE	DSM is not running on the local node.
DS$ER_INSUFFICIENT_RESOURCES	This situation may result from a lack of resources such as virtual circuits, memory, or ISC buffers, or else the queue to the DSM server may be full. You may need to restart DSM.
DS$ER_INTERNAL_ERROR	DSM has been unable to send the customer UM; the reason is unspecified.

Using the Subroutine

Ensure that only pertinent unsolicited messages are sent to DSM. A large number of messages may overload the system.

Choose the severity level carefully; fatal errors may go unnoticed if, for example, the severity level is set to INFORMATION, rather than FAILURE.

To load and link the application software containing the subroutine call(s), when running V-Mode or I-Mode programs, use the libraries DSMLIB.BIN and X409LIB.BIN within the ufd LIB. You cannot use the subroutine with R-Mode programs.

Example

Shown below is an example of a call to this subroutine. This example would typically be written as part of a user login program.

```
text= " user " || username || " logged in at " || date_time;

reserved =0;

call DS$SEND_CUSTOMER_UM(text,DS$INFORMATION,'LOGIN_MANAGER',reserved,return_code);

if return_code ^= DS$OK

then

    call ioa$("Unable to send UM %v%.",100,text);
```

D

GLOSSARY

.ALIEN_NODES$
A *nodegroup* that contains the list of nodes from outside the *configuration group* that have access to DSM commands within the group. Users on these nodes can invoke commands on nodes in the group if ALIEN$ allows them the correct access rights.

.ANY_FUNCTION$
Shorthand notation for all registered DSM *functions*. Cannot be changed, renamed or deleted.

.ANY_NODE$
Shorthand notation for any PRIMENET node name. Cannot be changed, renamed or deleted.

.ANY_USER$
Shorthand notation for any PRIMOS user name. Cannot be changed, renamed or deleted.

.GROUP$
A *nodegroup* that contains all nodes in the current configuration group. Cannot be renamed or deleted.

Access Control List (ACL)
A list of PRIMOS users and the file access rights granted to each. Independent of DSM access control.

ACL
See Access Control List.

Administrator
The administrator has responsibility for controlling DSM within a *configuration group*. The administrator defines all user access to DSM facilities and controls communication with other groups.

ALIEN$

The role assigned within a configuration group to users from other configuration groups. It is also the role assigned to a user in the same group where there is a configuration file mismatch.

AMLC

The PRIMOS command to configure asynchronous lines. Abbreviation of Asynchronous multiline Controller.

Application

A DSM application is any piece of software that uses DSM-supplied services to implement a networked systems management facility or service. Applications provide the user-visible functions of DSM and include RESUS, SIM, UMH, DSM security and the DSM logging service.

Application server

An application server (user DSMASR) is a PRIMOS process that runs DSM application code at a node on behalf of the user and provides secure interfacing with the DSM server (user DSMSR).

Configuration File

The configuration file is the file that defines the membership and security policy of a *configuration group*. Each node in a configuration group uses the same configuration file.

Configuration Group

A configuration group is a subset of nodes on the network that are run under the same set of administrative policies, through the medium of a replicated *configuration file.* Configuration groups are independent subsets of the network and cannot overlap.

Customer Product

A customer product is a user application that sends unsolicited messages by calling the subroutine DS$SEND_CUSTOMER_UM. Customer products are registered using CONFIG_DSM, and can be specified when you invoke the CONFIG_DSM and DISPLAY_LOG commands.

Destinations

Unsolicited messages can be directed to specific destinations using the CONFIG_UM command. Typically, destinations are either DSM logs or display devices.

Distributed System Management (DSM)

DSM comprises a group of distributed systems monitoring and management services known as *applications*, supported by essential services such as access validation and networked message interchange implemented by the DSM *kernel.*

DSM

See Distributed System Management.

DSMASR

See Application server.

DSM Server

The DSM server (user DSMSR) is the PRIMOS process that runs the DSM kernel. It acts on behalf of user processes to provide secure DSM functions such as access validation and message routing.

DSMSR

See DSM server.

FTS

Prime's File Transfer Service. A chargeable product that permits file transfer over a Prime network. For further details, see the *User's Guide to Prime Network Services.*

Function

A DSM function is a specific DSM facility to which DSM access control can be applied, through the setting up of user access definitions. DSM functions generally correspond to DSM commands. DSM function names are supplied at installation and can only be added to by Prime personnel.

Function Group

A function group is a collection of functions, used as a convenient method for configuring DSM access. Function groups can be defined using CONFIG_DSM.

ICE

The PRIMOS command that resets the user's terminal environment to system defaults. For further details see the *PRIMOS Commands Reference Guide.*

Kernel

The DSM kernel is the code that implements secure message exchange in DSM. It is used by DSM *applications.*

LOCAL$

A *nodegroup* that consists of the single node where the user is logged in.

Logging Service

The logging service is a DSM-supplied service that allows DSM applications to record messages in personal or system logs anywhere on the network. It includes the utilities for users to maintain and display those logs.

LOGOUT

The PRIMOS command for logging out a user. For further details see the *PRIMOS Commands Reference Guide.*

LTS300

See LAN300 Terminal Server.

Message

Messages are the format through which all information exchange in DSM takes place. All DSM application messages conform to the ASN.1 (CCITT X.409) standard.

Node

A DSM node is any PRIMENET node that can run a *DSM server* (DSMSR).

Nodegroup

A nodegroup is a list of related nodes, grouped for convenience. Nodegroups are a shorthand way of addressing several nodes at once when executing DSM commands and setting DSM access control.

PDN

Public Data Network.

PNC

See PRIMENET Node Controller.

PRIMENET Node Controller (PNC)

The PRIMENET hardware that controls Prime RINGNET protocols and the flow of data between nodes on a ring.

Product

A product is any piece of software that makes use of DSM features.

Product Register

The product register is part of a DSM configuration file that contains details of products. The customer product register is in the standard DSM configuration file, and the Prime product register is in the special file PRIME_REGISTER.CONFIG.

Remote File Access (RFA).

The mechanism that allows users to access files across a Prime network without logging in remotely. For further details see the *User's Guide to Prime Network Services.*

RESUS

RESUS (REmote System USer) is a DSM *application* that allows remote access to system command (User-1) facilities on any machine from any terminal on the network.

RFA

See Remote File Access.

Selection

A UMH selection is a set of criteria you can use to filter and route DSM Unsolicited Messages. Selections are defined through the command CONFIG_UM and constitute the database used by the UMH.

Severities

An attribute of an unsolicited message that indicates the nature and the importance of the message. See Chapter 5, UMH Configuration, for details on severities.

SIM

See System Information and Metering.

System Information and Metering (SIM)

The System Information and Metering facility (SIM) is a set of commands that allow operators to examine device and resource status of any system from any point on the network.

TERM

The PRIMOS command that sets the user's terminal environment. For further details see the *PRIMOS Commands Reference Guide.*

UM

See Unsolicited Message.

Unsolicited Message (UM)

An unsolicited message (UM) is any message sent to DSM's *Unsolicited Message Handling* service (UMH) to signal a system or network event. UMs are typically software-generated alarms and warnings.

Unsolicited Message Handler (UMH)

The unsolicited message handler is the generalized DSM mechanism that deals with asynchronous messages generated in a networked environment. It comprises the message filtering and routing software on a node, and the command CONFIG_UM that allows administrators to configure that software through the definition of UMH *selections.*

User access definitions

User access definitions are the elements of DSM's access control. They consist of PRIMOS user IDs linked to DSM *functions* and target *nodes*. User access definitions determine which commands users can invoke, and where they can invoke them.

USRASR

The PRIMOS command that allows the supervisor terminal to share another user's process on the system, and access the same memory space. An obsolete command. Do not use this command while in RESUS.

VC

Virtual circuit. The connection between two user processes on remote systems. Maps onto the physical connections through the PRIMENET software.

VCP

See Virtual Control Panel.

Virtual Control Panel (VCP)

The virtual control panel allows the supervisor terminal VDU to emulate the functions of the CPU switch panel.

INDEX

INDEX

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

SURVEYS

READER RESPONSE FORM

DSM User's Guide

DOC10061-3LA

Your feedback will help us continue to improve the quality, accuracy, and organization of our publications.

1. How do you rate this document for overall usefulness?

   ☐ *excellent* ☐ *very good* ☐ *good* ☐ *fair* ☐ *poor*

2. What features of this manual did you find most useful?

   _____
   _____
   _____
   _____
   _____
   _____

3. What faults or errors in this manual gave you problems?

   _____
   _____
   _____
   _____
   _____
   _____

4. How does this manual compare to equivalent manuals produced by other computer companies?

   ☐ *Much better* ☐ *Slightly better* ☐ *About the same*
   ☐ *Much worse* ☐ *Slightly worse* ☐ *Can't judge*

5. Which other companies' manuals have you read?

   _____
   _____

Name: _____ Position: _____
Company: _____
Address: _____
_____
_____ Postal Code: _____

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

First Class Permit #531 Natick, Massachusetts 01760

BUSINESS REPLY MAIL

Postage will be paid by:

Prime™

Attention: Technical Publications
Bldg 10
Prime Park, Natick, Ma. 01760