

---

---

# Unicenter

## Management Services User's Guide

11th edition

P01- 020



**Computer Associates**  
The Software That Manages eBusiness



<b>Edition</b>	<b>Publication Number</b>	<b>Publish Date</b>
11th Edition	P01-020	October 2001

This documentation and related computer software program (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by Computer Associates International, Inc. ("CA") at any time.

This documentation may not be copied, transferred, reproduced, disclosed or duplicated, in whole or in part, without the prior written consent of CA. This documentation is proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of this documentation for their own internal use, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the confidentiality provisions of the license for the software are permitted to have access to such copies.

This right to print copies is limited to the period during which the license for the product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to return to CA the reproduced copies or to certify to CA that same have been destroyed.

To the extent permitted by applicable law, CA provides this documentation "as is" without warranty of any kind, including without limitation, any implied warranties of merchantability, fitness for a particular purpose or noninfringement. In no event will CA be liable to the end user or any third party for any loss or damage, direct or indirect, from the use of this documentation, including without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised of such loss or damage.

The use of any product referenced in this documentation and this documentation is governed by the end user's applicable license agreement.

The manufacturer of this documentation is Computer Associates International, Inc.

Provided with "Restricted Rights" as set forth in 48 C.F.R. Section 12.212, 48 C.F.R. Sections 52.227-19(c)(1) and (2) or DFARS Section 252.227-7013(c)(1)(ii) or applicable successor provisions.

© 2001 Computer Associates International, Inc.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

---

# Table of Contents

<b>About This Manual .....</b>	<b>xiii</b>
Who Should Use This Manual.....	xiii
Notational Conventions .....	xiii
Commands.....	xiii
User Entries.....	xiv
Icons .....	xiv
References and Related Documentation.....	xiv
<b>Chapter 1 Introduction to Management Services .....</b>	<b>1-1</b>
What Is Management Services?.....	1-2
Operator Console .....	1-2
Security .....	1-3
Print Management .....	1-3
Communications .....	1-3
Alert Monitoring .....	1-3
Broadcasting.....	1-4
Report Writing .....	1-4
Application Development .....	1-4
Network Control Language.....	1-4
Managed Object Development Services.....	1-4
System Support .....	1-5
An Overview of the NetMaster and SOLVE Products .....	1-5
Management Services Operating Environments and Supported Terminals.....	1-6

<b>Chapter 2</b>	<b>Getting Started .....</b>	<b>2-1</b>
	User Action Conventions.....	2-2
	Accessing Management Services .....	2-2
	Logging On to Management Services.....	2-3
	Logging On to Multiple Sessions .....	2-4
	Security .....	2-4
	Changing Your Password .....	2-5
	Changing Your User Details.....	2-7
	Locking Your Terminal Against Access by Others.....	2-7
	Logging Off Management Services .....	2-8
	Accessing Functions of Management Services .....	2-9
	Selecting an Option .....	2-9
	Selecting a Function Directly—Using Shortcuts .....	2-9
	Accessing a Function by Using /shortcut-name .....	2-9
	Accessing a Function by Using =/shortcut-name .....	2-10
	Selecting a Function Directly—Skipping Panels.....	2-10
	Accessing a Panel That Is Lower in the Panel Hierarchy .....	2-10
	Accessing a Panel That Is Higher in the Panel Hierarchy .....	2-10
	Accessing a Panel That Requires Input Data.....	2-11
	Working in Two Windows .....	2-11
	Splitting Windows .....	2-11
	Swapping Between Windows .....	2-12
	Opening and Closing Windows .....	2-12
	Getting Help.....	2-12
	Getting Help for Panels.....	2-13
	Getting Help in OCS .....	2-13
	Command Help Information .....	2-13
	Getting Cursor-Sensitive Help.....	2-14
	Getting Help for Messages and Codes.....	2-14
<b>Chapter 3</b>	<b>About Operator Console Services (OCS).....</b>	<b>3-1</b>
	About OCS.....	3-2
	Accessing OCS .....	3-2
	The OCS Panel .....	3-3
	The Command Line .....	3-3
	Operating Mode Indicators .....	3-3
	The Roll Delete Area .....	3-3
	The Non-Roll Delete Area.....	3-4
	The Roll-Delimiter Line .....	3-4

The Title Line .....	3-4
The Time Display .....	3-4
Running Multiple OCS Panels .....	3-4
Setting Window IDs.....	3-4
Using Function Keys .....	3-5
Using Default Function Keys.....	3-6
Using Conversational Function Keys .....	3-6
Using Prefix and Suffix Function Keys .....	3-6
Using Function Keys to Enter Commands.....	3-7
Assigning Your Own Values to Function Keys .....	3-7
Specifying Commands to Function Keys.....	3-7
Setting Function Keys as ENTER Keys .....	3-8
Redefining the ENTER Key .....	3-8
Specifying Function Keys Using NCL Procedures.....	3-8
Using Commands.....	3-8
Command Authority Levels .....	3-9
Abbreviating Commands .....	3-9
Concatenating Commands .....	3-9
Preventing Command Concatenation .....	3-10
Reusing Commands .....	3-10
Using the Command Stack.....	3-10
Retaining Commands on the Command Line.....	3-11
Copying Display Lines into the Command Line .....	3-11
Renaming Commands .....	3-11

## **Chapter 4      Monitoring and Controlling Your Management Services Domains Using OCS..... 4-1**

About Monitoring and Controlling in OCS .....	4-2
Managing the Output on Your OCS Window .....	4-2
Controlling Message Presentation Speed.....	4-2
Stopping Message Flow Manually.....	4-2
Stopping Message Flow Automatically .....	4-3
Changing the Holding Limit .....	4-3
Contention Delay Interval.....	4-4
Unwrapping Messages .....	4-4
Clearing the OCS Window.....	4-4
Receiving Unsolicited Messages in OCS .....	4-5
Receiving Network Warning Messages .....	4-5
Replying to PPO messages.....	4-6
Intercepting and Processing PPO Messages .....	4-6

Receiving Non-Roll Delete (NRD) Messages .....	4-7
Hiding NRD Messages.....	4-7
Restoring Hidden NRD Messages .....	4-8
Deleting NRD Messages .....	4-8
Using NRD Messages with ROF Sessions.....	4-8
Using the Activity Log to Help Monitor Your Domains.....	4-9
Using the Information Database to Help Monitor Your Domain .....	4-9
Issuing Commands.....	4-10
Issuing Commands in Background Environments .....	4-10
Issuing Commands at Specified Times .....	4-11
Displaying Active Timer Commands .....	4-12
Deleting Timer Commands Manually .....	4-12
Deleting Timer Commands Automatically.....	4-13
Redirecting Timer Commands.....	4-13
Limiting Timer Command Executions .....	4-13
Executing a Timer Command under Another User ID .....	4-14
Specifying Concatenated Commands in Timer Commands .....	4-14
Executing or Starting NCL Processes from OCS .....	4-14
Executing NCL Procedures Serially .....	4-15
Executing NCL Processes Concurrently .....	4-15
NCL Identifiers .....	4-15
Executing an NCL Process from a Serial or Concurrent Process ..	4-16
The Advantages of Started Procedures .....	4-16
Monitoring and Controlling in a Restricted Environment.....	4-17
Displaying Network Partition Tables .....	4-17
Entering Commands in a Restricted Environment.....	4-17
Receiving Messages in a Restricted Environment .....	4-18
Changing the Status of Message Tables .....	4-18
Changing the Severity Level of Messages You Receive .....	4-18
Detecting Errors in Your Restricted OCS Environment.....	4-18
Using a Restricted Monitoring Environment with the Remote Operator Facility (ROF).....	4-19

<b>Chapter 5</b>	<b>Monitoring and Controlling Multiple Applications .....</b>	<b>5-1</b>
	About MAI-OC.....	5-2
	Logging On to Another Application.....	5-2
	Creating a Session Identifier .....	5-2
	Listing Established Sessions .....	5-3
	Starting an MAI-OC Session with a Specific LU .....	5-3
	Choosing an LU Name from a Pool.....	5-3
	Choosing a Specific LU Name .....	5-4
	Logging Off an Application.....	5-4
	Disconnecting an MAI-OC Session.....	5-5
	Interrupting an MAI-OC Session .....	5-5
	Sending Data to an Application .....	5-6
	Receiving Data from an Application .....	5-6
	Issuing Commands to an Application.....	5-7
	Issuing Commands while Waiting for Application Response .....	5-7
	Abbreviating Commands .....	5-7
	Issuing Multi-segment Commands to an IMS Application.....	5-8
	Session Protocols .....	5-8
	SCS Character Support .....	5-9
	SCS Characters Sent by MAI-OC.....	5-10
	Strike-over Masks .....	5-11
	JES MAI-OC Sessions .....	5-11
<b>Chapter 6</b>	<b>Monitoring and Controlling Remote Domains. ....</b>	<b>6-1</b>
	About the Remote Operator Facility (ROF).....	6-2
	Getting Maximum Benefit from ROF.....	6-2
	Using ROF in OCS.....	6-2
	Signing on to a Remote Domain.....	6-3
	Signing on to a Remote Domain over an Inactive Link.....	6-3
	Restarting a ROF Session.....	6-3
	Issuing Commands on a Remote Domain .....	6-4
	Using Command Separators.....	6-4
	Simplifying Remote Command Execution .....	6-4
	Issuing Commands from a Remote Domain .....	6-4

	Receiving ROF Messages .....	6-5
	Using Color Coded Messages .....	6-5
	Using the Message ID .....	6-5
	Signing Off a Remote Domain .....	6-6
<b>Chapter 7</b>	<b>Sending Broadcasts.....</b>	<b>7-1</b>
	About Broadcast Services .....	7-2
	Types of Broadcasts .....	7-2
	Accessing Broadcast Services .....	7-3
	Listing Broadcasts .....	7-4
	Viewing Active Broadcasts.....	7-4
	Deleting Active Broadcasts.....	7-4
	Listing System Groups .....	7-5
	Adding a Broadcast System Group.....	7-5
	Broadcasting to Generic Resources .....	7-8
	Enabling Broadcasts to Generic Resources .....	7-8
	Sending Broadcasts to Generic Resources.....	7-10
	Setting General Broadcasts.....	7-11
	Setting Primary Menu Broadcasts .....	7-12
	Reviewing Active Broadcasts.....	7-13
	Sending Dynamic Broadcasts .....	7-13
	Entering Broadcast Text.....	7-14
	Receiving Broadcasts.....	7-15
<b>Chapter 8</b>	<b>Communicating Between Management Services Domains .....</b>	<b>8-1</b>
	About Communicating Between Management Services Domains.....	8-2
	Using INMC to Communicate Between Management Services Domains .....	8-2
	Using APPC to Communicate Between Management Services Domains .....	8-2
	Using INMC to Link Management Services Domains.....	8-3
	Starting an INMC Connection .....	8-3
	Stopping INMC Links.....	8-4
	Resetting an INMC Link.....	8-4
	Displaying INMC Link Status .....	8-4
	Displaying Domain Information .....	8-5

	Troubleshooting for INMC Links .....	8-6
	Using APPC to Link Management Services Domains .....	8-7
	Starting APPC Links .....	8-7
	Displaying APPC Link Status .....	8-7
	Stopping APPC Links .....	8-8
<b>Chapter 9</b>	<b>Printing.....</b>	<b>9-1</b>
	About Print Services Manager .....	9-2
	Accessing PSM.....	9-2
	Listing Entries in the Print Queue .....	9-3
	Displaying the Output of a Print Request .....	9-4
	Modifying a Printer Entry .....	9-5
	Confirming Printing.....	9-6
	Selecting the Printer You Require.....	9-6
<b>Chapter 10</b>	<b>Linking Programs.....</b>	<b>10-1</b>
	About PPI.....	10-2
	Accessing PPI Facilities from Management Services .....	10-2
	Accessing PPI from NCL Processes .....	10-3
	NCL PPI System Variables.....	10-3
	NCL PPI User Variables .....	10-4
	Accessing PPI Facilities from Other Programs .....	10-5
	Making PPI Calls .....	10-5
	Constructing an RPB.....	10-5
	Making the Call.....	10-8
	Checking PPI Status .....	10-9
	Controlling Receiver Programs .....	10-10
	Checking the Status of a Receiver Program.....	10-10
	Obtaining ASCB and TCB Addresses .....	10-11
	Defining and Initializing a Receiver .....	10-12
	Deactivating a Receiver .....	10-14
	Deleting an Active Receiver .....	10-16
	Sending a Generic Alert to Management Services .....	10-17
	Controlling Data Buffers .....	10-19
	Sending a Data Buffer to a Receiver.....	10-19
	Allowing a Receiver to Receive a Data Buffer.....	10-21
	Purging the Data Buffer .....	10-23

	Waiting On an ECB .....	10-24
	Obtaining a Unique Sender or Receiver ID .....	10-25
	Receiving Information from a Receiver Program .....	10-27
	Tracing the Cause of a Processing Error .....	10-29
	Debugging Codes .....	10-31
<b>Chapter 11</b>	<b>Issuing System Commands from Your Console .....</b>	<b>11-1</b>
	About the SYSCMD Facility .....	11-2
	Using the SYSCMD Facility in OS/390, z/OS, MSP, and VOS3 .....	11-3
	Entering Master Console Commands .....	11-3
	Locking a Console .....	11-3
	Simulating Command Issue from a Specific Console .....	11-4
	Displaying the Status of the Console Pool .....	11-4
	Using the SYSCMD Facility in VM .....	11-5
	SYSCMD Command Summary .....	11-6
<b>Appendix A</b>	<b>Management Services Commands .....</b>	<b>A-1</b>
	Summary Table .....	A-2

## Glossary

## Index

---

# Figures and Tables

Figure 2-1.	Unicenter NetMaster: Primary Menu (Example).....	2-3
Figure 2-2.	Management Services : Primary Menu.....	2-4
Figure 2-3.	UAMS : Primary Menu.....	2-5
Figure 2-4.	UAMS : User Password Maintenance .....	2-6
Figure 2-5.	NetMaster : Terminal LOCK Panel .....	2-8
Figure 2-6.	NETINFO : Browse Utility File .....	2-14
Figure 3-1.	OCS Window Layout.....	3-2
Figure 3-2.	Setting OCS Window ID .....	3-5
Figure 7-1.	Broadcast Services : Primary Menu.....	7-3
Figure 7-2.	Broadcast Services : List Broadcasts Panel .....	7-4
Figure 7-3.	Broadcast Services : Group Definition .....	7-5
Figure 7-4.	Broadcast Services : Resource List.....	7-6
Figure 7-5.	Broadcast Services : Resource Definition.....	7-7
Figure 7-6.	Broadcast Services : Group Definition Panel .....	7-8
Figure 7-7.	Broadcast Services : Resource Definition Panel.....	7-9
Figure 7-8.	Broadcast Services : Send Menu.....	7-10
Figure 7-9.	Broadcast Services : Edit Broadcast Text Panel .....	7-11
Figure 7-10.	Broadcast Services : Review Broadcasts Panel .....	7-13
Figure 7-11.	Broadcast Services : Send Menu.....	7-14
Figure 7-12.	A Broadcast Exceeding One Screen .....	7-15
Figure 9-1.	PSM : Primary Menu .....	9-3
Figure 9-2.	Output Queue Panel .....	9-4
Figure 9-3.	Browse Output Panel .....	9-4
Figure 9-4.	Print Request Panel .....	9-5
Figure 9-5.	Confirm Printer Panel .....	9-6
Figure 9-6.	Printer List .....	9-7

Figure 11-1.	Overview of the SYSCMD Facility .....	11-2
Figure 11-2.	Results of the SHOW CONSOLES Command .....	11-4
Table 10-1.	Request Parameter Block (RPB) Format .....	10-5
Table 10-2.	Possible Return Codes from PPI and Their Causes .....	10-27
Table 10-3.	Possible Combinations of RC90 Trace Module IDs and Reason Codes .....	10-31

---

# About This Manual

Management Services is a set of features that are commonly available to all NetMaster, NetSpy, and SOLVE products. The *Management Services User's Guide* is designed to provide information on how to use the standard features of Management Services.

---

## Who Should Use This Manual

This manual is for those who use the common features of Management Services for monitoring and controlling their system in an operations environment. It is intended to cover all aspects of terminal operation, system characteristics, and system commands.

---

## Notational Conventions

This section explains the conventions used in this manual when referring to various types of commands and user entries.

### Commands

All commands in this manual are shown in uppercase. For example, SHOW USERS.

## User Entries

All examples that can be entered by a user are displayed in bold. For example, Enter **O** at the Select Option prompt ==>>.

## Icons

Icons are used to draw your attention to important information. The following icons are used in this manual:



### Warning

This icon indicates a warning to alert you to consequences of certain actions.



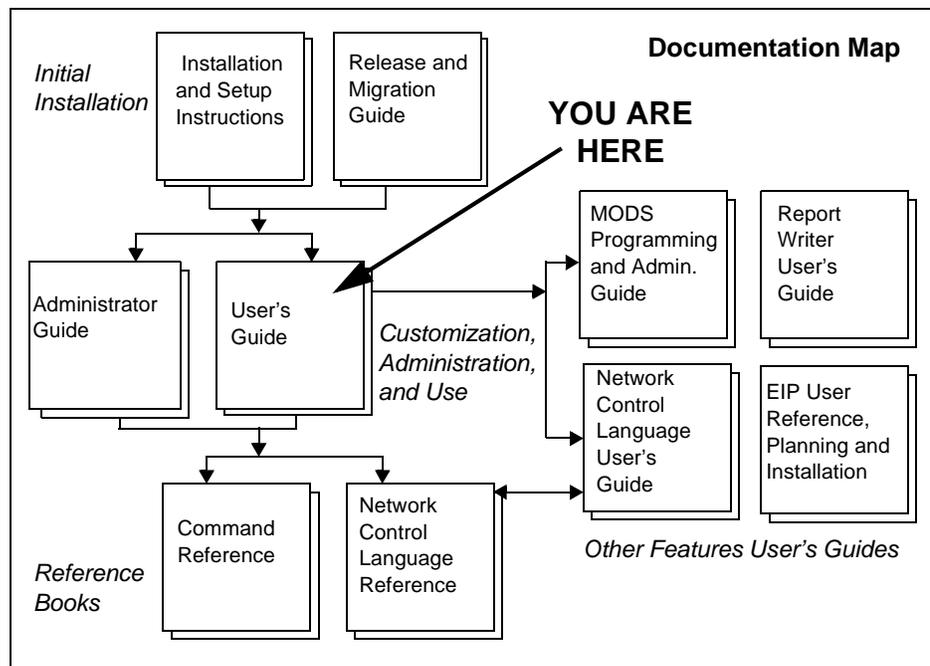
### Key Concept

This icon indicates conceptual information to help you understand the task you are performing.

---

## References and Related Documentation

This manual is part of the Management Services library. The documentation map shows the manuals in the library.



Along with the *Management Services User's Guide*, the Management Services documentation set is made up of the following manuals:

- *Management Services Version 5.01 Release and Migration Guide*—provides information about the Version 5.0 release of Management Services
- *Management Services Administrator Guide*—provides information on the implementation, customization, and administration of Management Services
- *Management Services Command Reference*—describes each of the commands available to Management Services along with examples of their use
- *Network Control Language Reference*—describes the verbs, built-in functions, and variables that make up the language that Management Services is written in
- *Network Control Language User's Guide*—describes how to use NCL to write your own code within Management Services
- *MODS Programming and Administration Guide*—describes how to use MODS to create your own panels and applications
- *Report Writer User's Guide*—describes how to use report writer to produce and print your own reports
- *EIP User Reference*—describes how to use the External Interface Package to access Management Services without using a terminal



# 1

---

## **Introduction to Management Services**

This chapter introduces Management Services and provides an overview of the services and functions provided as part of Management Services.

---

## What Is Management Services?

The NetMaster and SOLVE products are designed with a central core of functions and services. These functions and services are referred to as Management Services.

Management Services works in conjunction with any number of enterprise platforms. It provides a range of tools, general services, and facilities and is supplied with each product.

Management Services provides the following services:

- An Operator Console
- Security
- Print Management
- Communications
- Alert Monitoring
- Broadcasting
- Report Writing
- Application Development
- System Support

## Operator Console

Operator Console Services (OCS) provides an operator environment for command entry to allow monitoring and control of your domain.

OCS is used in conjunction with other features of Management Services to assist you in this task:

- Activity Log—allows you to access all the commands, messages, or errors that have been issued and logged in the domain for any given day
- Network Information Utility File—provides descriptions of errors and codes that are displayed in OCS
- Remote Operator Facility (ROF)—allows you to monitor and control remote domains through OCS
- Network Partitioning Facility (NPF)—allows you to subdivide your network so that different parts are controlled by different operators
- Event Distribution Services (EDS)—allows you to filter out unwanted messages in OCS before they are passed to an application procedure
- Multiple Access Interface-Operator Console (MAI-OC)—allows you to log on to VTAM applications for monitoring and control

For more information see chapters 3, 4, 5, and 6 in this manual, and the *Management Services Administrator Guide*.

## Security

Security for Management Services is provided by the User ID Access Maintenance Subsystem (UAMS). UAMS provides logon and password checking facilities, and the ability to control the authority and privileges of users.

For more information see the *Management Services Administrator Guide*.

## Print Management

Management Services provides a Print Services Manager (PSM). PSM is a spooling facility which allows you to control the physical printing of the reports your organization generates on JES or network printers.

For more information see Chapter 9, *Printing*, in this manual, and the *Management Services Administrator Guide*.

## Communications

Management Services provides several facilities which allow you to communicate between Management Services domains and programs, and to collect different types of message flows:

- Inter-Management Services Connection (INMC)—allows you to establish and monitor links between multiple domains
- Advanced Program-to-Program Communication (APPC)—allows you to use the APPC protocol to connect multiple domains
- Inter System Routing (ISR)—allows you to use INMC to provide centralized control at the system level
- Program-to-Program Interface (PPI)—allows you to communicate between programs

For more information on Communication Services, see Chapter 8, *Communicating Between Management Services Domains*, in this manual, and the *Management Services Administrator Guide*.

## Alert Monitoring

The alert monitor provides an event notification system that tells you that a problem has been detected and that some action needs to be taken.

For more information see the *Unicenter NetMaster Network Management for TCP/IP User Guide*.

## Broadcasting

Broadcast Services allows you to send broadcast messages to all users defined to Management Services. Messages can be sent to terminals or can be sent to specific users based on selection criteria.

For more information see Chapter 7, *Sending Broadcasts*, in this manual.

## Report Writing

Report Writer provides a facility for defining report layouts and generating reports to suit your particular site requirements.

For more information see the *Report Writer User's Guide*.

## Application Development

Application development services allows you to use facilities provided with Management Services to write your own menus, panels, and applications. Two facilities are provided for this task:

- Network Control Language (NCL)
- Managed Object Development Services (MODS)

### Network Control Language

NCL is the interpretive language which is used within Management Services to develop procedures that can then be executed by Management Services.

NCL also includes the following types of database support:

- User Database support
- NetMaster database support—by using NDBs
- Sequential database support—by using dataset services
- External database support—by using EDBS

For more information about NCL and its features, see the *Network Control Language User's Guide* and the *Network Control Language Reference*.

### Managed Object Development Services

MODS allows you to create your own applications and develop panels to provide access to them. The following features are available:

- Application Register—the definitions of all applications that are built in MODS must be defined in the application register

- Common Application Services (CAS)—a collection of high-quality, special-purpose NCL routines designed to facilitate program development
- Panel Services—a facility for creating and maintaining full-screen panel definitions
- Object Services—an object-oriented development environment used to define and maintain an application’s data and methods
- Mapping Services—a facility that enables programmers to define complex data structures for use by NCL applications
- Administrative Functions—used to maintain MODS control libraries, panel libraries, and object services support functions

For more information about MODS, see the *MODS Programming and Administration Guide*.

## System Support

System support services provides facilities to change system parameters so that you can tune, diagnose, and tailor your Management Services domain.

## An Overview of the NetMaster and SOLVE Products

The NetMaster and SOLVE products address key operational areas of the modern information processing environment. These operational areas (network management, systems administration, and systems operations) require specialized management software to maximize their effectiveness.

- Network Management  
The NetMaster products provide software that optimize the operation and services of SNA and TCP/IP networks. These products simplify network management tasks and provide user access services.
- Systems Administration  
The SOLVE:Central products help you to manage complex, modern IS environments and provision of services. For example, they allow you manage your financial assets, your domain configuration, changes to the system environment, and help desk calls and problems.

- Systems Operations  
The Automation Services and SOLVE:Operations products provide software that manages the automated monitoring of operating system activity and the automation of routine operational tasks.

## **Management Services Operating Environments and Supported Terminals**

Management Services operates within the following operational environments:

ACF/VTAM under:

- z/OS, OS/390, MVS/ESA, and MVS/XA
- VM/ESA

VTAM-G under:

- MSP/EX, MSP/E20AE, and MSP
- FSP/E26 and XSP

ECS/VTAM and XNF under:

- VOS3/AS

Management Services is designed to support large numbers of terminals concurrently. More specifically, it supports 3270-type devices (LU-0 and LU-2), and LU-1 devices. It provides all the necessary services required to establish and disconnect sessions with all 3270 model display terminals (or their equivalent).

On a Hitachi VOS3 system, Management Services also supports connection of 560/20 display terminals.

---

## Getting Started

This chapter describes the basic tasks that you need to perform to be able to navigate around Management Services, get help, and access functions.

**This chapter contains the following topics:**

- User Action Conventions
- Accessing Management Services
- Accessing Functions of Management Services
- Working in Two Windows
- Getting Help

---

## User Action Conventions

The following conventions are used when providing information on how to use Management Services:

- You select *menu options* at the Select Option ===> prompt on the second line of a menu. Type the option code or number (for example, type **O** for Operator Console Services), and press ENTER.
- You enter *shortcuts* at the ===> prompt on any panel. Type the shortcut, preceded by / (for example, type **/BCAST** for Broadcast Services), and press ENTER.
- You enter *commands* at the ===> prompt on the second line of any panel. Some commands may be valid only on certain panels. To enter system commands, type **CMD** at the ===> prompt and press ENTER. The Command Entry panel is displayed. You can now enter system commands (for example, SHOW USERS).

Frequently used commands such as EXIT and FILE are assigned to function keys which are listed at the bottom of most panels. Press the appropriate function key to execute these commands.

*Enter* used in conjunction with commands means: type the commands at the ===> prompt, and press ENTER.

- You can apply *actions* to listed items (if the list is an action list, such as the XXX list). You can apply actions such as browsing, copying or updating to individual items. Press TAB to move the cursor down to the required item and enter the action code (for example, B for browse) beside the item.

*Enter* used in conjunction with actions means: position the cursor beside the required item, type the action code, and press ENTER.

- You can enter options, commands, and action in either upper or lower case.
- Use the TAB key to move the cursor from field to field on a panel.

---

## Accessing Management Services

To access Management Services you must log on to the system. Before you can do this, you need to have a user ID and password. Ensure that your systems administrator has defined your user ID to Management Services and has allocated the relevant level of authority.

For more information on defining user IDs and access authorities, see the *Management Services Administrator Guide*.

When you log on to Management Services for the first time, the UAMS : Password Maintenance panel is immediately presented so that you can change your password. See steps 4 and 5 in the section titled, *Changing Your Password*, on page 2-5, for details on how to use this panel.

## Logging On to Management Services

You can begin a Management Services session in a number of different ways:

- Natively, by logging on directly from a terminal
- Indirectly, via Remote Operator Facility (ROF) connection from another system where you are directly logged on
- Externally, via a Multiple Application Interface (MAI) session
- Externally, via a session from a TSO/TSS address space (for z/OS, OS/390, or MSP systems), using the External Interface Package (EIP) option

To log on to Management Services in any of these ways, type your user ID and password at the logon panel, and press ENTER. The Unicenter NetMaster : Primary Menu is displayed (see Figure 2-1 for an example).

*Figure 2-1. Unicenter NetMaster: Primary Menu (Example)*

```
PROD----- Unicenter NetMaster : Primary Menu -----
Select Option ==>

M - Monitors                               Userid USER01
H - Historical Data                          LU      NMMAF057
D - IP and SNA Network Diagnosis            Time    10.18.44
I - Information Management                  THU 05-JUL-2001
MAI - Access Services                       OPSYS   OS390
U - User Services                           Window  1
O - Operator Console Services
A - Administration and Definition
SP - SNA Performance (Appl ID NSD1VD1N)
X - Terminate Window/Exit

Tip of the day: Use a combination of a shortcut + options to access a function

(C) 1981,2001 Computer Associates International, Inc. All Rights Reserved.
F1=Help      F2=Split      F3=Exit      F4=Return
              F9=Swap
```

The functions displayed on the menu depend on which functions you are authorized to access. If you are authorized for only one function, then the Unicenter NetMaster : Primary Menu is not displayed—the menu for the function you are authorized for is displayed.

Enter **/MS** at the **====>** prompt on the Primary Menu. The Management Services : Primary Menu is displayed.

*Figure 2-2. Management Services : Primary Menu*

```
PROD----- Management Services : Primary Menu -----/MS
Select Option ==>

  U - Userid Access Maintenance Subsystem          UAMS
  LU - Active User List                            USERS
  B - Broadcast Services                          BCAST
  D - Managed Object Development Services          MODS
  S - System Support Services                      SS
  I - INMC Link Maintenance                       INMCL
  WS - Data Warehouse Services                    WS
  E - Help Messages and Error Codes               CODES
  PS - Print Services Manager                     PSM
  R - Report Writer                               REPORT
  LA - Activity Log Administration                 LOADMIN
  L - Activity Log                                LOG
  X - Exit

User ID ..... (Optional LU)
Link or Domain Name ....+ (Optional LU L)

F1=Help      F2=Split      F3=Exit      F4=Return
              F9=Swap
```

## Logging On to Multiple Sessions

You can log on to multiple Management Services sessions concurrently under the same user ID on the same system provided you are authorized to do this in your user ID definition.

By default, the system allows you to have the following combination of sessions concurrently:

- One ROF connection from another system
- One EIP connection from a TSO address space
- Either one direct terminal session, or one MAI connection

If your user ID is authorized for multiple signon privileges, you can have multiple ROF, EIP, direct, and MAI connections concurrently under the same user ID.

## Security

Management Services provides the Userid Access Maintenance Subsystem (UAMS) to maintain your password and User ID information. Your systems administrator uses UAMS to control the privileges and authorities assigned to you. UAMS also allows you to perform the following security functions:

- Change your password
- Change your user details

Management Services also provides a terminal lock facility that allows you to lock your terminal against access by other users.

These tasks are described in the following sections.

## Changing Your Password

You can change your password at any time after you log on to Management Services. The change becomes effective immediately. You are also automatically prompted by the system to change your password when it is about to expire.

### Note

Your installation might have an external security package. If this is the case, your systems administrator will tell you if there are any special considerations that apply when changing your password.

To change your password, complete the following steps:

- Step 1. Enter **/UAMS** at the **====>** prompt on any panel. The **UAMS : Primary Menu** is displayed.

Figure 2-3. *UAMS : Primary Menu*

```
PROD----- UAMS : Primary Menu ----- $UA001
Select Option ==>

  A - Add User Definition                Userid USER01
  B - Browse User Definition             LU      NMMAF057
  C - Copy User Definition               Time   10.26.17
  D - Delete User Definition             THU   05-JUL-2001
  F - Force User's Password Change
  L - List User Definitions
  M - MAI Session Definition Maintenance
  P - Password/Details Change for your User
  U - Update User Definition
  X - Exit

User ..... USER01      (Required A B C D F U Optional L M )
Definition Type .... User (Required A - 'USER' or 'GROUP')
Confirm Delete? .... Yes (Required D )

F1=Help   F2=Split   F3=Exit   F4=Return
           F9=Swap
```

- Step 2. Enter **P** at the **====>** prompt on the **UAMS : Primary Menu**.  
The **UAMS : User Password Maintenance** panel is displayed).

Figure 2-4. UAMS : User Password Maintenance

```
USER01----- UAMS : User Password Maintenance -----Page 1 of 2
Command ===>                                     Function=Request

User ID ..... USER01

Current Password .....
New Password .....

User Name ..... User One
User Location ..... Sydney
Telephone Number ..... Ext 999

Time Zone Name .....+

F1=Help      F2=Split    F3=File
              F8=Forward  F9=Swap
                                           F12=Cancel
```

Step 3. Type in your current password and the new password in the appropriate fields, and press ENTER.

To ensure security, what you type is not displayed. Your current password must be entered correctly before you can enter a new password.

Step 4. Re-enter the new password to verify the change.

Step 5. Press F3 (File) to save the change.

Passwords can be from 1 to 8 characters long and cannot contain embedded blanks. Your installation might require that passwords be of a minimum length, and reject a password that is too short.

### *Expired Passwords*

The system enforces a password change for each user ID after an elapsed interval which can be installation defined. Unless it has been changed in your installation, this interval is 30 days. If you let your password interval expire, the system forces you to change passwords the next time you log on, by presenting you with the password maintenance panel.

### *Forgotten Passwords*

If you forget your password, you should contact your systems administrator who will generate a new password for you. For security reasons, once you have logged on successfully with your new password, you will be requested to change it.

## Changing Your User Details

Your user details are on the same panel as you use to change your password.

To change your user details, complete the following steps:

- Step 1. Enter **/UAMS** at the `====>` prompt on any panel. The UAMS : Primary Menu is displayed.
- Step 2. Enter **P** at the `====>` prompt on the User Services : Primary Menu. The UAMS : Password Maintenance panel is displayed.
- Step 3. Overtyping the incorrect information displayed on the User Password Maintenance panel.
- Step 4. Press F3 (File) to save the changes.

Your new user details come into effect the next time you log on to the system.

## Locking Your Terminal Against Access by Others

A terminal lock facility is provided with Management Services to prevent unauthorized access to a terminal. When you leave your terminal unattended, you can use the lock facility so others cannot use your terminal. You can also type a message to appear on your screen letting other users know where you are. The lock can only be released by typing in your password.

To invoke the terminal lock facility manually, complete the following steps:

- Step 1. Enter **LOCK** at the `====>` prompt at the top of any panel. The NetMaster : Terminal LOCK panel is displayed.
- Step 2. Type up to three lines of text explaining why the terminal is locked.

To unlock your terminal, enter your password at the Enter password to unLOCK terminal `====>` prompt, and press ENTER. You are returned to the same panel from where you entered the LOCK command.

Figure 2-5. NetMaster : Terminal LOCK Panel

```
PROD----- NetMaster : Terminal LOCK -----
                                                    Time  10.38.17
                                                    THU 05-JUL-2001

This terminal, ASYD3207 , has been LOCKed by USER01

Enter password to unLOCK terminal ===>

Optional text to explain the reason for this LOCK:

===> Gone to meeting
===> Back at 16:00
===>

F1=Help          F3=Disc
```

The lock facility can also be initiated automatically by the timeout facility. This can be specified in your user ID definition. See your systems administrator for more information about this.

A locked terminal can be disconnected by pressing the F3 (Disc) key. The disconnect function does not cancel any currently active sessions.

## Logging Off Management Services

To end a Management Services session, enter =x at the ===> prompt on any panel.

If you are at the Unicenter NetMaster : Primary Menu, enter x at the ===> prompt to end your current session.

**Note**

If you have more than one session or window connected to Management Services, repeat the procedure to end all remaining sessions.

---

## Accessing Functions of Management Services

You can access the functions of Management Services through the user interface menus by doing one of the following:

- Selecting an option from each menu that leads to a function
- Specifying the shortcut to go to the function directly
- Specifying the path to go to the function directly

### Selecting an Option

The primary menu lists the functions provided by Management Services (see Figure 2-2). Each entry in the list is preceded by a letter. To select the function you want, enter its corresponding letter at the `====>` prompt.

For example, to access the OCS console, enter **O** at the `====>` prompt on the Unicenter NetMaster : Primary Menu.

### Selecting a Function Directly—Using Shortcuts

You can jump to the panel of a function directly by using shortcuts. You can specify the shortcut at a `====>` prompt in one of the following ways:

- Specify `/shortcut-name` to retain the current panel on return.
- Specify `=/shortcut-name` to close the current panel and return to the primary menu on exit.

Each entry on a menu may be followed optionally by a shortcut, displayed in turquoise. If you do not remember a shortcut, enter `/` or `=/` to list the shortcuts and then select one.

#### Accessing a Function by Using */shortcut-name*

##### Caution

If your current panel does automatic updates and you no longer need this information, use `=/shortcut-name` rather than a nested shortcut. This saves storage and resources because the region does not need to maintain a display that you no longer need.

To select the function you want, enter its corresponding shortcut, preceded by the slash (`/`) character, at a `====>` prompt.

For example, to access the Broadcast Services menu, enter `/BCAST` at the `====>` prompt on your current panel. When you have finished with the menu, press F3 to redisplay your previous panel.

When you access a function by using its shortcut, your current panel is retained. When you press F3 to exit out of the function, this panel, with any updates, is restored. By using shortcuts, panels can be nested to a maximum of 64 levels.

### Accessing a Function by Using `=/shortcut-name`

Whenever you have finished with your current panel, you can access the next function by prefixing the shortcut call with the equals (=) sign. This goes directly to the function without retaining the current panel and closes all other nested panels in this window.

For example, to access the Broadcast Services menu without retaining the current panel, enter `=/BCAST` at the `====>` prompt on your current panel. When you have finished with the menu, press F3 to display the primary menu.

### Selecting a Function Directly—Skipping Panels

You can jump to the panel of a function directly by specifying the exact path to that panel. Construct the path by linking the options you need with periods. Depending on which panel you start from, you specify the panel path in one of the following ways:

#### Accessing a Panel That Is Lower in the Panel Hierarchy

If you start from a menu and want to access a panel lower in the panel hierarchy, specify the path as it is. For example, if you are at the primary menu and want to send a message to all system users via broadcast services, type `A.MS.B.S` at the `====>` prompt and press ENTER. The Broadcast Services : Send Menu is displayed.

#### Accessing a Panel That Is Higher in the Panel Hierarchy

If you want to access a panel that requires you to pass through a panel higher up in the panel hierarchy, you must precede the path specification with the equals sign (=). The = character brings you back to the primary menu and then to the required panel. You can specify such a path at any `====>` (or `=>`) prompt. For example, if you are at the UAMS : Primary Menu and want to access the Broadcast Service : Send Menu, enter `=A.MS.B.S` at the `====>` prompt and press ENTER. The Broadcast Services : Send Menu is displayed.

To return to the primary menu, enter `==`.

## Accessing a Panel That Requires Input Data

If you want to access a panel that requires you to enter data, you can enter the data by separating them from the path by a semicolon (;). For example, if you are at the primary menu and want to access the IP resource monitor for the linked region PROD2, type **M.I;PROD2** at the ==> prompt and press ENTER.

### Note

Before letting you access any panel, Management Services automatically checks whether you are authorized to use that function.

---

## Working in Two Windows

If you want to have two functions of Management Services running at once, you can split the screen to create two windows. Each of these windows can have a different function of Management Services running, and you can swap between the two.

### Splitting Windows

To split your screen, press F2 (Split) at any panel to create a second window with a copy of the primary menu.

The screen can be split in the following two ways:

- Horizontally—put the cursor on any line of the main body of the screen except the top line, or the bottom line of the screen. Press F2 to divide the screen horizontally, with each window one above the other. The boundary of the two windows is on the same line as the cursor.
- Vertically—put the cursor anywhere on the bottom line of the screen, excluding the first and last column, and press F2 to show two windows side by side. The boundary of the two windows is on the same column as the cursor. Vertical splitting is particularly useful when using a wide screen, such as a Model 5 3270 terminal.

### Note

If you press the F2 (Split) key when the screen is already split, the split orientation is swapped.

The system default F2 function key might have been overridden in your application, in which case use the SPLIT command.

## Swapping Between Windows

To swap between the two windows you have created, press F9 (Swap). This will cycle through the two windows. F9 also opens a new window if only one window is open.

## Opening and Closing Windows

The system lets you operate a terminal in split-screen mode where one window has zero size, and the second window occupies the whole screen. The zero window is said to be closed.

To close a window, put the cursor anywhere on the top line, or in column 1 of the bottom line of the screen, and press F9 (Swap). Any messages arriving at a closed window are queued for display as soon as the window is reopened.

To reopen the closed window, position the cursor where the split is required and press F9 (Swap).

To exit from split screen mode, enter =x.

---

## Getting Help

Extensive online help is available for Management Services.

Online help is context sensitive and available at different levels. When you are viewing a help panel, the following function keys are useful:

<b>Function Key</b>	<b>Description</b>
F1 (Help)	Takes you to the next level
F3 (Exit)	Takes you back to the previous level of help, or exits help and returns you to the application
F4 (Return)	Exits help and returns you to the application immediately

The following types of help are available:

- Application level help—provides information about the application you are using, for example, Management Services
- Function level help—provides information about the function you are using, for example, Broadcast Services
- Panel level help—provides information about using a panel, how to complete the fields, and the actions you can perform on a panel
- Field level help—provides specific information on the selected field

- Command help—provides information about the use of the Management Services commands and their syntax
- Message help—provides information about what a message means

You can get help about how to use help by pressing F6 (HelpHelp) when you are already in help.

## Getting Help for Panels

To find out what a panel is used for, what each of the options mean, and how to fill out the fields on a panel, press F1 (Help) while the required panel is displayed on your screen.

## Getting Help in OCS

There are several types of Help information available from your OCS window. These are described in the following sections:

- Command help
- Cursor-sensitive help
- Messages and codes help

### Command Help Information

Help information is available for Management Services commands directly, or you can display a list of all Management Services commands from which a specific selection can be made, as follows:

- If you know the name of the command for which you need help, enter that command at the OCS window command line and press F1 for details. (Instructions are displayed on-screen to help you move around the Help information panels.)
- If the command you type in is not recognized by the system, a selection list is displayed, starting with the nearest matching command. Position the cursor next to a specific command on the list and enter **S** (Select).
- If you leave the command line blank and press F1, a Help screen is displayed which explains how to use the help facility.

#### Note

Using the full screen help facilities does not erase or alter the original OCS display. When you exit from Help mode, by using the F3 key, the original OCS window reappears.

## Getting Cursor-Sensitive Help

To display online help information for any command or message number appearing on the OCS screen, position the cursor on the line with that command or message number, and press F1.

## Getting Help for Messages and Codes

Additional help information about messages and codes can be accessed from a special help database supplied with Management Services—the Network Information Utility File. This contains several categories of commonly-used information.

To get help information from one of these categories, complete the following steps:

- Step 1. Type NETINFO at the ==> prompt in the OCS window, and press F1. The NETINFO : Browse Utility File panel is displayed.

*Figure 2-6. NETINFO : Browse Utility File*

```
----- NETINFO : Browse Utility File -----
SELECT CATEGORY ==>>

      Category      Contents
      1 - 3274 Error Codes
      2 - SNA Sense Codes
      3 - SNA Status Codes
      4 - SOLVE Messages
      5 - 3174 Error Codes
      6 - VTAM ACB Error Codes
      7 - Dynamic Allocation Error Codes
      8 - VSAM OPEN Macro Return Codes
      9 - NDB Error Codes
     10 - HELP DESK Control Data
     11 - SQL Error Codes
     12 - DB2 Error Codes
     25 - NPSI Error Codes
          **END**
```

- Step 2. Type the corresponding number of the category you require at the SELECT CATEGORY ==>> prompt, and press ENTER.

A full screen display of the information available for that item is displayed. Press the ENTER key to scroll forward to display successive values within the same category. The exception to this is option 4 - SOLVE Messages, where standard function keys are used to scroll backward (F7) to the previous message and forwards (F8) to the next message.

If you know the number of the category that you want to access, you can enter this category number followed by the code directly at OCS window command line. For example, to display help for the SNA Status Code PCTD2, type **3 PCTD2** and press F1.

Each of the information categories (numbered 1 to 12 and 25) are described below:

No.	Category	Description
1	3274 Error Codes	Use the 3-character 3274 terminal error codes as the command line subject value. The error codes raised are listed along the bottom line of any 3270 terminal when connected to a 3274 controller
2	SNA Sense Codes	Error conditions for physical or logical resources within an SNA network are identified by 4-character Sense Codes
3	SNA Status Codes	Network resource VTAM displays will identify the status of each physical and logical network resource with a unique code word
4	SOLVE Messages	Details for any message are available on-line
5	3174 Error Codes	Use the 3174 terminal error codes as the command line subject value. These error codes display in the operator information area of any 3270 terminal
6	VTAM ACB Error Codes	If Management Services cannot open any of its Access Control Blocks (ACBs) to connect to VTAM, it logs an error message indicating the cause of the failure
7	Dynamic Allocation Error Codes	Allocation errors, caused from ALLOC command execution, or when File Transmission Services (FTS) attempts to allocate a file, are logged to authorized OCS operators
8	VSAM Open Macro Return Codes	VSAM ACB open processing errors generate messages where the cause of the error is indicated by a return code
9	NDB Error Codes	Commands and NCL verbs used to access Management Services Databases (NDBs) may return NDB error codes, or messages with NDB error codes
10	Help Desk Control Data	Display details for Network Control System (NCS) Help Desk facility screen definitions. Enter the Help Desk screen name as the command line subject value
11	SQL Error Codes	Return codes returned to &SQL, as determined by DB2 database
12	DB2 Error Codes	Return codes returned to EDB, as determined by DB2 database

No.	Category	Description
25	NPSI Error Codes	Error conditions for X25 Network session or session start errors

To return to the OCS window, press F3.

**Note**

Your site might have added categories of help.

---

## About Operator Console Services (OCS)

This chapter describes how to use the basic functions of OCS.

**This chapter contains the following topics:**

- About OCS
- Accessing OCS
- Using Function Keys
- Assigning Your Own Values to Function Keys
- Using Commands



The OCS window (Figure 3-1) is described in detail in the following sections.

## The OCS Panel

The OCS panel has two distinct activity areas: a one-line command input area at the bottom of the window, and an output message display area called the roll delete area, which occupies the remaining space above the command line.

### The Command Line

The command line is the bottom line of the OCS window. The command line is the only display field where input is allowed. The cursor is automatically positioned to the left of the line when the panel is first displayed. To enter a command, you must position the cursor in the command line and press ENTER.

### Operating Mode Indicators

A mode indicator might appear to the left of your command entry area to indicate how the OCS window is currently operating. Values of the operating mode indicators and their meanings are as follows:

#### **M (Monitor)**

Terminal has monitor status and receives monitor messages

#### **P (Paused)**

An NCL procedure has paused awaiting the entry of a GO, END, or FLUSH command. The SHOW NCL command gives you further details.

#### **W (Waiting)**

An NCL procedure is waiting for specific text to arrive. The SHOW NCL command gives you further details.

### The Roll Delete Area

When you receive messages as the result of commands entered on the command line, they are reported in the roll delete area with any unsolicited information you are profiled to receive.

Output to the roll delete area is written line-by-line from top to bottom of the screen. When the display area is full, new output messages wrap back to the top of the screen, overwriting the oldest displayed messages first.

## The Non-Roll Delete Area

Any messages that you receive that require a reply are delivered as non-roll delete messages. This means that the messages stay on your screen until they are dealt with by you. These messages are displayed at the top of an OCS window above the roll delete area. The non-roll delete area is only created when a non-roll delete message is delivered to your OCS window.

## The Roll-Delimiter Line

Messages are written from top to bottom of the screen. The next line for use is filled by a line of underscore (\_) characters. This line is called the roll-delimiter line. It separates the oldest and newest output displayed. Output below this line is the oldest display information; output above the line is the most recent.

### Note

The underscore characters used for this line can be changed using the PROFILE DELCHAR command.

## The Title Line

The top of the roll delete display area is reserved for a title which can be set/reset by using the TITLE command.

## The Time Display

The top left-hand side of the title line includes the present time in HH.MM format and is automatically updated each time anything is written to the OCS window.

## Running Multiple OCS Panels

You can use the screen-splitting function to run two OCS windows in parallel on the same screen. See Chapter 2, *Getting Started*, for more information about this function.

You can have one screen window operating in OCS with the remaining part-screen or window in fullscreen mode (for example, as a menu).

## Setting Window IDs

When two OCS windows are running simultaneously, it helps if you can distinguish each window while executing NCL procedures.

To set a name for each OCS window, enter the OCSID command followed by a 1- to 8-character name at the command prompt on an OCS window and press ENTER. The name for each window is displayed to the right of the line, immediately above the command line.

For example, to set a window ID of NET01, enter the following command:

```
OCSID NET01
```

After pressing ENTER, NET01 appears to the right of the line immediately above the command line (see Figure 3-2).

Figure 3-2. Setting OCS Window ID

```
(16.49)----- Operator Control Services (PROD) -----  
ocsid net01  
N16201 NEW OCS WINDOW ID SET.  
  
-----NetMaster-----NET01  
==> OCSID NET01
```

**Note**

Profile attributes can be set for each OCS window, so that you can have two OCS windows on the same terminal with different profiles and appearances. The PROFILE command, which governs the attributes of each OCS window, is described in the *Management Services Command Reference*.

---

## Using Function Keys

OCS windows have full support for 24 function keys. Function keys can be set for each OCS window to suit your requirements. If you are running two OCS windows, each window can have a separate set of function key definitions.

A variety of function keys are available:

- Default (system-wide) function keys
- Immediate function keys
- Conversational function keys
- Prefix function keys

- Suffix function keys
- NCL controlled function keys

## Using Default Function Keys

The values assigned to function keys on a system-wide or global basis are defined when your system is first set up. The OCS function keys are always set to these system default values when you enter OCS. The default system-wide function key settings are described in the *Management Services Administrator Guide*.

When you redefine a function key, its defined value applies only to the function key settings for your current window, and only remains in effect while your current window is active. See the section, *Assigning Your Own Values to Function Keys*, on page 3-7, for details on how to redefine function key values.

When you press an immediate function key, its assigned value is immediately entered into the system, without the need for further action by you (compare this with *Using Conversational Function Keys*, below).

To discover the assignment of each function key, use the PF LIST command.

## Using Conversational Function Keys

When you press a conversational function key, its assigned value is displayed in the command line, so you can add to or modify the text. Press the ENTER key to enter the command once the command has been modified.

## Using Prefix and Suffix Function Keys

A prefix function key assigns a set value as a prefix to the line of text where the cursor is located when that function key is pressed (that is, either the command line or any other line in the OCS window display area).

For example, if F6 has been defined using the following command:

```
PF6 PREF,MSG USER1+
```

when you enter a message in the command line saying: SYSTEM DOWN AT 17.00, and press F6, the following command is generated and entered:

```
MSG USER1 SYSTEM DOWN AT 17.00
```

### Note

The plus sign (+) leaves a blank after the text before concatenating it with the entered string.

A suffix function key acts like a prefix key, but adds its value to the end of the line of text where your cursor is positioned (that is, either the command line or any other line in the OCS window display area).

## Using Function Keys to Enter Commands

You can assign values to function keys by using the PF command. Whenever you press that function key it is equivalent to entering the set command from the command line. See the following section, *Assigning Your Own Values to Function Keys*, for details.

---

## Assigning Your Own Values to Function Keys

You can assign your own values to function keys so that they invoke an NCL procedure or act as the ENTER key. If a function key is being used as the ENTER key, you can redefine the ENTER key to perform an OCS function.

## Specifying Commands to Function Keys

The Management Services system provided already has some default function key values. To display the current function key settings for your OCS window, enter the PF LIST command at the prompt on your OCS window.

To specify different values to any of the function keys, use the PF command. You can specify the new function key value as one of the following:

- Conversational—the value of the function key appears in the command line so that it can be edited before being issued
- Immediate—the function key performs an immediate function such as ENTER
- Suffix—the function key value is placed at the end of an entry in the command line
- Prefix—the function key value is placed at the beginning of an entry in the command line

For example, to assign the SHOW NCL command as a conversational function key to the F4 key, enter the following command:

```
PF4 CONV,SHOW NCL=
```

When you press F4 from now on, SHOW NCL= is displayed at the command prompt so that you can add to it before executing it.

For more information about the PF command, see the *Management Services Command Reference*.

## Setting Function Keys as ENTER Keys

The PF command is also used to set a function key to act as the ENTER key. The ENTER key is defined as an immediate function key with no associated value. For example, to define PF12 as the ENTER key, enter the following:

```
PF12 IMM
```

PF12 now acts as the ENTER key as there is no entry after IMM. Now when you press F12, text is entered in the command line as if the ENTER key had been pressed.

## Redefining the ENTER Key

The ENTER command is used to reset the value of the ENTER key. For example, if you wanted to reset the value of the ENTER key to act as the CLEAR command, type the following:

```
ENTER CLEAR
```

The ENTER key no longer acts in its standard manner, so you must define at least one other OCS function key to replace the ENTER key function, *before* you can redefine the ENTER key value.

For more information about the ENTER command, see the *Management Services Command Reference*.

## Specifying Function Keys Using NCL Procedures

You can also assign values to a function key from an NCL procedure. By setting the appropriate function keys in an NCL procedure and setting your initial command to execute the NCL procedure on entry to OCS, you can reset the function keys for your OCS session.

---

## Using Commands

OCS windows can be used to enter Management Services commands and monitor the results. These commands include:

- VTAM network control commands
- Operating system commands
- Management Services commands

Commands are entered on the command line and take effect once the ENTER key is pressed. For a list of commands available for manipulating the system see Appendix A, *Management Services Commands*. These commands are fully described in the *Management Services Command Reference*.

You can access a list of all Management Services commands from on-line help. To access this list, press F1 (Help) from any OCS window. You can select any of the commands displayed to get more information about its use and syntax.

## Command Authority Levels

All commands are assigned an authority level within the range 0 to 255, zero being the lowest and 255 the highest authority level. The operands on some commands might require a higher authority than the base command itself.

You are allocated a command authority level in your user ID definition, corresponding to the scope of system control you require. Whenever you enter a command, your user ID authority level must be equal to or higher than the authority level of the command entered, otherwise the command is rejected.

This authority level checking also applies to commands executed from NCL processes invoked under your user ID.

## Abbreviating Commands

All commands consist of a single command which can be followed by one or more operands. Most commands can be abbreviated to the smallest number of characters consistent with their being distinguishable from any other Management Services command. For example, the SHOW command can be abbreviated to SH.

## Concatenating Commands

Several commands can be entered simultaneously by concatenating them into the same OCS command line and separating each command in the line with the command separator: a semicolon (;). The concatenated commands are processed from left to right in the order in which they are entered.

For example, the command string `D LU10;D LU11` is treated by the system as two independent commands:

```
D LU10
D LU11
```

You can use the CLEAR command in this manner to clear the display area before the results of the next command are displayed. For example:

```
CLEAR;D BFRUSE
```

If you need to enter a semicolon as part of a command (that is, to use it as part of the command text), you must enter two semicolons instead of one.

For example, to enter the command `a ; b`, you must enter `a ; ; b`. The second semicolon is stripped from the text and the `a;b` string passed to the system as a single command. The remaining semicolon is not regarded as a command separator character.

Command separators are specified by using the `PROFILE CMDSEP` command (see the *Management Services Command Reference* for more detail).

## Preventing Command Concatenation

You can prevent command concatenation, by using the `CMDSEP` operand of the `PROFILE` command. When `CMDSEP` is set to `NO`, semicolons are not regarded as command separators and are always treated as part of the command string.

You can still assign concatenated commands to function keys as the value of the `CMDSEP` operand is overridden by the value that the operand contained when the function key was defined.

## Reusing Commands

If you enter a command regularly, you do not need to retype it every time you want to issue the command. There are two facilities provided with OCS which allow you to reuse commands you have previously entered. These facilities are explained below.

### Using the Command Stack

Each OCS window keeps a stack of the commands most recently entered from its command line. The stack does not include immediate function key entries. The number of entries kept in this stack can be changed by using the `PROFILE CMDSTACK` command (see the *Management Services Command Reference* for more details).

You can use the command stack to retrieve previous commands entered and re-display them on the command line so they can be modified for re-entry.

Commands are retrieved from the stack using the `CS+` or `CS-` commands. The default system function key series includes settings for the `CS+` and `CS-` commands. These are `F10` and `F11` respectively. It is recommended that you retain these. The `CS+` and `CS-` commands are fully described in the *Management Services Command Reference*.

## Retaining Commands on the Command Line

When you execute a command, the command can be retained on the command line so that you can execute it again, or edit the command before executing it again. This facility lets you increment and enter command sequences with minimal effort.

This feature can be turned on or off using the `PROFILE CMDKEEP` command. When turned off, the command line is cleared as soon as the `ENTER` key is pressed and a command must be retrieved from the command stack if it is required again. When turned on, the command you enter is retained on the command line so that it can be entered again.

## Copying Display Lines into the Command Line

To copy a command (or some other message) from an OCS window display area to the command line, put the cursor on the line you wish to copy, and enter `CS+` or `CS-` (or press `F10` or `F11`). The command or message appears in the command line.

## Renaming Commands

`EQUATE` commands can be included in initialization procedures to do the following:

- Override or rename standard commands
- Define a series of 1- to 8-character length strings for use in place of lengthy command strings

The `EQUATE` command and its use is fully described in the *Management Services Command Reference*.



# 4

---

## Monitoring and Controlling Your Management Services Domains Using OCS

This chapter describes how to use OCS to monitor and control your Management Services domains.

**This chapter contains the following topics:**

- About Monitoring and Controlling in OCS
- Managing the Output on Your OCS Window
- Receiving Unsolicited Messages in OCS
- Receiving Non-Roll Delete (NRD) Messages
- Using the Activity Log to Help Monitor Your Domains
- Using the Information Database to Help Monitor Your Domain
- Issuing Commands
- Executing or Starting NCL Processes from OCS
- Monitoring and Controlling in a Restricted Environment

---

## About Monitoring and Controlling in OCS

OCS allows you to monitor and control your domains by receiving messages and allowing you to issue commands. Events from your network are sent to your OCS window so that you can act appropriately. You can issue commands to take control of any problems that might occur.

You can also use other Management Services features to assist you with monitoring and controlling your domains. The activity log provides details of all commands and messages that were issued and received for a specified day, and the information database provides information about the messages that you receive.

---

## Managing the Output on Your OCS Window

As you receive messages and output from commands, you can control, re-order, or clear output on the screen so that it can be read more easily. These options for managing the output on your OCS window are described below.

### Controlling Message Presentation Speed

When the bottom line of the display area is filled, the system pauses before wrapping back to the top of the display area to write the next message.

Sometimes, a large number of messages might be sent to the screen within a very short period of time. This causes the display to roll messages faster than you can read them. There are two options you can use to temporarily suspend message delivery or change the way the messages display:

- The HOLD option
- The AUTOHOLD option

### Stopping Message Flow Manually

To stop the flow of output to the screen at any time, press the ENTER key while nothing is in the command line. This freezes the display and no further messages appear until you enter data.

While the screen is frozen, the word HOLDING appears immediately above the command line.

## Stopping Message Flow Automatically

The default value for automatic hold supplied with your system automatically freezes an OCS window when a message fills the last line and there are messages queued to wrap back to the top of the screen. This is specified by the AUTOHOLD command.

When AUTOHOLD freezes your screen, the caption AUTOHOLD is displayed above the command line. No further messages appear until you input something.

The AUTOHOLD command option is part of your operator profile. See the AUTOHOLD command description in the *Management Services Command Reference* for more information.

### Note

If more unsolicited messages arrive while the screen is in HOLDING or AUTOHOLD mode, the caption above the command line changes to MSG QUED, and the terminal alarm sounds.

## Changing the Holding Limit

Management Services only queues a limited number of messages for an OCS window while in the HOLDING or AUTOHOLD mode. The queue limit default before any OCS window messages are discarded is 200 messages.

The HOLDING or AUTOHOLD caption above the command line changes to 75% LIMIT, HOLD LIMIT, and then MSGS LOST, as this limit is approached, reached, and then exceeded. Each caption change also sounds the terminal alarm. These conditions vary and update while you actively monitor and release system messages in the OCS window.

The queue limit can be defined for each OCS user window by using the PROFILE command.

If you want to change this limit, see the PROFILE command in the *Management Services Command Reference*.

## Contention Delay Interval

One of the characteristics of an OCS window is that Management Services can send messages to your window at the same time as you are entering a command. These messages are displayed differently depending on the type of terminal you are using:

- A non-SNA terminal—any data you have just entered is immediately frozen and any new data entered is ignored while the message writes to the screen. You can then continue to type in your command text when message delivery has finished.
- An SNA 3270 terminal—a contention condition arises. The terminal is seen as being in a send state (because you have started typing on the keyboard), and refuses to accept any output from Management Services until your input has been sent. However, rather than defer Management Services indefinitely, the system interrupts you after a set period and forces the output of a message.

The default contention delay interval is 15 seconds. This is usually long enough to let you complete a standard command input operation.

## Unwrapping Messages

To resequence or unwrap messages displayed in your OCS window, enter the ORDER command. The OCS messages are re-displayed in the window in chronological order, with the oldest messages at the top of the window.

The ORDER command is assigned to F12, by default.

### Note

This command does not affect the HOLDING or AUTOHOLD condition.

## Clearing the OCS Window

After many messages have appeared in your OCS window, you might want to clear the window before any new messages arrive. To clear your OCS window, enter the CLEAR or K command.

The CLEAR and K commands are described in more detail in the *Management Services Command Reference*.

---

## Receiving Unsolicited Messages in OCS

Events occur within a network or within Management Services itself, which do not result directly from any operator action you have taken, yet need to be reported. The various kinds of messages resulting from these events are termed unsolicited messages.

### Receiving Network Warning Messages

VTAM generates messages for events taking place within the network, called Primary Program Operator (PPO) messages. VTAM can route these messages to the system console (to notify the system operator), and to any suitably authorized programs such as Management Services.

When Management Services receives any PPO messages from VTAM, it filters out messages, by message number, through the DEFMSG table, and passes them to PPOPROC, if active. It then checks to see if any OCS operators logged on have the authority to receive such messages.

By default, a PPO message for a particular resource is sent out to ALL operators authorized to receive it. If a message cannot be delivered to any operator, it is sent to the system console.

A PPO message which does not concern a particular resource and cannot be delivered to an appropriate operator is tagged as undeliverable. These messages are sent to all operators that are profiled to receive undeliverable messages. These messages are prefixed by U when displayed on your terminal. If there are no such operators, it is sent to the system console.

If you are authorized to receive VTAM PPO messages, they appear in your OCS window. All VTAM messages are displayed in high-intensity, and are time-stamped. Your terminal alarm sounds to notify you whenever an unsolicited event has been reported.

In addition, your VTAM message access can be prescribed for receiving only those messages above a given severity level.

## Replying to PPO messages

Some VTAM messages sent to you through the PPO interface require a reply. These messages are delivered to appropriate operators in the same way as standard non-reply PPO messages, as described above.

PPO messages that require a reply are delivered as non-roll delete messages that remain on your screen unchanged, until answered (see the section, *Receiving Non-Roll Delete (NRD) Messages*, on page 4-7, for more information about non-roll delete messages). To reply to these messages, use the REPLY command. Replying to a VTAM message automatically changes the NRD status of the message and places it on the roll delete area list.

For more information about the REPLY command see the *Management Services Command Reference*.

## Intercepting and Processing PPO Messages

The special, system-level, PPOPROC NCL procedure lets you intercept and process PPO messages before they are routed to OCS operators. PPOPROC procedures can be used to analyze VTAM messages and change the normal PPO message delivery rules described above.

For example, a procedure could collect a series of related PPO messages, extract a summary of the information included, and write a single-line warning message to all monitor status operators.

See the *Network Control Language User's Guide* for additional information on how to write PPOPROC procedures.

### Note

Any output messages generated by a PPOPROC procedure are prefixed by P to indicate their origin.

---

## Receiving Non-Roll Delete (NRD) Messages

Most messages displayed on an OCS window are classified as roll delete messages. This means they are displayed once and eventually roll off the top of the screen as subsequent messages arrive and overwrite them.

When an NRD message is delivered to an OCS window, it remains in your OCS window until deleted. There are two categories of NRD messages:

- Those that are remembered by the system and are retained until explicitly deleted by the issuing process
- Those that are only displayed at individual OCS windows until deleted, and are not remembered by the system

The non-roll delete area is separated from the roll delete area by a delimiter line. This line is usually a series of underscore ( \_ ) characters, but you can change the base character using the PROFILE NRDELCH command.

NRD messages are managed centrally and held in a queue. The size of this queue is determined by your systems administrator. If there are more NRD messages than this limit, the oldest outstanding NRD message is deleted to remove copies of the message from all affected OCS windows.

However, NRD messages from &WRITE NCL statements are never deleted automatically. It is therefore only possible to exceed the NRDLIM queue depth if very large numbers of &WRITE-generated NRD messages exist at the same time.

A warning message is sent to all OCS users with monitor status to notify them once the NRD message queue reaches 75% full.

You can hide these messages to allow other message flows to continue in your OCS window, and then reveal them again when you are able to deal with them.

## Hiding NRD Messages

To remove an NRD message from the OCS display, move your cursor to the line on the screen with the NRD message you want to remove, then press ENTER. The NRD message disappears and the screen is reformatted. Removing NRD messages in this way provides more room either for pending NRD messages or a larger roll delete area.

### Note

System NRD messages are not deleted from the NRD message queue, only from your OCS window. NRD messages specific to your OCS window are deleted, and cannot be recalled.

## Restoring Hidden NRD Messages

Hidden NRD messages can be restored by entering the NRDRET command. The oldest hidden NRD messages are returned to the non-roll delete area first, until the area has expanded to its maximum size.

The NRDRET command displays all hidden NRD messages that you are entitled to view, including those that occurred before you entered OCS and any that are still outstanding.

NRDRET can be issued from any environment capable of receiving NRD messages, including NCL &INTCMD environments.

## Deleting NRD Messages

An NRD message is automatically deleted when one of the following conditions is satisfied:

- The condition to which an NRD message refers is satisfied
- An NCL process issues an &NRDDEL NCL statement to delete a specific NRD message
- An NCL process is terminated

You can only delete NRD messages that are remembered by the system by using the PURGE command (see the *Management Services Command Reference* for details on how to use this command).

## Using NRD Messages with ROF Sessions

Messages that originate from a remote system carry the NRD message attribute and appear as NRD messages, in the same way as locally-produced messages.

When an INMC link fails and breaks any ROF sessions travelling across it, all NRD messages from that remote system are automatically deleted.

When you close a ROF session to a particular remote system by using the SIGNOFF command, any NRD messages you have received across the ROF session are deleted from your window. Other users displaying the same NRD messages are not affected.

---

## Using the Activity Log to Help Monitor Your Domains

The activity log records all commands, responses to commands, and messages that occur in your domains. By accessing the activity log when you are in OCS you can browse through recent activity on the system to assist you in locating information and analyzing problems.

To access the activity log browse function from OCS, enter **/LOG** at the ==> prompt.

On initial entry to the activity log, you are positioned at the end of the log for the current day. You can use the F8 (Forward) and F7 (Backward) function keys to scroll through the log for the current day as well as for previous days.

For further information about locating information in the activity log, press F1 (Help) from the activity log panel.

---

## Using the Information Database to Help Monitor Your Domain

The information database provides categories of commonly used information about codes and errors. By accessing the information database from OCS, you can get information about error messages that appear in your OCS window.

To access the information database from OCS, type **NETINFO** at the ==> prompt and press F1. The **NETINFO** panel is presented and you can then choose the required category of information. For more information about the categories provided and how to use the information database, see Chapter 2, *Getting Started*.

---

## Issuing Commands

Being able to issue commands from OCS is an important part of controlling your domains. OCS allows you to issue commands to the background processes of Management Services, and allows you to set commands to issue automatically based on a specified time.

### Issuing Commands in Background Environments

Background environments are internal to Management Services and are designed to process commands submitted to them by users, or to support system level procedures such as LOPROC and PPOPROC. Each background process has a user ID, but is not associated with any physical terminal

There are four background environments:

- BSYS—background system environment
- BMON—background monitor environment
- BSVR—background server environment
- BLOG—background logger environment

You can send commands to these environments for them to execute, as if they were real OCS users by using the SUBMIT command. You can submit either commands or NCL procedures. For example, if you want the background system environment to start the procedure MONPROC, enter the following command:

```
SUBMIT BSYS START MONPROC
```

Once a command is submitted, its processing is managed entirely by that environment. It is not affected if you then log off or leave OCS, but its authority remains the same as the submitter's user ID.

Background environment processing is ideal for monitoring an NCL procedure that regularly checks the status of network components. Commands directed to the Background Monitor route the command and its results to all monitor status terminals logged on to the system, and to the activity log. Commands directed to the Background Logger for execution log the command and its results only.

Timer commands (described below) can also be routed to background environments by either the SUBMIT command, or by using the ROUTE operand for the timer command being issued.

## Issuing Commands at Specified Times

Management Services allows you to issue commands at specified times and at specified intervals. These commands are called timer-initiated commands. There are two timer-initiated commands available:

- AT—execute commands at a specified time of day
- EVERY—repeat commands at a given time frequency

Timer commands can be entered in OCS, or included in NCL procedures.

Timer commands use a 24-hour clock with the format HH.MM.SS. The maximum value for an AT command is 24.00.00 (midnight), and the default minimum frequency for an EVERY command is ten seconds.

For example, if you want to monitor the users that are logged on to the system every half hour, enter the following command:

```
EVERY .30 CMD=SHOW USERS
```

Also, if you wanted to remind users of a 3 o'clock meeting one hour before it commences, enter the following command:

```
AT 14.00 MSG=ALL DON'T FORGET MEETING AT 15.00
```

When a timer command executes, the command text is echoed on all applicable terminals as if the command had been entered from those terminals. The command text echo is prefixed by the unique timer ID for the command, and has the following format:

```
#nnnn command text
```

A maximum of 9999 concurrent timer commands is supported, and this is the default.

If you log off after issuing a timer command, that command is not executed. However, you can specify the ROUTE or KEEP operand when you enter an AT command, to specify another user to issue the command in your place. This allows you to sign off and have the results of the command returned to you when you sign on again. See the section, *Redirecting Timer Commands*, on page 4-13, for more information about using KEEP.

The ROUTE and KEEP options are ideal if you are including timer commands for specific operators in the system initialization procedures that are executed automatically during startup.

Timer commands can also be specified with a limit to the number of times they can execute before being automatically purged.

For more information about the AT and EVERY commands, see the *Management Services Command Reference*.

## Displaying Active Timer Commands

You can display pending timer commands by using the SHOW TIMER command. By default, this command allows you to display any timer commands initiated by your user ID. However, by specifying the ALL operand you can display all outstanding timer commands on your system.

For example, if you want to find out what timer commands you have initiated, enter the following command:

```
SHOW TIMER
```

Using the example given above, the following is displayed:

```
ID BY INTERVAL -USERID-R LIM CNT K/P ENV P/M TID NEXT
 4 EV 00:30:00 USER01      0  0 NO PRI YES - 12:29:48
   CMD=SHOW USERS
 5 AT 14:00:00 USER01      0  0 NO PRI YES - 14:00:00
   MSG=ALL DON'T FORGET MEETING AT 15.00
NUMBER OF TIMER COMMANDS DISPLAYED WAS 2.
```

For more information about the SHOW TIMER command, see the *Management Services Command Reference*.

## Deleting Timer Commands Manually

When you initiate a timer command, the system allocates a unique four-digit number known as the timer ID, or purge ID. This number prefixes all displays resulting from that command, and must be used when manually deleting a timer command.

To delete a timer command manually, use the PURGE command. For example, if you want to delete the AT timer command in the example above, enter the following command:

```
PURGE TIMER=5
```

where 5 is the purge ID assigned to the AT command.

To delete a timer command created by another user, you require a command authority level of 2 or higher.

For more information about the PURGE command, see the *Management Services Command Reference*.

## Deleting Timer Commands Automatically

By default, your timer commands only remain active while you remain logged onto Management Services. Before each attempt to execute the command, the system checks that you are still logged on.

If you are no longer logged on to Management Services the timer command is automatically deleted, without further execution.

## Redirecting Timer Commands

If you want your timer-initiated commands to continue to execute after you log off, you can redirect the command results to the background logger, background monitor, or the system background environment.

To redirect the timer command, you must specify any AT or EVERY commands with the KEEP operand. For example, to redirect the SHOW USERS command to be executed by the background system environment, enter the following command:

```
EVERY .30 KEEP=SYS CMD=SHOW USERS
```

By default, the KEEP operand requires a command authority level of 2 or higher.

If the KEEP operand is in use, and you log back onto the system later, it is then ignored and the execution of timer commands resumes as normal.

For more information about redirecting commands to background processes, see the EVERY and AT command descriptions in the *Management Services Command Reference*.

## Limiting Timer Command Executions

When defining a timer command, you can use the LIMIT operand to specify a limit on the number of times the command is executed. Once this limit is reached, the command is automatically purged. For example, if you want to limit the number of times the SHOW USERS command is executed to 5, enter the following command:

```
EVERY .30 LIMIT=5 CMD=SHOW USERS
```

Once the SHOW USERS command has been executed 5 times, the timer command is deleted.

The limit you assign and the number of times a command has already executed are displayed by the SHOW TIMER command.

## Executing a Timer Command under Another User ID

The ROUTE operand lets you direct a command for execution under another user ID—the target user ID. For example, if you want USER02 to execute the SHOW USERS command, enter the following command:

```
EVERY .30 ROUTE=USER02 CMD=SHOW USERS
```

With this option, the timer command is retained even if the target user ID is not logged on. Command execution is bypassed and the time interval reset. The command is attempted again only after the time interval has again elapsed.

## Specifying Concatenated Commands in Timer Commands

Concatenated commands can be specified in the command text for a timer command. Separate each command in the concatenation with a colon (:). These are internally translated into normal concatenation characters, that is, semicolons (;), before execution.

---

## Executing or Starting NCL Processes from OCS

There is an NCL processing environment for each window of your terminal which allows commands and NCL processes to execute on behalf of that window.

When you use an EXEC or START command to invoke an NCL process, the NCL process executes in the NCL processing environment for the OCS window.

### Note

If you enter the EXEC or START command incorrectly, the system attempts to execute the command as if it were an NCL process.

Any NCL process can have a dependent processing environment which lets it issue commands, or execute other NCL processes independently, using the &INTCMD statement. NCL procedures can also use ROF sessions to collect information from other systems.

The following sections explain how to execute NCL processes from OCS both serially and concurrently. How to execute an NCL process from already executed NCL processes is also explained.

For additional information about NCL processes, see the *Network Control Language User's Guide*.

## Executing NCL Procedures Serially

An OCS window can execute a serial stream of NCL processes so that they are invoked one after the other. Serial execution is suitable for processes with a short duration.

To execute NCL processes serially use the EXEC command. For example, if you want to execute PROC1 and PROC2 in sequence, enter the following commands:

```
EXEC PROC1
EXEC PROC2
```

Your OCS window places the two processes in an EXEC queue, which are executed on a first-come, first-served basis. Process PROC1 is scheduled for immediate execution and process PROC2 is queued to execute once PROC1 ends.

Processes invoked by the EXEC command can issue the &PAUSE statement to wait for further input from the OCS window (see the *Network Control Language Reference* for details about &PAUSE). The GO, END, FLUSH, and INTQ commands, together with the process's unique identifier, let you communicate with the process (see the *Management Services Command Reference* for details about these commands).

## Executing NCL Processes Concurrently

OCS can also execute NCL processes in parallel so that they are executed at the same time.

For example, if you want PROC1 and PROC2 to execute at the same time, enter the following commands:

```
START PROC1
START PROC2
```

Any started procedure can issue an &PAUSE statement (see the *Network Control Language Reference* for details about &PAUSE) to wait for further input from GO, END, and FLUSH commands (see the *Management Services Command Reference* for details about these commands) from the OCS window. These commands, together with the process's unique identifier, let you communicate with the process explicitly.

## NCL Identifiers

Each NCL process is allocated a unique identifier which links it to the issuing OCS window. This ensures any &WRITE or &PANEL statements issued by the NCL process (or any other processes it starts or executes), are returned to that window only. If the window is terminated, any queued process is deleted.

## Executing an NCL Process from a Serial or Concurrent Process

An NCL process executed from an OCS window (or any process it invokes), can itself issue EXEC or START commands for other NCL process.

If an EXEC command is used to execute an NCL process, the process issuing the command is suspended when the new process starts executing. Only when the new process ends does the issuing process resume processing.

Invoking a process from within another process in this way is called nesting. Nesting is an easy way to structure a series of processes.

### Note

The &CALL PROC NCL statement is the recommended method for nesting procedure calls.

If a START command is used to execute an NCL process, the new process starts executing immediately. The new process runs concurrently with the invoking process and independently of it. It is unaffected by the termination of the invoking process, and vice versa.

You can START as many new processes as you require, subject to the maximum number of processes allowed for concurrent execution by a single user (the system default provided is 128).

## The Advantages of Started Procedures

Using the START command to invoke NCL processes has the following advantages:

- You can perform relatively complex, long-term tasks from your OCS window which do not tie up any of the window's resources or prevent other operations from performing concurrently
- You can perform periodic checking of the network status without operator involvement
- You can operate a large number of independent, slave procedures on behalf of one OCS window. This allows you to monitor many different aspects of the same operation, and various procedures need only communicate with you if errors are detected.

---

## Monitoring and Controlling in a Restricted Environment

The Network Partitioning Facility (NPF) is used to limit the range of resources that you receive messages from and can control.

Your user ID can be defined so that commands and messages can be accepted for some network resources, but you are not authorized to issue commands for others.

If you are restricted in your ability to control only particular resources, your user ID is said to be *command partitioned*. If you are restricted to receiving messages from only specific resources, your user ID is said to be *message partitioned*.

The resources available to you are defined within a series of NPF resource tables that reside on the system NPF dataset. The set of resources you can influence is set by your systems administrator and cannot be changed from the OCS window. However, you can list the NPF tables for your user ID or list the resources within each table to see which network resources are available to you (see, *Displaying Network Partition Tables*, below for details on how to do this).

### Displaying Network Partition Tables

Two commands allow you to display the command and message table details that apply to your user ID. They are the SHOW NP and SHOW NPTAB commands.

The SHOW NP command first displays your current NPF environment, including the status of any message tables. Tables that apply to commands only cannot have their status changed and are always classified as ACTIVE. Message tables can have a status of ACTIVE or INACTIVE.

The SHOW NP command returns a list of table names (showing any that are in error) which you then use in the SHOW NPTAB command to display the resources defined within those tables.

#### Note

Resources named within a table can be specified using a generic form containing wildcard characters. The wildcard character, usually an asterisk (\*), lets Management Services accept any character for that position in the name for the item. For example, L5\*8, targets any resource name that is four characters long and starts with the characters L5, and ends with an 8. Any character in the third position is accepted (for example L5B8 or L598).

### Entering Commands in a Restricted Environment

If your user ID has a command table specified, any attempt you make to issue a VTAM command for a resource not defined in this table is rejected. As an option, your organization might let you see any resource within the network, but restrict the issuing of commands.

## Receiving Messages in a Restricted Environment

Where message partitioning has been specified for your user ID, you only receive unsolicited VTAM messages for those resources defined within your message resource tables.

Message tables are allocated an initial status of ACTIVE or INACTIVE when they are defined. An INACTIVE message table is not used when determining whether you should receive messages about a particular resource. This lets operators have overlapping spheres of control and allows for time zones or geographical boundary requirements in a network.

### Changing the Status of Message Tables

You can change the status of your message resource tables so that you can control the sections of the network about which you want to be kept informed.

To change the status of message resource tables, use the NPTAB command. For example, if you want to inactivate the message table ZONE1 and activate the message table ZONE2, enter the following command:

```
NPTAB ACT=ZONE1 INACT=ZONE2
```

Changes to the status of message tables apply immediately to all OCS windows where you are operating, and continue to apply if you exit from OCS. Once you log off, they reset to their previous status for when you log on again.

### Changing the Severity Level of Messages You Receive

NPF allows you to change the severity level of the unsolicited messages you receive, so that you see only SEVERE messages, for example. A severity selection is first set when your user ID is defined and can be changed for the duration of an OCS session, by using the PROFILE PPO command.

As an option, you can be profiled to receive undeliverable messages, which are displayed on your terminal prefixed by U.

## Detecting Errors in Your Restricted OCS Environment

The NPF environment defined for you can contain syntax errors, or errors can occur when the environment is being created during logon.

This situation causes one or more error messages to be displayed identifying the types of error that have occurred, when you enter OCS. You must then determine if these errors significantly affect your use of the system.

## Using a Restricted Monitoring Environment with the Remote Operator Facility (ROF)

If you have used ROF to connect to a remote system, then the authority and privileges assigned to your user ID for the remote system apply as follows:

- Any network partitioning defined for your user ID in the remote system, functions as described in this section.
- To display your NPF environment in the remote system, use the ROUTE command to direct the SHOW NP command to the remote system for execution. The results are returned to your terminal.



---

# Monitoring and Controlling Multiple Applications

This chapter describes how to use the Multiple Application Interface-Operator Console (MAI-OC) facility to monitor and control multiple applications.

**This chapter contains the following topics:**

- About MAI-OC
- Logging On to Another Application
- Logging Off an Application
- Disconnecting an MAI-OC Session
- Interrupting an MAI-OC Session
- Sending Data to an Application
- Receiving Data from an Application
- Issuing Commands to an Application
- Session Protocols

---

## About MAI-OC

MAI-OC allows you to start multiple sessions with VTAM applications using Logical Unit Type-1 (LU.1) protocols. It is available from OCS or from an NCL procedure, and appears to the application as a line-by-line device such as an IBM 3767 terminal.

You can use MAI-OC to provide centralized operation of both the network and of major systems such as CICS, IMS, or JES, where the MAI-OC sessions act as the master consoles of the other application systems.

An MAI-OC session can also be operated from an NCL procedure (using standard internal command environment processing through the &INTCMD facility). The NCL procedure can send data across the MAI-OC session(s) that it is maintaining and receive output from those sessions.

MAI-OC sessions with other applications can be created from any processing environment. Most things that can be done from a native terminal can be done by using an MAI-OC session.

---

## Logging On to Another Application

To log on to another application using MAI-OC, use the MAILOGON command. Logging on creates an MAI-OC session. Sessions can be created with as many applications as you require and multiple sessions can be created with the same application.

For example, to establish a session with a CICS application with the application ID of CICSA, enter the following command:

```
MAILOGON CICSA
```

When the connection is established you receive an initial message from the application informing you that you have been connected.

**Note**

If the session is established with JES, you do not receive a message to confirm connection.

## Creating a Session Identifier

Each session you create is given a unique session identifier. This identifier defaults to the name of the application program with which the session is established, but you can choose any 1- to 8-character name.

For example, to change the session ID of your CICS application from CICSA to CICSPROD, enter the following command:

```
MAILLOGON CICSA ID=CICSPROD
```

The session identifier is used in all MAI-OC commands, so you should make it as meaningful as possible.

If you create multiple sessions with one application from the same window, a unique identifier must be allocated to each session. If the first session's identifier defaults to the application name, you must specify a unique identifier for subsequent sessions with the same application.

The uniqueness of a session identifier only applies to the primary environment. You can open another window at the terminal and create more MAI-OC sessions using identifiers already used in the first window.

For more information about the MAILLOGON command, see the *Management Services Command Reference*.

## Listing Established Sessions

To list all active MAI-OC sessions, enter the SHOW MAI command. This allows you to list all the MAI-OC sessions that have been established and the identifiers used for each.

## Starting an MAI-OC Session with a Specific LU

Before an MAI-OC session can be started with a target application, the system must allocate the LU name that is to be used to act as the *terminal* end of the session.

The LU name may be allowed to default or a particular LU name may be specified on the LU operand of the MAILLOGON command.

### Choosing an LU Name from a Pool

If no specific LU name is provided on the MAILLOGON command, MAI-OC generates one consisting of the MAIOPREF prefix (set by the SYSPARMS MAIOPREF command) followed by a number in the range 001 - 999. The number chosen is the first that is not already in use by another MAI-OC session.

This technique allows the user to establish an MAI-OC session without needing to know the identity of the 'terminal' that MAI-OC will simulate. It also implies that when the session is established, the LU name used by MAI-OC is unpredictable.

When an MAILOGON request without a specified LU name fails because MAI has chosen an unknown LU name, MAI will try up to five successive LU names (each beginning with the MAIOPREF prefix) before indicating that no MAI-OC LUs are available. This is because a defined MAI-OC LU may have been varied and therefore will appear to MAI the same as an LU that has not been defined.

## Choosing a Specific LU Name

If the user requires an MAI-OC session with a target application in which the MAI-OC LU name must be the name of a specific terminal, use of the MAILOGON LU operand allows the user to specify the LU name that MAI-OC is to use.

This technique requires the user to have knowledge of the *terminal* that is to be used on the session, but it also means that the identity of the *terminal* is predictable.

This facility is necessary for establishing an MAI-OC session which has to have particular attributes. For example, an IMS system is generated with its IMS Master Terminal (primary operating console) having the LU name of MTO3767P. The Operator requests the MAI-OC session with a MAILOGON command, specifying LU=MTO3767P on the command text. MAI-OC will open a VTAM ACB whose APPL name is MTO3767P and which must have been defined to VTAM as an APPL (see the section *VTAM APPL Definitions* in the *MAI Installation* chapter in the *SOLVE:Access Planning and Installation Guide*).

---

## Logging Off an Application

Most MAI-OC sessions can be terminated by sending a logoff command of the type expected by the application. For example, for TSO this would be LOGOFF, for IMS it would be /RCL.

However, some applications (such as JES) do not have a logoff command, or you might have trouble sending the command. In these cases, you can use the MAIDISC command to force the disconnection (see, *Disconnecting an MAI-OC Session*, on page 5-5, for details).

If you exit OCS with MAI-OC sessions still intact, Management Services automatically generates MAIDISC commands for all your MAI-OC sessions. This causes lost terminal conditions at the applications for all your MAI-OC sessions. It is not recommended that you use MAIDISC to end TSO sessions as the logoff leaves a reconnect environment pending for a system-defined period.

---

## Disconnecting an MAI-OC Session

If you cannot log off an MAI-OC session normally, you can use the MAIDISC command and specify the session ID that you want to disconnect with. For example, to end the session with the CICS application that was established above, enter the following command:

```
MAIDISC CICS
```

See the *Management Services Command Reference* for more detail about the MAIDISC command.

---

## Interrupting an MAI-OC Session

You can interrupt an MAI-OC session to achieve different effects depending on the application you are connected to. For example, if you have a TSO session established, an interrupt cancels the current operation. If you have an IMS session, it dequeues the current message and request the next one. See the relevant product manual for information about the effect of an interrupt.

To interrupt an MAI-OC session, use the MAIINT command. For example, to interrupt the session established with CICS, enter the following command:

```
MAIINT CICS
```

The MAIINT command can also be specified to generate an attention interrupt to the application by using the TYPE=ATTN operand, and a cancel interrupt by using the TYPE=CNCL operand.

For more information about the MAIINT command, see the *Management Services Command Reference*.

---

## Sending Data to an Application

Once you have logged on to an application, you might want to send data to the application.

To send data to an application, use the MAISEND command. This command nominates the session identifier of the session over which you wish to send the data, followed by the data you wish to send. For example, to send data to the CICS session, enter the following command:

```
MAISEND CICS CEMT I TRAN
```

MAI-OC might append a new line character to the message (to simulate a RETURN key) and the data is sent.

Remember that an MAI-OC session looks like a session with a hard-copy terminal. It does not function on a full screen basis. For example, an attempt to invoke ISPF on a TSO session is rejected.

---

## Receiving Data from an Application

Data received from an application is issued as line messages to the environment that last issued an MAI-OC command against that session. For example, if you issued an MAILOGON command from OCS, then the initial application messages resulting from the session establishment are received by the OCS environment. If the next MAI-OC command for that session is from a dependent environment, for example MAISEND via \$CMDENT, then further messages are returned to the dependent environment.

Application data is displayed unchanged, with the possible addition of some information before the text. This information is the session identifier of the session from which the data was received. For example:

```
(CICS) H2002I TERMINAL CONNECTED
```

The presence of the prefix information and its format is controlled by options specified on the MAILOGON command.

The messages might be in response to a command or NCL system variable that was issued, or they might be unsolicited information, depending on the way the application functions. However, all messages are flagged as unsolicited.

### Note

The PROFILE UNSOL=NO command does not prevent the receipt of messages generated by an MAI-OC session.

---

## Issuing Commands to an Application

When you issue commands to an application using an MAI-OC session, it works in the same way as issuing commands using OCS. However, there are some special considerations for sessions with IMS applications (see, *Issuing Multi-segment Commands to an IMS Application*, on page 5-8, for details).

MAI-OC allows you to simulate a logical keyboard locked condition, as well as abbreviate commands, use function keys, and use NCL procedures to simplify control procedures for the application.

Any commands which can be issued from an OCS window can also be issued from an NCL procedure. Even NCL procedures operating in full-screen mode (for example, invoked through an FSPROC command) can make use of MAI-OC sessions.

### Issuing Commands while Waiting for Application Response

Since MAI-OC simulates a real terminal, it is possible to get a logical keyboard locked condition in which MAI-OC is, for instance, waiting for a response from the application. At this time, the MAISEND command cannot be used to send data to the application and if entered is rejected with an appropriate error message. Normally the command can be retried later. Of course, any other Management Services commands can be entered while you are waiting.

### Abbreviating Commands

NCL procedures and terminal function keys can be used to simplify MAI-OC command requirements, and many MAI-OC commands can be shortened or automated using the EQUATE command.

It is possible that EQUATE commands and NCL procedures have already been set up that you can use. Check with your systems administrator.

See the *Management Services Command Reference* for detailed information on the use of the EQUATE command.

## Issuing Multi-segment Commands to an IMS Application

When sending commands to an IMS application over an MAI-OC session, IMS requires that some input messages be multi-segment. Specifically, a /BRO command must be in two segments. Consider, for example, the following command:

```
/BRO NODE NMMAV003 COFFEE TIME
```

To make this command form two segments, IMS requires a new line character after the node name and before the message.

The MAILLOGON command allows you to specify a character to represent a new line character in data sent via an MAISEND command.

For example, you can create an MAI-OC session using the following command:

```
MAILLOGON IMS NL=+
```

This command defines the new line character as the plus sign (+). You can now send the above broadcast command by entering the following command:

```
MAISEND IMS /BRO NODE NMMAV003+COFFEE TIME
```

The plus sign (+) is replaced by the necessary new line character.

---

## Session Protocols

An MAI-OC session functions as a true SNA LU-type 1, and adheres to the protocols described in the IBM publication *3767 Component Description*.

When MAI-OC has a session with JES2 or JES3, it appears as a 3776-type RJE device. This is still an LU-type 1, and the protocols used are a subset of those described above.

As MAI-OC is simulating a real terminal, it is possible to get a logical *keyboard locked* condition in which MAI-OC might be waiting for a response from the application. You cannot use the MAISEND command to send data to the application during a keyboard locked condition, and if entered is rejected with an appropriate error message.

To determine the sessions states of MAI sessions, use the `SHOW MAI` command. Information given includes whether the *keyboard* is locked or unlocked, the SNA bracket state and the session state generally. Abbreviations used for states in the display are generally those used in the *3767 Component Description*:

<b>INB</b>	In Bracket
<b>BETB</b>	Between Brackets
<b>BBP</b>	Begin Bracket Pending
<b>SEND</b>	Send State (can send to application)
<b>RCV</b>	Receive State (cannot send)
<b>DRWT</b>	Waiting for a definite response (cannot send)
<b>STBY</b>	Standby State (can send)
<b>-</b>	Indeterminate state (state change in progress or not in session)

The CON field in the display can contain:

<b>YES</b>	Session established and available
<b>NO</b>	Session not yet established
<b>LCK</b>	Session established but keyboard locked, because session state is not such that data may be sent

## SCS Character Support

SCS control characters are used by some systems for print layout instructions. They tell an output device (usually a printer) how to respond to tab, spacing, line break and other formatting control sequences.

Not all SCS control characters can be fully simulated at a Management Services terminal. However, none cause a session to be rejected, and wherever possible MAI-OC translates the SCS character to the best equivalent function that OCS mode can provide.

This section details the actions taken by MAI-OC on receiving datastreams containing the following SCS characters:

### **New Line X'15'**

Data following the character will be displayed on a new line of the operator window.

**Form Feed X'0C'**

As New Line.

**Line Feed X'25'**

Stripped from the datastream.

**Vertical Tab X'0B'**

As New Line.

**Record Separator X'1E'**

As New Line.

**Carriage Return X'0D'**

As New Line.

**Vertical Channel Select X'04nn'**

As New Line.

**Horizontal Tab X'05'**

Replaced by a blank.

**Backspace X'16'**

Logically deletes previous character in the line.

**Inhibit Print X'24'**

Stops data sent to the application being echoed to the Management Services panel or the activity log. Data is replaced by asterisks.

**Enable Print X'14'**

Resumes echoing after a previous Inhibit Print.

**Set Horizontal Format X'2BC1'**

Stripped from the data stream (together with all associated counts etc.).

**Set Vertical Format X'2BC2'**

As Set Horizontal Format.

## SCS Characters Sent by MAI-OC

The only SCS character sent by MAI-OC to an application is the New Line (X'15') character. This character is appended to each message sent, and you can embed it in any data you send (see the description of the NL operand of the MAILOGON command in the *Management Services Command Reference* for more information).

## Strike-over Masks

MAI-OC allows you to prevent passwords and other important data from appearing on a terminal or in the activity log by using strike-over masks.

For example, MAI-OC receives the following string of characters from the application:

```
XXXXXXXX<LLLLLLLL<OOOOOOOO<
```

where < is an SCS carriage return (X'0D'). If you send the characters MYPASSWORD to the application, those characters are echoed to the Management Services panel and log as \*\*\*\*\*RD, because the first 8 characters are obscured on a real terminal. Multiple backspace characters instead of carriage return could be used in the mask.

An alternative to the use of strike-over masks is the use of the Inhibit and Enable Print SCS control characters (see *SCS Character Support*, on page 5-9, for details).

## JES MAI-OC Sessions

JES regards an MAI-OC session as a session with an RJE workstation. This means that data sent to JES is regarded as input from a remote console, and so any authorized JES command can be sent, and the results returned to the Management Services window.

JES limits the scope of commands that can be entered from a remote console. You can issued commands to perform any JES display-type function provided you have the correct authorization within JES and use the appropriate operands. However, commands can only change the status of jobs, and so on, owned by the workstation. The OPSYS OCS command can also be used to enter commands if required.

You can use JES commands to shorten responses to commands (for example to remove the leading time stamps). Their use should be considered to make the display as neat as possible.

When using JES2 or JES3, there is no indication that an MAI-OC session request has completed. Use the SHOW MAI command to determine when the session is established.

To terminate a JES MAI-OC sessions, use the MAIDISC command.



# 6

---

## Monitoring and Controlling Remote Domains

This chapter describes how to use the Remote Operator Facility (ROF).

**This chapter contains the following topics:**

- About the Remote Operator Facility (ROF)
- Signing on to a Remote Domain
- Issuing Commands on a Remote Domain
- Receiving ROF Messages
- Signing Off a Remote Domain

---

## About the Remote Operator Facility (ROF)

ROF lets you log on to one MS domain and act as a remote operator for one or more other domains that are connected by the Inter-Management Services Connection (INMC) component.

You must have your user ID defined to any remote domains that you want to log on to. Your privileges there, your command authority level, and NPF restrictions depend upon your user ID definition in the remote domain. For example, it might be that you have level 3 authority in one domain, but might only be able to execute level 1 commands in a remote domain.

### Getting Maximum Benefit from ROF

The following list can help you gain maximum benefit from ROF:

- Ensure you have a user ID defined for each remote domain where you might want to have an ROF session. Make sure those user IDs have the appropriate authority levels and NPF requirements.
- For those domains where you often have ROF sessions, include SIGNON commands within an NCL procedure which is executed automatically on entry to OCS.
- Use EQUATE command values to abbreviate long, frequently-used command strings to a single character, or to a shorter string.

### Using ROF in OCS

Using ROF in OCS allows you to sign on to remote domains, issue commands on that remote domain, and receive the results of those commands at your own terminal.

Include SIGNON commands in each remote domain from which you want to be able to monitor unsolicited messages from other remote domains. You must also include SIGNON commands for each remote domain in any NCL procedures that are executed automatically when you access OCS.

**Note**

The NCL procedure that is executed automatically on entry to OCS is initially set in your user ID definition.

---

## Signing on to a Remote Domain

To sign on to a remote domain, use the `SIGNON` command. For example, if you want to sign on to the remote domain `PROD01`, enter the following command:

```
SIGNON PROD01
```

The remote domain checks to see if you are authorized and then notifies you of the connection.

Once the connection is established, you receive any unsolicited messages from that domain. See the section, *Receiving ROF Messages*, on page 6-5, for more information.

## Signing on to a Remote Domain over an Inactive Link

If there is no active INMC link to the remote domain you want to sign on to, you can issue a `SIGNON` command to wait in a queue for the INMC link to become active.

For example, if you want to sign on to `PROD01` but the INMC link to it is not active, enter the following command:

```
SIGNON PROD01
```

This places your signon in a queue and waits until the INMC link to the remote domain becomes active. Once the link becomes active, the ROF session is established and you are notified of this by the system.

All ROF sessions and queued signons are cancelled when you exit OCS.

## Restarting a ROF Session

If an INMC link to a remote domain fails while you are connected, your ROF sessions to that domain are terminated and queued for reestablishment when the link becomes active again. You are notified when the ROF session is re-established.

If you exit OCS before the link becomes active, the queued `SIGNON` is cancelled.

---

## Issuing Commands on a Remote Domain

To issue a command on the remote domain, use the ROUTE command. For example, to send a SHOW USERS command to PROD01, enter the following command:

```
ROUTE PROD01 SHOW USERS
```

The SHOW USERS command executes in PROD01 as if it had been entered from a local terminal, and the result of the command is returned to your OCS window.

### Note

If you route a command to a remote domain that you are not signed on to, a signon to that remote domain is automatically initiated.

## Using Command Separators

The ROUTE command allows support for a single embedded colon (:) character as a command separator. When the ROUTE command processor encounters a single colon in the command string, it substitutes a semicolon. If the processor encounters two colons, it eliminates the first and sends the second to the target domain as part of the transmitted command.

## Simplifying Remote Command Execution

Sending commands to remote domains for execution can be simplified by using EQUATE command strings. See the *Management Services Command Reference* for more information on the EQUATE command.

## Issuing Commands from a Remote Domain

You can issue a command on another remote domain through your current ROF session. This lets you establish ROF sessions to remote domains through any number of intermediate domains. For example, to send a SHOW USERS command to PROD02 through PROD01, enter the following command:

```
ROUTE PROD01 ROUTE PROD02 SHOW USERS
```

This command sends the SHOW USERS command to PROD02 via an intermediate ROF session with PROD01. This provides an alternative to a direct ROF session, and can be useful if direct contact cannot be established with the target domain.

---

## Receiving ROF Messages

Whenever you receive messages from remote domains, whether as unsolicited information or in response to a command, each message is color coded and prefixed with a message ID.

### Using Color Coded Messages

The messages from remote domains can have different colors depending on which remote domain they originate from. This helps you to identify the source of a message if you are connected to multiple remote domains.

The `SIGNON` command lets you override the default color/highlight attributes which were specified when the INMC link to the remote domain was established. For example, to specify the color red for any messages received from `PROD01`, enter the following command:

```
SIGNON PROD01 COLOR=RED
```

### Using the Message ID

By default, ROF messages returned from a remote domain across an ROF session are prefixed with a 1- to 4-character identifier of the remote domain specified when the INMC link was established.

The `SIGNON` command lets you override the ROF message ID prefix default. This prefix can be any 1- to 8-character string. For example, to specify the message ID for any messages received from `PROD01` as `TEST`, enter the following command when you sign on:

```
SIGNON PROD01 ID=TEST
```

Your prefix, and not the default `PROD01`, appears as the first word of each ROF message from the remote domain.

Such prefixes are private to you and can be varied for each of your OCS windows, or be different for each `SIGNON` command issued by NCL processes executing in your NCL processing region.

---

## Signing Off a Remote Domain

To sign off a remote domain, use the `SIGNOFF` command. For example, to sign off `PROD01`, enter the following command:

```
SIGNOFF PROD01
```

This command is used for explicit signoff; however, if you exit OCS, all ROF sessions are terminated automatically.

---

## Sending Broadcasts

This chapter describes how to use broadcast services to send messages to users of your domains.

**This chapter contains the following topics:**

- About Broadcast Services
- Accessing Broadcast Services
- Listing Broadcasts
- Listing System Groups
- Broadcasting to Generic Resources
- Setting General Broadcasts
- Setting Primary Menu Broadcasts
- Reviewing Active Broadcasts
- Sending Dynamic Broadcasts
- Receiving Broadcasts

---

## About Broadcast Services

Broadcast Services allows you to utilize the various broadcasting capabilities of Management Services. Broadcast messages can be sent to terminals, users, and applications, and can be stored on a file.

Broadcast services allows you to send the following types of broadcast:

- A general broadcast of one to four lines
- A primary menu broadcast of one line
- A broadcast of up to four lines to all, or specific, EASINET terminals
- A broadcast of up to four lines to all, or specific, Management Services attached terminals (including EASINET terminals)
- A broadcast of up to four hundred lines to all, or specific, users
- A broadcast of up to four hundred lines to a selected list of users
- A broadcast of up to four lines to MAI users of an application (for example CICS or IMS)
- A broadcast of up to four lines to users of an NCL application
- A broadcast to a specific user ID according to their preferred method of notification (as indicated in their UAMS security profile)

### Types of Broadcasts

The broadcasts listed above can be grouped into the following types:

- General
- Primary Menu
- User

These broadcasts are either static or dynamic.

---

## Accessing Broadcast Services

To access broadcast services, complete the following steps:

- Step 1. Enter **/BCAST** at a **====>** prompt. The Broadcast Services : Primary Menu is displayed.

**Note**

Broadcast capabilities are also provided by the \$BSCALL NCL interface. This interface and how to use it are described in the *Network Control Language Reference* manual.

Figure 7-1. Broadcast Services : Primary Menu

```
PROD----- Broadcast Services : Primary Menu -----/BCAST
Select Option ==>

  L - List Active Broadcasts                Userid USER01
  LS - List System Groups                   LU    TERM01
  G - Set and Store General Broadcast       Time  14.59.44
  P - Set and Store Primary Menu Broadcast  THU 05-JUL-2001
  R - Review Broadcasts for USER01 at NMMAF063
  S - Send a Broadcast
  X - Exit

F1=Help      F2=Split      F3=Exit      F4=Return
              F9=Swap
```

For details of the options available on this menu, press F1 (Help).

## Listing Broadcasts

To display a list of all active broadcasts in the system, enter **L** at the `====>` prompt on the Broadcast Services : Primary Menu (/BCAST). The Broadcast Services : List Broadcasts panel is displayed.

Figure 7-2. Broadcast Services : List Broadcasts Panel

```
PROD----- Broadcast Services : List Broadcasts -----
Command ===>                                         Scroll ===> PAGE

                S=Browse D=Delete FD=Force Delete
Date          Time Userid  ID      Retain Type      Mask      Viewed RCVO#
05-JUL-2001  14.05 ACSDBMON 00000001 VIEWED USERID    IN0069    0      1
05-JUL-2001  20.31 ACSDBMON 00000003 VIEWED USERID    IN0069    0      1
05-JUL-2001  01.11 ACSDBMON 00000008 VIEWED USERID    NMTBY     0      1
05-JUL-2001  01.11 ACSDBMON 00000012 VIEWED USERID    IN0069    0      1
**END**

F1=Help      F2=Split    F3=Exit     F4=Return   F5=Find     F6=Refresh
F7=Backward  F8=Forward  F9=Swap
```

The broadcasts in the selection list are either permanent or still to be viewed. A permanent broadcast is displayed until deleted by a user. Other broadcasts are displayed until they have been viewed by all target recipients.

For details of the information displayed about each listed broadcast, press **F1** (Help).

## Viewing Active Broadcasts

To view the contents of an outstanding broadcast, enter **S** (Browse) next to the required broadcast in the selection list.

## Deleting Active Broadcasts

To delete a broadcast that is no longer required, enter **D** (Delete) next to the required broadcast in the selection list. If you want to delete a broadcast before all target recipients have received the broadcast, enter **FD** (Force Delete) next to the required broadcast in the selection list.

---

## Listing System Groups

The group list panel displays a selection list of broadcast system groups. Broadcast groups are useful when you need to send broadcasts to multiple remote domains.

Groups can be:

- Added
- Browsed
- Copied
- Deleted
- Updated
- Resource listed

## Adding a Broadcast System Group

To add a new system group definition, complete the following steps:

- Step 1. Enter **LS** at the **===>** prompt on the Broadcast Services : Primary Menu. The Broadcast Services : Group List panel is displayed.
- Step 2. Press **F4** from the Broadcast Services : List Groups panel. The Broadcast Services : Group Definition panel is displayed.

*Figure 7-3. Broadcast Services : Group Definition*

```
PROD----- Broadcast Services : Group Definition -----
Command ===>                                         Function=ADD

Group Name ..... _____
Description ..... _____
Include Local System? ... ___ (Yes or No)

F1=Help      F2=Split      F3=File      F4=Save      F5=Resources
              F9=Swap

F12=Cancel
```

- Step 3. Enter the name of the new system group in the Group Name field.
- Step 4. Enter a description of the system group in the Description field.

- Step 5. To include the local system in this system group, enter **YES** in the Include Local System? field; otherwise enter **NO**.
- Step 6. Press F4 to save the group definition.
- Step 7. Press F5 to access the Broadcast Services : Resource List.

The resource list panel allows you to copy, browse, delete, and update resource definitions once they are part of a system group definition. The following steps describe how to add a new resource definition to your system group.

*Figure 7-4. Broadcast Services : Resource List*

```

PROD----- Broadcast Services : Resource List -----
Command ==>                                     Scroll ==> PAGE

                                         C=Copy S=Browse D=Delete U=Update

Type      Name
DOMAIN    SOLVPROD
**END**

F1=Help    F2=Split    F3=Exit    F4=Add    F5=Find    F6=Refresh
F7=Backward F8=Forward  F9=Swap

```

- Step 8. Press F4 (Add) to add the required remote systems. The Broadcast Services : Resource Definition panel is displayed.

Figure 7-5. Broadcast Services : Resource Definition

```

PROD----- Broadcast Services : Resource Definition -----GROUP1
Command ==>                                         Function=ADD

Resource Type ..... _____ (APPCLINK, DOMAIN, LU)
Resource Name ..... _____

F1=Help      F2=Split      F3=File      F4=Save
              F9=Swap

F12=Cancel
    
```

Step 9. Enter the type of resource in the Resource Type field. The following types of resource are supported:

- |          |  |
|----------|--|
| APPCLINK | A predefined APPC Link name between two systems of up to 12 characters.            |
| DOMAIN   | A system attached via INMC. The name can be up to 4 characters.                    |
| LU       | A network resource name of up to 8 characters that identifies the required system. |

**Note**

When adding Domain or LU type resources, ensure that the requisite DEFLINK commands have been issued to allow the system to connect using APPC. See the *Management Services Administrator Guide* for more information on defining APPC links.

Step 10. Enter the name of the resource in the Resource Name field. This name is used on the Broadcast Services : Send Menu when sending a broadcast to the system group.

Step 11. Press F3 (File) to save the changes and exit to the Resource List panel. The resources you added will be listed. Multiple resources can be added by entering details for each resource and pressing F4 (Save).

---

## Broadcasting to Generic Resources

This section describes how to use the Broadcast Services facilities of Management Services to enable broadcasts to domains belonging to a VTAM generic resource.

These facilities are available from the Broadcast Services : Primary Menu (/BCAST).

### Enabling Broadcasts to Generic Resources

To enable broadcasts to domains belonging to a VTAM generic resource, there must be a broadcast system group corresponding to that generic resource.

To add a broadcast system group corresponding to a generic resource, complete the following steps:

- Step 1. Enter **LS** at the `====>` prompt on the Broadcast Services : Primary Menu (/BCAST). The Broadcast Services : Group List panel is displayed.
- Step 2. Press **F4 (Add)**. The Broadcast Services : Group Definition panel is displayed.

*Figure 7-6. Broadcast Services : Group Definition Panel*

```
PROD----- Broadcast Services : Group Definition -----
Command ===>                                         Function=ADD

Group Name ..... _____
Description ..... _____
Include Local System? ... ___ (Yes or No)
```

- Step 3. In the Group Name field and the Description field, enter the name and a brief description of the new broadcast group.
- Step 4. In the Include Local System? field, specify (by entering **YES** or **NO**) whether the local system is to be included in the broadcast group.  
  
YES indicates that broadcasts can be issued on this system. NO indicates that broadcasts can be issued on remote systems only.
- Step 5. Press **F4 (Save)** to save the group definition—a message is returned, confirming that the new broadcast group has been added.

## Adding Resources to a Broadcast System Group

To add resources to a broadcast system group corresponding to a generic resource, complete the following steps:

- Step 1. From the Broadcast Services : Group Definition panel, press F5 (Resources). The Broadcast Services : Resource List panel is displayed.

The resource list panel allows you to copy, browse, delete, and update resource definitions once they are part of a system group definition. The following steps describe how to add a new resource definition to your broadcast system group.

- Step 2. Press F4 (Add). The Broadcast Services : Resource Definition panel is displayed.

Figure 7-7. Broadcast Services : Resource Definition Panel

```
PROD----- Broadcast Services : Resource Definition -----
Command ==>                                         Function=ADD

Resource Type ..... _____ (APPCLINK, DOMAIN, LU)
Resource Name ..... _____
```

- Step 3. In the Resource Type field, enter the type of resource to be added. The following types of resource are supported:

APPCLINK	A predefined name (with up to 12 characters) of an APPC link between two domains
DOMAIN	A domain (with a name of up to four characters) attached by INMC
LU	A network resource name (up to eight characters) that identifies the required domain

### Note

When adding DOMAIN or LU resources, ensure that the necessary DEFLINK commands have been issued to allow the domain to connect by using APPC. See the *Management Services Administrator Guide* for more information about defining APPC links.

- Step 4. In the Resource Name field, enter the name of the resource to be added. This name is used on the Broadcast Services : Send Menu when sending a broadcast to the system group.

Step 5. Press F3 (File) to save your changes. The Broadcast Services : Resource List panel is redisplayed, with the new resource added.

Step 6. Repeat Steps 1 to 5 for each resource that you want to add to the broadcast group.

## Sending Broadcasts to Generic Resources

Once you have defined a broadcast system group for your generic resource, you can use that system group to send broadcasts to domains belonging to the generic resource. To do this, complete the following steps:

Step 1. Enter **S** at the `====>` prompt on the Broadcast Services : Primary Menu (/BCAST). The Broadcast Services : Send Menu is displayed.

Figure 7-8. Broadcast Services : Send Menu

```
PROD----- Broadcast Services : Send Menu -----$BS020
Select Option ==>

  A - Broadcast to All EASINET Terminals and SOLVE Users
  AP - Broadcast to MAI users of an Application
  E - Broadcast to All EASINET Terminals
  NCL - Broadcast to Users of an NCL Application
  TA - Broadcast to Specific Terminals - EASINET & SOLVE
  TE - Broadcast to Specific Terminals - EASINET Only
  U - Broadcast to Specific SOLVE Users
  N - Send a User Notification
  X - Exit

Send Options
Retain Broadcast? ..... _____ ( Required A AP NCL TA U PERM VIEWED or NO )
Destination Mask .....+ _____ ( Required AP NCL TA TE U N )
Immediate Broadcast? .. _____ ( Required A AP NCL TA TE U YES or NO )
System Group .....+ _____

F1=Help      F2=Split      F3=Exit      F4=Return
              F9=Swap
```

Step 2. Enter the system group name for your generic resource in the System Group field.

Step 3. Enter the mnemonic of the type of broadcast that you want to send.

---

## Setting General Broadcasts

A general broadcast allows you to notify potential users of the system about critical events. For example, the impending unavailability of a major application such as production CICS or IMS subsystems.

A general broadcast can be up to four lines and can be sent to all EASINET terminals or all Management Services terminals, including EASINET terminals. The lines of broadcast appear at the bottom of the terminal display and are available across system restarts.

To set a general broadcast, enter **G** at the ===> prompt on the Broadcast Services : Primary Menu. The Broadcast Services : Edit Broadcast Text panel is displayed.

*Figure 7-9. Broadcast Services : Edit Broadcast Text Panel*

```
PROD----- Broadcast Services : Edit Broadcast Text -----Columns 001 074
Command ===>                                     Function=Set Scroll ===> PAGE
N30006 SAVED BROADCAST TEXT WAS RESET BY USER01 AT 10.55.46 05-JUL-2001

LINE<-----10-----20-----30-----40-----50-----60-----+
*** ***** TOP OF DATA *****
0001
0002
0003
0004
*** ***** BOTTOM OF DATA *****

F1=Help      F2=Split    F3=File      F5=Find      F6=Change
F7=Backward  F8=Forward  F9=Swap     F10=Left    F11=Right   F12=Cancel
```

On entry to this panel, the lines in the editor display the text from the last general broadcast that was issued. Details of the user who issued the last broadcast are also displayed.

If you do not wish to change the broadcast text, you can press F12 (Cancel) to cancel any updates.

Enter the text you want to send as a general broadcast in the text lines provided and press F3 (File) to save the broadcast. F3 sets the broadcast so that it can be displayed and saves the broadcast in the Management Services VFS file so it is available across system restarts.

When you send a general broadcast, the NCL variables &BROLINE1 to 4 are updated, and any panel containing these variables displays the text you have entered the next time those panels are accessed by a user.

To clear a general broadcast, delete any text in the text lines and press F3 (File) to perform the update.

---

## Setting Primary Menu Broadcasts

The primary menu broadcast allows you to set one line of text to be displayed on the primary menu. This type of broadcast is useful for reminding users of something about the system they have logged on to. For example, you might want to remind users that the system is a test system and they should not change anything.

To set a primary menu broadcast, enter **P** at the ===> prompt on the Broadcast Services : Primary Menu (/BCAST). The Broadcast Services : Edit Broadcast Text panel is displayed. This looks similar to the edit panel for a general broadcast except there is only one text line available for input.

When you first access this panel, details are given of when the text was last updated, and by which user ID.

Enter the text you want displayed on the primary menu in the text line, and press F3 (File) to save the broadcast. When you enter text in this line, the NCL variable &ZPMTEXT1 is updated which is contained on the primary menu panel. When you press F3, the primary menu is updated and the broadcast is displayed when a user next accesses that menu. F3 also saves the broadcast so that it is redisplayed across system restarts.

To clear a primary menu broadcast, delete any text in the line, and press F3 (File) to perform the update.

---

## Reviewing Active Broadcasts

To review active dynamic broadcasts that are applicable to your terminal and user ID, enter **R** at the `====>` prompt on the Broadcast Services : Primary Menu (/BCAST). The Broadcast Services : Review Broadcasts panel is displayed. An example of this panel is shown in Figure 7-10.

*Figure 7-10. Broadcast Services : Review Broadcasts Panel*

```
PROD----- Broadcast Services : Review Broadcasts -----Columns 001 079
Command ====> --Scroll ====> PAGE

***** TOP OF DATA *****
----- RETAINED -----

      User broadcast issued by USER01 at 10.47.55 on THU 05-JUL-2001 :
      Application CICSPROD will be unavailable for 10 mins.

-----
***** BOTTOM OF DATA *****

F1=Help      F2=Split      F3=Exit      F5=Find
F7=Backward  F8=Forward    F9=Swap
```

This panel displays all the broadcasts for your user ID and terminal in the same way you receive a broadcast when you sign on. To view subsequent broadcasts, press F8 (Forward).

The dashed line above each broadcast on the review panel, includes a message which indicates whether the broadcast is deleted or whether it has been retained by the review function. Retained broadcasts can only be deleted from the List Broadcasts panel.

---

## Sending Dynamic Broadcasts

A dynamic broadcast allows you to send a message to a specific user, or to a range of users.

When a broadcast is sent, a panel is displayed containing the broadcast lines and details of the broadcast initiation.

To send a dynamic broadcast, enter **S** at the ==> prompt on the Broadcast Services : Primary Menu (/BCAST). The Broadcast Services : Send Menu is displayed.

Figure 7-11. Broadcast Services : Send Menu

```
PROD----- Broadcast Services : Send Menu -----$BS020
Select Option ==>

  A - Broadcast to All EASINET Terminals and SOLVE Users
  AP - Broadcast to MAI users of an Application
  E - Broadcast to All EASINET Terminals
  NCL - Broadcast to Users of an NCL Application
  TA - Broadcast to Specific Terminals - EASINET & SOLVE
  TE - Broadcast to Specific Terminals - EASINET Only
  U - Broadcast to Specific SOLVE Users
  N - Send a User Notification
  X - Exit

Send Options
Retain Broadcast? ..... VIEWED ( Required A AP NCL TA U PERM VIEWED or NO )
Destination Mask .....+ _____ ( Required AP NCL TA TE U N )
Immediate Broadcast? .. NO ( Required A AP NCL TA TE U YES or NO )

F1=Help      F2=Split      F3=Exit      F4=Return
              F9=Swap
```

For details of the fields and options available on the prompt on the Broadcast Services : Send Menu, press F1 (Help).

## Entering Broadcast Text

When you have selected the type of broadcast you want to send, and you have set the appropriate fields on the Send Menu, press ENTER to invoke the Broadcast Services : Edit Broadcast Text panel. If you select option U, you can specify a maximum of 400 lines of broadcast text. If you select any of the other options, you can specify a maximum of four lines of broadcast text.

### Note

If you specified option U and prompting in the Destination Mask field, you are presented with a list of user IDs. You must select the users you want to send the broadcast to and then press ENTER to invoke the Broadcast Services : Edit Broadcast Text panel.

When you have entered the broadcast text, press F3 (File) to initiate the broadcast. An acknowledgment message is displayed when processing is complete. This message shows the total number of terminals and users that have received the broadcast at that point in time.

**Note**

If you send a broadcast to a user who is logged on more than once, the acknowledgment message includes each of their logons in the total number of user IDs that have received the broadcast. However, once the user has viewed the broadcast, the broadcast is discarded for their duplicate logons.

After a broadcast is sent, it is retained until you exit broadcast services. If you want to send another broadcast, the previous broadcast is displayed on the editor if you have not left broadcast services. This allows you to send the same broadcast again, or edit it to send to another user, or group of users.

---

## Receiving Broadcasts

When you receive a broadcast that has more lines than the screen has available, you can use the F8 (Forward) and F7 (Backward) keys to scroll through the broadcast. Figure 7-12 is an example.

*Figure 7-12. A Broadcast Exceeding One Screen*

```

PROD----- Broadcast Services : Broadcast Display -----
Command ==>

      User broadcast issued by USER01 at 17.20.30 on THU 05-JUL-2001 :

===== Broadcast Text =====

Harry,

Here are the statistics you wanted from NCPView:

      Name                Current Maximum Current Maximum      Free   Free
      Use                 Used      Use      Used      Total Unrsvd  Rsvd
BSB-D-LU-LU              98%      100%   1338   1353   1353    15    0
BSB-D-SSCP-LU           98%      100%   1338   1353   1353    15    0
LND/LNB                  98%      100%   1338   1353   1353    15    0
NSC                      100%     100%   2181   2181   2181     0    0
NSX                      100%     100%   1210   1210   1210     0    0
NNT                      66%       73%     20     22     30    10    0
CBB                      61%       61%     52     52     84    32    0
CXB                      61%       61%     52     52     84    32    0
===== Press F8 to View Remaining Lines =====
F1=Help                F3=Exit
F7=Backward  F8=Forward

```

To acknowledge receipt of the broadcast, you must press F3 (Exit). However, once you have pressed F3, you no longer have access to the broadcast. If the broadcast is more than one screen, you can press F3 before you have read the whole broadcast.



---

# Communicating Between Management Services Domains

This chapter describes how to use INMC and APPC to communicate between your domains.

**This chapter contains the following topics:**

- About Communicating Between Management Services Domains
- Using INMC to Link Management Services Domains
- Troubleshooting for INMC Links
- Using APPC to Link Management Services Domains

---

## About Communicating Between Management Services Domains

Management Services provides you with two methods to communicate between domains:

- INMC—Inter Management Services Connection
- APPC—Advanced Program-to-Program Communication

If two or more domains are connected, you need to be aware of which domains are connected and ensure the links are active when required. To perform this function use the `SHOW LINKS` command to monitor the status of links between domains and ensure that the appropriate VTAM cross-domain managers and resources are active.

For information on defining domains see the *Management Services Administrator Guide*.

### Using INMC to Communicate Between Management Services Domains

Domains running in a network containing multiple CPUs can communicate with each other, providing general-purpose data transfer between CPUs within the network. This facility is called the Inter-Management Services Connection (INMC). This transport facility can be accessed by other system components (for example ROF) so that you can log on to one domain and route commands for execution in other domains in the network.

### Using APPC to Communicate Between Management Services Domains

APPC is an IBM protocol for communication between programs. APPC allows a program to communicate with another program via a conversation. Management Services provides APPC functionality for communication between domains using LU6.2 (Logical Unit Type 6.2) sessions as a communication path.

APPC allows you to establish parallel and single session links, and provides a range of LU6.2 options for these links.

---

## Using INMC to Link Management Services Domains

You can run INMC connections between your current domain to one or more remote domains, elsewhere in the network.

When linking domains using INMC, each domain must have a unique link name by which it can be identified. The link name used for each domain should be the same in every INMC link definition so that they can be identified by other operators.

Domains connected using INMC can exchange information about each other and about the environment in which they are operating. For example, the domain ID.

### Starting an INMC Connection

To enable a static INMC connection, use the LINK command. For example, if you want to start an INMC link between SOLVE01 and SOLVE02, enter the following command from SOLVE01:

```
LINK TYPE=INMC START=SOLVE02
```

SOLVE01 will attempt to open communications with SOLVE02; however, SOLVE02 does not know that SOLVE01 wants to communicate. To complete the connection, enter the following command in SOLVE02:

```
LINK TYPE=INMC START=SOLVE01
```

Communication between the two domains is now established and you can now receive messages from SOLVE01 in SOLVE02 and vice versa.

**Note**

LINK commands can be included in system startup procedures so that links are activated upon initialization.

This command also allows you to specify the following:

- The name of the VTAM APPL definition used by the remote domain
- The message prefix for messages received in the local domain from the remote domain
- The color and highlight for the messages displayed
- The interval at which contact will be retried if the connection has failed

For more information about using this command, see the *Management Services Command Reference*.

## Stopping INMC Links

To inactivate an INMC link, use the `LINK STOP` command, specifying the link name required. All sessions with the specified link name are immediately terminated and the status of the link is changed to `STOPPED`. If any traffic or activity is in progress at the time of the `LINK STOP` command, it too is terminated.

The status of the link in the remote domain after a `LINK STOP` command is changed to `PEND-ACT`.

## Resetting an INMC Link

To reset an INMC link, use the following command:

```
LINK RESET=linkname
```

This command, which is valid only if the link is already stopped, removes the current link definition information from storage. A subsequent `LINK START` command is required to redefine the link.

## Displaying INMC Link Status

To display the status for all links to remote domains, enter the `SHOW LINK` command.

The resulting display shows each defined remote domain, with the following information:

- Its link name
- The VTAM node name it uses
- The 1- to 4-character string (`MSGID`) used to prefix messages received from the remote domain
- The current status of the link
- The status of individual sessions maintained by the local system

The link status can be one of the following values:

### **STARTING**

Indicates that the remote domain is in the process of being connected.

### **ACTIVE**

Indicates that the remote domain is successfully connected.

**STOPPED**

Indicates that the link to the remote domain is closed and cannot be opened until a LINK START command is issued. (This status arises from an earlier LINK STOP command.)

**PEND-ACT**

Indicates a connection has either never been successfully opened, or has been lost and not yet reestablished. The system tries to reopen the link every 60 seconds (or at a frequency specified by the RT operand of the LINK command) and does this indefinitely. This status might indicate the following:

- VTAM cannot presently provide a path between the two domains
- The remote domain is not running
- The remote domain is rejecting the local domain's connection requests because of a definition error, or because its link has been stopped

**FAILED**

Indicates that the connection has failed and cannot be automatically re-established. This is an unusual situation and should be referred to your systems administrator. When the cause is corrected, issue a LINK START command to reestablish the connection.

## Displaying Domain Information

When an INMC link is established, the local and remote domains exchange domain information. To display the domain information for your domain and all other domains connected to it using INMC, whether the links are active or not, use the SHOW DOMAINS command.

The first entry in the list is always your local domain, from where commands are issued. The following domain information is displayed:

- Domain Name
- Link name
- Link MSGID
- Remote network name
- Remote VTAM version, release and level data
- Remote domain version and release level
- Remote operating system type
- Current status of the domain information

For more information about using this command, see the *Management Services Command Reference*.

---

## Troubleshooting for INMC Links

For any given pair of domains with defined links, establishing a connection should be automatic once there is a path to each domain through the network.

If a link cannot be activated, check the following:

- Has each domain been defined to the other? If not, see your systems administrator.
- Does a SHOW LINK display in either domain have a link status of PEND-ACT? If so, check that both domains are active, and check the status of the appropriate VTAM cross-domain resource managers and resources.
- Does a SHOW LINK display in one domain indicate a link status of ACTIVE, but show as STOPPED or PEND-ACT in the other domain? If so, this is a system error and you should see your systems administrator. The link definitions for both domains should be stopped, reset, and redefined.
- Does a SHOW LINK display give the status in one domain as PEND-ACT, and as STOPPED in the other domain? If so, issue a LINK START=*linkname* for the INACTIVE definition.
- If both domains indicate a status of PEND-ACT for the link while there appears to be a network path open between the domains, see your systems administrator.
- Does a SHOW LINK command in either domain have a link status of FAILED? If so, check backwards through the activity log for error messages recorded at the time of the failure. Refer these to your systems administrator. The link can be restarted using a LINK START command.
- If a SHOW LINK command shows any session with a status of DISABLED (that is, Management Services makes no further attempt to open this session), use the link monitoring facilities available from the System Support Services component to show why the session has been disabled.

---

## Using APPC to Link Management Services Domains

APPC allows you to establish links between domains as well as between a domain and other applications. APPC links are defined during setup by your system administrator and can be established, monitored, and stopped by you.

### Starting APPC Links

To start an APPC link, use the LINK command and specify the type of link, along with the link name of the domain or application you are connecting with. For example, to establish an APPC link with NMA from SOLVE01, enter the following command:

```
LINK TYPE=APPC START=NMA
```

Sometimes you might have to supply a password before an APPC session is established. This is set up in the APPC link definition by your system administrator.

For more information on establishing an APPC link, see the LINK command in the *Management Services Command Reference*.

### Displaying APPC Link Status

The SHOW LINK command is used to display APPC link status, however, the type of link must be specified or only INMC links are displayed. For example, to find out the status of all APPC links in your domain, enter the following command:

```
SHOW LINK TYPE=APPC
```

The following information about APPC links is displayed:

- Link Name
- Remote LU Name
- Link status (see the section, *Displaying INMC Link Status*, on page 8-4, for a list of possible statuses for APPC links)
- Link type (parallel or single session)
- LU6.2 options supported (for example, mapping)
- Link and conversation level security supported
- The session limit for the link

For more information about displaying the status of APPC links, see the SHOW LINK command in the *Management Services Command Reference*.

## Stopping APPC Links

An APPC link can be stopped in the same way as an INMC link; however, the type of link must be specified. For example, to stop the APPC link between SOLVE01 and NMA, enter the following command:

```
LINK TYPE=APPC STOP=NMA
```

---

# Printing

This chapter describes how to use Print Services Manager (PSM) when printing from your system.

**This chapter contains the following topics:**

- About Print Services Manager
- Accessing PSM
- Listing Entries in the Print Queue
- Confirming Printing

For information on customizing and administering PSM, see the *Management Services Administrator Guide*.

---

## About Print Services Manager

PSM enables you to control the physical printing of the reports your organization generates on JES or network printers. Output can be viewed on-line before or after printing and can be redirected to another destination.

PSM provides the following facilities:

- Print-spooling—writes output to a print spool providing more control over output. This allows you to redirect output to another printer if one is not available.
- Centralized printer definition facilities—supports VTAM (LU1) and JES (SYSOUT) devices and lets you assign printer aliases. It also allows the output destination to be a printer exit
- Print request control—allows you to hold, release, browse and delete print requests, redirect print requests to another printer, change priorities and numbers of copies, and display the status of requests

### Note

References to JES in this chapter also apply to VOS3's JES3 and JES4 subsystems.

---

## Accessing PSM

PSM can be accessed in two ways:

- By selecting the Print Services Manager option at the Select Option ==> prompt on a panel
- By directly invoking the \$PSCALL NCL procedure from an OCS screen or an installation written NCL procedure. The PSM NCL interface is fully described in the *Network Control Language Reference*.

To access PSM from the Select Option ==> prompt, complete the following steps:

Step 1. Enter **/PSM** at a ==> prompt. The PSM : Primary Menu is displayed.

Figure 9-1. PSM : Primary Menu

```
SOLVPROD----- PSM : Primary Menu -----$PS001
Select Option ==>

  Q - Output Queue                               Userid USER01
  P - Printer Definition Maintenance             LU      TERM01
  F - Form Definition Maintenance               Time   11.04.33
  S - Setup Definition Maintenance              MON 24-SEP-2001
  D - Default Printer Assignment Maintenance
  A - Administration
  X - Exit

Userid ....  USER01__      ( Optional Q )
Printer ...   _____    ( Optional Q )

F1=Help      F2=Split      F3=Exit      F4=Return
                F9=Swap
```

For details of the options and fields available on this menu, press F1 (Help).

Option Q is discussed in this chapter. The remaining options are used for administrative functions and are described in the *Management Services Administrator Guide*.

---

## Listing Entries in the Print Queue

You can display a list of all the entries that are queued to print, and on which printer they are to print. To display this list, enter **Q** at the ==> prompt on the PSM : Primary Menu (/PSM). The PSM : Output Queue is displayed.

You can limit the display to the print queue for a specific printer by specifying a printer in the Printer field on the PSM : Primary Menu when entering the Q option.

Figure 9-2. Output Queue Panel

```

SOLVPROD----- PSM : Output Queue -----
Command ==> Scroll ==> PAGE

          S/B=Browse R=Release H=Hold M=Modify D=Delete I=Information
Userid   Req#  Status   Pr K  Lines Cpy Printer      Created
USER01   0070 HELD     50 K  4149  1 PSM-PRT001    16-JUN 10.01
USER01   0071 QUEUED   50 Y   93  2 PSM-PRT001    16-JUN 10.08
USER02   0074 HELD     50 K   223  1 PSM-PRT002    18-JUN 15.31
USER01   0075 HELD     50 Y   541  1 PSM-PRT002    26-JUN 10.05
USER03   0078 PRINTING 50 Y   41  1 PSM-PRT001    26-JUN 14.01
USER04   0079 BUILD    50 K  4000  1 PSM-PRT003    26-JUN 14.11
**END**

F1=Help      F2=Split    F3=Exit     F4=Return   F5=Find     F6=Refresh
F7=Backward  F8=Forward  F9=Swap

```

For details of the information displayed and actions available on this panel, press F1 (Help).

The S and M options are described in the following sections. For further information about the other options available, press F1 (Help).

### Displaying the Output of a Print Request

To browse the output of a print request, enter **B**, **I**, or **S** next to the required print request in the PSM : Output Queue. Figure 9-3 is an example.

Figure 9-3. Browse Output Panel

```

PROD----- PSM : Browse Output -----REQ# 0265
Command ==> Scroll ==> PAGE

S A B U Data
--+-----10---+-----20---+-----30---+-----40---+-----50---+-----60---+-----70
N N =====
1 N  COMMAND ENTRY CAPTURE PRINT
1 N =====
2 N  USERID : USER01                NAME : USER NUMBER 1          LO
2 N  DATE   : MON 24-SEP-2001
2 N  TIME   : 11.16.39
2 N  =====
2 N  pr
1 N  N10601 USERID: USER01 TERMINAL-ID: TERM02
1 N  N10602 NCL PROCEDURE LIBRARY ID: COMMANDS
1 N  N13450 PANEL SERVICES PATH NAME: PANELS
1 N  N10603 AUTHORITY LEVEL IS 82
1 N  N13451 NO EDS PROFILES ACTIVE IN ENVIRONMENT.
1 N  N13433 USER SERVICES PROCEDURE: $USERSER
1 N  N10624 NO NPF COMMAND RESTRICTIONS.
1 N  N10627 PPO MESSAGE DELIVERY DETAILS:
1 N  N10628 ..NO NPF MESSAGE RESTRICTIONS.
F1=Help      F2=Split    F3=Exit     F4=Return   F5=Find     F6=Refresh
F7=Backward  F8=Forward  F9=Swap     F11=Right

```

The information provided allows you to discover exactly how the print request looks when printed.

**Note**

Only data lines, not heading lines, are displayed.

For details of the information provided for each line of output on this panel, press F1 (Help).

### Modifying a Printer Entry

You can modify a print request to change where and how it is to be printed. To modify a print request, enter **M** next to the required print request in the output queue. The PSM : Print Request panel is displayed (see Figure 9-4).

*Figure 9-4. Print Request Panel*

```
PROD----- PSM : Print Request -----Page 1 of 1
Command ==>                                     Function=Modify

Userid ..... USER01           Lower Case? ..... JES
Request Number ... 1718         Form Name ..... FORM#60
Status ..... HELD              Lines/Cols per Page 60/132
Creation Date .... 01-JAN-1993  Banner Page ..... *DEFAULT
Creation Time .... 16.45.34     Setup Name .....
Lines ..... 31                 JES Form Name .....
                                   JES FCB/UCS .....
Priority ..... 50_ (1 to 99)    JES PGM .....
Copies ..... 1_ (1 to 255)     Destination ..... PRT01
Keep? ..... NO_ (YES or NO)    LU Name .....
Error Date/Time ..              Exit Name .....

PSM Printer
Printer Name ... PRT01_____
Output Class ... A_
Logmode .....
Exit Data .....

F1=Help      F2=Split      F3=File      F4=Save
              F9=Swap
```

The PSM : Request Panel provides all details about the print request. You can alter some of the fields on the panel.

For details of the information displayed on this panel, press F1 (Help).

---

## Confirming Printing

When you send a print request to a printer, the PSM : Confirm Printer panel is displayed. This panel is used to confirm the printer name, the number of copies, and the hold and keep settings that you require for your print request.

The fields displayed on the panel are set to the values last used by you. To change any of these fields, overwrite them with the desired information, and press F6 (Confirm). The new information is then used to print your print request.

*Figure 9-5. Confirm Printer Panel*

```
PROD----- PSM : Confirm Printer -----
Command ==>

Printer Name ..+ PRT01_____
Copies ..... 1__ (Range 1 to 255)
Hold? ..... NO_ (YES or NO)
Keep? ..... NO_ (YES or NO)

F1=Help      F2=Split      F9=Swap      F6=Confirm
F12=Cancel
```

For details of the information displayed on this panel, press F1 (Help).

## Selecting the Printer You Require

If you do not know what printers are available to send your print request to, you can display a list of active printers by entering a question mark (?) in the Printer Name field. The list of active printers is displayed on the PSM : Printer List panel.

To select a printer from the list, enter its selection code at the Select Entry ==> prompt.

Figure 9-6. Printer List

```
PROD----- PSM : Printer List -----
Select Entry ==>                               Scroll ==> PAGE

      Name      Type  Description
1 - MACHINE    VTAM  Alias for Machine Room Printer PRT003
2 - PRT001     JES   Network Operations JES Printer
3 - NMEXIT     EXIT  Print exit
4 - PRT002     JES   Development Group Printer
5 - PRT003     VTAM  Machine Room Printer
6 - PRT04      JES   Tokyo Office Printer
      **END**

F1=Help      F2=Split      F3=Exit      F5=Find
F7=Backward  F8=Forward    F9=Swap
```

If the list is longer than a full page, use F8 (Forward) and F7 (Backward) to scroll through the list.

For details of the information displayed on this panel, press F1 (Help).



# 10

---

## Linking Programs

This chapter describes how to use the Program to Program Interface (PPI) to link and send data to programs.

**This chapter contains the following topics:**

- About PPI
- Accessing PPI Facilities from Management Services
- Accessing PPI Facilities from Other Programs
- Checking PPI Status
- Controlling Receiver Programs
- Sending a Generic Alert to Management Services
- Controlling Data Buffers
- Waiting On an ECB
- Obtaining a Unique Sender or Receiver ID
- Receiving Information from a Receiver Program
- Tracing the Cause of a Processing Error

---

## About PPI

The Program-to-Program interface (PPI) provides a general-purpose protocol for programs, executing in the same OS/390 or z/OS system and written in any language, to freely exchange data. A PPI can use either Cross-Memory Services or Service Request Block (SRB) scheduling.

PPI was defined by IBM, however, an implementation of PPI is provided by Management Services. This implementation provides the same functionality as IBM's PPI as well as a facility for any program to send error information about itself to Management Services.

The Management Services PPI is currently supported on z/OS, OS/390, MSP, MSP/AE, MSP/EX, and VOS3/AS.

For more information about the Management Services PPI, see the *Network Control Language User's Guide* and the *Management Services Administrator Guide*.

For more information about IBM's PPI see the *IBM NetView Application Programming Guide: Program to Program Interface* manual, or the *NetView Application Programming Guide*.

---

## Accessing PPI Facilities from Management Services

To access PPI facilities from Management Services, use the &PPI verb. Each facility is identified by a keyword that is specified after the &PPI verb. The facilities take the form of requests that can be sent to other programs, including:

- &PPI ALERT
- &PPI DEACTIVATE
- &PPI DEFINE
- &PPI DELETE
- &PPI RECEIVE
- &PPI SEND
- &PPI STATUS

The &PPI verb and its use is fully described in the *Network Control Language Reference*.

## Accessing PPI from NCL Processes

To access PPI facilities in NCL, use the `&PPI` NCL verb and two NCL system variables, `&ZPPI` and `&ZPPINAME`. These verbs and system variables are fully described in the *Network Control Language Reference*.

After an `&PPI` verb is executed from an NCL process, the `&RETCODE` NCL system variable contains the return code that indicates success or failure. This value can be used as a quick test to check whether the operation worked or not. Generally, 0 indicates that there are no problems, 4 is a warning, 8 or 12 indicate errors of some sort. Return code 20 is only returned after `&PPI RECEIVE WAIT=NOTIFY` if a notification message arrives later.

If an error code is returned in `&RETCODE`, the `&ZFDBK` system variable can be used to investigate the error further. `&ZFDBK` contains the actual PPI return code as returned in the RPB after a call, or a simulated return code if NCL detected an error condition itself.

Any NCL process in the system can use PPI services. These are the only restrictions:

- To receive data, a process must register itself to PPI with a unique name, using the `&PPI DEFINE` option
- If a process does not register itself, and sends data, the PPI sender ID used is the 6-digit NCLID (leading zeros) prefixed with a hash (#) character
- An NCL process can be defined as only one receiver at a time

### NCL PPI System Variables

The following system variables are available with the NCL PPI facility:

#### **&ZPPI**

Indicates whether or not PPI is available in this system.

#### **&ZPPINAME**

Contains the defined receiver ID of the current NCL process.

#### **&RETCODE**

Contains a normalized return code after `&PPI` verb execution. See the `&ZFDBK` system variable for more detail.

#### **Note**

As `&RETCODE` is set by many NCL statements, it should be inspected immediately after an `&PPI` statement, or saved in a user variable for later inspection.

**&ZFDBK**

Contains the actual PPI RPB RETCODE value after an &PPI verb execution. It can be inspected as required when &RETCODE indicates an error condition to determine the exact error.

**Note**

As &ZFDBK is set by many NCL statements, it should be inspected immediately after an &PPI statement, or saved in a user variable for later inspection.

**&ZVARCNT**

Set after a successful &PPI RECEIVE to indicate the number of NCL tokens that have had data placed in them.

**NCL PPI User Variables**

The following NCL user variables can be set by some &PPI verb operations:

**&PPISENDERID**

Set to the sender ID of a data buffer after a successful &PPI RECEIVE operation. The sender ID can contain ampersand (&) characters.

**&PPIDATALEN**

Set to the actual byte length of the received data buffer after a successful &PPI RECEIVE operation.

The &PPI RECEIVE also sets nominated user variables with the received data.

---

## Accessing PPI Facilities from Other Programs

To access PPI facilities from non-Management Services programs, you have to construct calls to the PPI. To make a call you have to know the code for the request you are making, construct a Request Parameter Block (RPB), and specify the PPI API.

IBM's PPI uses an API module called CNMNETV to manage the data that is exchanged between programs. Management Services provides CNMNETM as the PPI API which has an alias of CNMNETV.

### Making PPI Calls

To make a PPI call, you must perform the following steps:

- Step 1. Construct a request parameter block (RPB) in a block of storage.
- Step 2. Make the call.

These two steps are described in detail in the following sections.

### Constructing an RPB

All PPI calls require an RPB. An RPB is a block of storage and must be exactly 56 bytes long. An RPB describes the request you want to make of the PPI. The fields specified in the RPB depend on the type of request you are making. PPI uses other fields in the RPB to return data to your program.

Table 10-1 describes the fields that can be used to construct the RPB (note that some fields overlap):

*Table 10-1. Request Parameter Block (RPB) Format (Sheet 1 of 3)*

Bytes	Name	Description
00-03	RPBLEN	A binary full word that must contain the length of the RPB. This field must be set to 56 (decimal or 38 hex). Note: For compatibility with earlier releases of PPI, a length of 40 (28 hex), 46 (2E hex), or 52 (34 hex) is permitted.
04-05	REQUEST	A binary half word that must be set to the request code for the PPI call. Valid request codes are described later.

Table 10-1. Request Parameter Block (RPB) Format (Sheet 2 of 3)

Bytes	Name	Description
06-07	RECOPT	A binary half word that must be set to one of the following values: 0 - no recovery is requested. 1 - ESTAE recovery is requested. Not valid if the program is executing in cross-memory mode.
08-11	RETCODE	A binary full word that is set by the PPI with the return code from the requested function. Refer to the function descriptions for possible return codes.
12-15	WORKADR	A binary full word that must be set to the address of a 128-byte work area. This area must be provided on all calls to the PPI. It need not be preserved across calls.
16-19	ASCBADDR	A binary full word, that is used to contain or return the ASCB address of the current address space. This is used in various PPI calls.
16-23	SENDERID	For those calls that require it, the 1 to 8 character sender ID. See the section <i>Obtaining a Unique Sender or Receiver ID</i> for details. If the supplied ID is less than 8 characters, it must be left-justified and blank-padded.
20-23	ECBADDR	A binary full word, returned when a receiver is defined, containing the address of an ECB that PPI posts when data arrives.
20-23	BUFFQL	A binary full word, supplied when defining or inactivating a receiver, that contains the receiver buffer queue limit. The supplied value is used to limit the number of buffers that can be queued to the receiver.
24-31	RECVRID	For those calls that require it, the 1 to 8 character receiver ID. See the section <i>Obtaining a Unique Sender or Receiver ID</i> for details. If the supplied ID is less than 8 characters, it must be left-justified and blank-padded.
32-35	BUFFLEN	A binary full word, supplied on some PPI calls, and returned on others, that contains the length of a supplied buffer or data, or the returned actual data length.
32-33	AUTHIND	A binary half word, used when defining a receiver to indicate whether senders must be APF authorized or not. The following values are allowed: 0 - No APF authorization is required. 1 - Senders must be APF authorized to send to this receiver.

Table 10-1. Request Parameter Block (RPB) Format (Sheet 3 of 3)

Bytes	Name	Description
34	FLAG1	Bit 0 (X'80') is set or reset by a request code 2 (query receiver) to indicate if the receiver queue is full—it is set if queue is not full, reset if it is full.
36-39	BUFFADDR	A binary full word that must be set to the address of a sending or receiving buffer on some calls. The length of this buffer must be set in the BUFFLEN field.
36-39	TCBADDR	A binary full word that must be set to the address of the current TCB when defining a receiver, or is returned on the 'get TCB/ASCB addrs' call.
40-45	RESERVED	These fields are not used in MVS.
46	REQIND1	Request indicator 1. Set bit 0 (X'80') before issuing a DEFINE RECEIVER (request code 4) if you do not want to change an existing receiver definition, even when the TCB/ASCB addresses match. A return code of 16 is returned instead. Set bit 1 (X'40') before issuing a QUERY PPI STATUS (request code 1) if you want to determine the version of PPI in use.
47	REQIND2	Request indicator 2 (presently unused).
48-51	VERSION	Request code 1 returns the PPI version here if requested to (by setting REQIND1 to X'40' before the call). The version returned is a full word 1 indicating NetView 2.4.
52-55	RESERVED	Presently unused.

### Specifying Sender and Receiver IDs

The SENDERID and RECVERID fields of the RPB are used to specify sender and receiver IDs as required. These IDs must adhere to the following rules:

- 1 to 8 characters—if shorter than 8 characters, must be left justified and blank padded, embedded blanks are not allowed
- The following characters can be used: A-Z, 0-9, @, #, \$, %, & no other characters are allowed
- IDs starting with NETV or NETM are reserved and can only be defined by the Management Services main task

## Making the Call

When making the PPI call, the following conventions must be followed:

- Register 1 must point to a full word in storage that points to the RPB. The *end of parmlist* bit (bit 0) of the full word can, but need not, be set.
- Register 13 must point to a standard 18-word save area.
- Register 14 must contain the return address in the calling program. This is normally done using the BALR instruction.
- Register 15 must contain the entry point of CNMNETM (or CNMNETV).
- The program must be in primary addressing mode, not secondary, AR, or HOME mode. It must be in TCB mode. SRB mode callers and cross-memory callers are not supported.

In an XA or ESA environment, all addresses in these registers and in the pointer to the RPB must be valid for the AMODE of the calling program. There is no requirement to be in 31 bit mode.

### Note

If a LOAD macro was used to obtain the address of CNMNETM (CNMNETV), the top bit of the returned address can be set. It is acceptable to use BALR, BASR, or BASSM to call it.

Most high-level languages follow the above conventions automatically.

Upon return, registers are restored. Register 15 is set to 0. It does not contain a return code. The return code is in the RPB.

### Example

Some examples of PPI calls in various languages follow:

Assembler	CALL CNMNETV, (RPB) CALL (R15), (RPB)
PL/1	CALL CNMNETV (RPB);
C	CNMNETV (RPB);
COBOL	CALL 'CNMNETV' USING RPB

**Note**

It is strongly recommended that CNMNETV not be link-edited with the program.

- In Assembler, use the LOAD macro to load CNMNETV and save the returned address.
- In PL/1, use the FETCH statement to load CNMNETV.
- In COBOL (VS COBOL II, pointer ability is needed), use the DYNAM option.

---

## Checking PPI Status

To check the status of PPI, use request code 1. This allows an application program to inquire about the status of the PPI facility. The return code indicates whether it is active or not.

The following RPB fields must be set:

Bytes	Field Name	Set to...
00-03	RPLEN	56
04-05	REQUEST	1
12-15	WORADDR	address of 128 byte work area
46	REQIND1	bit 1(X'40') if you want the PPI version returned
48-51	VERSION	binary 0 so that a back-level PPI can be detected correctly

The following RPB fields are returned after the call:

Bytes	Field Name	Contains
08-11	RETCODE	see below
48-51	VERSION	the PPI version number is RETCODE 10 is returned. F'1' indicates NetView 2.4. F'0' indicates a prior release.

The following return codes are possible:

<b>Return Code</b>	<b>Description</b>
10	PPI is active and available to process requests
24	PPI is not active
28	This release of Management Services does not support PPI requests
90	A processing error occurred

---

## Controlling Receiver Programs

There are a number of request codes that can be used to obtain information from, and control receiver programs:

- 2—Check the status of a receiver program
- 3—Obtain the ASCB and TCB addresses of a receiver program
- 4—Define and initialize a receiver program
- 9—Deactivate a receiver program
- 10—Delete an active receiver program

Each of these functions is described in the following sections.

### Checking the Status of a Receiver Program

To check the status of a receiver program, use request code 2. The return code from this request indicates whether the receiver is defined, active, or inactive.

The following RPB fields must be set up before the call:

<b>Bytes</b>	<b>Field Name</b>	<b>Set to...</b>
00-03	RPLEN	56
04-05	REQUEST	2
12-15	WORADDR	address of 128 byte work area
24-31	RECVRID	name of receiver you want to query

The following RPB fields are returned after the call:

<b>Bytes</b>	<b>Field Name</b>	<b>Contains</b>
08-11	RETCODE	see below
34	FLAG	Bit 0 is set if there is space on the receiver queue, or cleared if the receiver queue is full (for RETCODE 14 and 15)

The following return codes are possible:

<b>Return Code</b>	<b>Description</b>
14	The receiver program is active
15	The receiver program is not active
22	The requestor is not in primary addressing mode
24	PPI is not active
26	The receiver program is not defined
28	This release of Management Services does not support PPI requests
90	A processing error occurred

## Obtaining ASCB and TCB Addresses

To obtain ASCB and TCB addresses, use request code 3. This request code allows application programs written in languages that do not allow you to obtain the ASCB and TCB addresses of the current program, to obtain them. These addresses are required for some other PPI request codes.

The following RPB fields must be set up before the call:

<b>Bytes</b>	<b>Field Name</b>	<b>Set to...</b>
00-03	RPLEN	56
04-05	REQUEST	3
12-15	WORADDR	address of 128 byte work area

The following RPB fields are returned after the call:

Bytes	Field Name	Contains
08-11	RETCODE	see below
16-19	ASCBADDR	address of current ASCB
36-39	TCBADDR	address of current TCB

The following return codes are possible:

Return Code	Description
0	Request completed successfully
22	The requestor is not in primary addressing mode
24	PPI is not active
28	This release of Management Services does not support PPI requests
90	A processing error occurred

## Defining and Initializing a Receiver

To define or initialize a receiver, use request code 4. This request code allows you to perform the following functions:

- Define a receiver—it declares the name of the receiver and the buffer limit
- Initialize a receiver that does not exist
- Reactivate a defined but inactive receiver
- Alter the buffer queue limit—this can be performed at any time, as long as all the fields are specified, and the TCB/ASCB addresses match those of the defined receiver

Changing the value of the buffer queue limit does not cause buffers to be dropped if it is reduced. The change only prevents additional buffers from being queued.

- Prevent the accidental overwrite of an existing receiver definition by setting REQIND1 to X'80'—this flag causes an exclusive-active check to be made, that is, if the receiver is presently active, no change is made to it, regardless of a match on the TCB/ASCB addresses

The following RPB fields must be set up before the call:

<b>Bytes</b>	<b>Field Name</b>	<b>Set to...</b>
00-03	RPLEN	56
04-05	REQUEST	4
06-07	RECOPT	as required
12-15	WORADDR	address of 128 byte work area
16-19	ASCBADDR	address of the current ASCB (can be obtained by a request type 3)
20-23	BUFFQL	buffer queue limit. 0 to PPI maximum parameter
24-31	RECVRID	the receiver ID
32-33	AUTHIND	0 if senders do not require authorization. 1 if senders must be APF authorized
36-39	TCBADDR	address of the current TCB (can be obtained by a request type 3)
46	REQIND1	bit 0 (X'80') if an exclusive-active check is wanted

The following RPB Fields are returned after the call:

<b>Bytes</b>	<b>Field Name</b>	<b>Set to...</b>
08-11	RETCODE	see below
20-23	ECBADDR	address of receiver ECB. See below.

The following return codes are possible:

<b>Return Code</b>	<b>Description</b>
0	Request completed successfully—ECB address is set
16	The receiver program is already active, and the TCB/ASCB address did not match, or they matched but the exclusive-active check flag (REQUIND=X'80') is set
22	The requestor is not in primary addressing mode
24	PPI is not active
25	The ASCB address is not correct
28	This release of Management Services does not support PPI requests
32	No storage available
36	ESTAE could not be established as requested
40	Invalid receiver ID
90	A processing error occurred

**Note**

Receiver ID names starting with NETM or NETV can only be defined by Management Services, unless the PPINETM/R parameters are set to NO.

The returned ECB-address field provides the address of an ECB, in the caller's TCB key, in a protected subpool (that is, cannot be freed by user code), that is posted when buffers are available to the receiver. The user should never alter this ECB. It is automatically cleared and posted when relevant.

The return code is 0 if buffers are available, and 99 if the PPI facility is shutting down.

**Note**

NetView 2.4 allows you to define a receiver passing a zero ASCB address—in this case it does not allocate an ECB. The SOLVE PPI does not support this and returns RETCODE=25 (invalid ASCB address).

## Deactivating a Receiver

To deactivate a receiver program, use request code 9. If a receiver is not deactivated explicitly, it is deactivated at end of task or end of address space of the associated task/address space. Explicit deactivation allows you to reset the buffer queue limit.

The following RPB fields must be set up before the call:

Bytes	Field Name	Set to...
00-03	RPLEN	56
04-05	REQUEST	9
06-07	RECOPT	as required
12-15	WORADDR	address of 128 byte work area
16-19	ASCBADDR	address of the current ASCB (can be obtained by a request type 3)
20-23	BUFFQL	buffer queue limit. 0 to PPI maximum parameter
24-31	RECVERID	the receiver ID

The following RPB Field is returned after the call:

Bytes	Field Name	Set to...
08-11	RETCODE	see below

The following return codes are possible:

Return Code	Description
0	Request completed successfully—ECB address is set
15	The receiver program is already inactive
22	The requestor is not in primary addressing mode
24	PPI is not active
25	The ASCB address is not correct
26	The receiver program is not defined
28	This release of Management Services does not support PPI requests
36	ESTAE could not be established as requested
40	Invalid receiver ID
90	A processing error occurred

**Note**

Only the owning task/address space can explicitly deactivate a receiver.

## Deleting an Active Receiver

To delete an active receiver program, use request code 10. Any unreceived data buffers are purged.

The following RPB fields must be set up before the call:

Bytes	Field Name	Set to...
00-03	RPLEN	56
04-05	REQUEST	10
06-07	RECOPT	as required
12-15	WORADDR	address of 128 byte work area
16-19	ASCBADDR	address of the current ASCB (can be obtained by a request type 3)
24-31	RECVRID	the receiver ID

The following RPB Field is returned after the call:

Bytes	Field Name	Set to...
08-11	RETCODE	see below

The following return codes are possible:

Return Code	Description
0	Request completed successfully—the receiver has been deleted
15	The receiver program is already inactive
22	The requestor is not in primary addressing mode
24	PPI is not active
25	The ASCB address is not correct
26	The receiver program is not defined
28	This release of Management Services does not support PPI requests
36	ESTAE could not be established as requested
40	Invalid receiver ID
90	A processing error occurred

**Note**

Only the owning task/address space can explicitly delete a receiver.

---

## Sending a Generic Alert to Management Services

To send a generic alert to Management Services, use request code 12. There is no special PPI setup required to do this.

The following RPB fields must be set up before the call:

Bytes	Field Name	Set to...
00-03	RPLEN	56
04-05	REQUEST	12
06-07	RECOPT	as required
12-15	WORKADDR	address of 128 byte work area
32-35	BUFFLEN	length of the generic alert data
36-39	BUFFADDR	address of the generic alert data

The following RPB Fields are returned after the call:

Bytes	Field Name	Set to...
08-11	RETCODE	see below

The following return codes are possible:

<b>Return Code</b>	<b>Description</b>
0	Request completed successfully
4	The ALERT receiver task (NETVALERT) is not active—the alert has been queued
22	The requestor is not in primary addressing mode
24	PPI is not active
26	The NETVALERT receiver program is not defined
28	This release of Management Services does not support PPI requests
32	No storage available
33	Invalid buffer length
35	Alert receiver buffer queue full
36	ESTAE could not be established as requested
40	Invalid sender ID
90	A processing error occurred

**Note**

The generic alert must include the 8-byte NMVT header.  
The default buffer queue limit for the alert receiver is 1000 generic alerts.  
A return code of 22 or greater means that the alert has not been copied to the alert receiver queue.  
If no hierarchy/resource list subvector is provided in the generic alert, the sender-ID is used as the resource name.  
PPI does not release the data buffer storage. Your program must do this if required.

---

## Controlling Data Buffers

There are a number of request codes that can be used to control the sending and receiving of data buffers:

- 14—sending a data buffer to a receiver program
- 22—allowing a receiver program to receive a data buffer
- 23—purging a data buffer from a receiver program

### Sending a Data Buffer to a Receiver

To send a data buffer to a receiver program, use request code 14. The receiver program does not need to be active. As long as its buffer queue limit is not exceeded, the data buffer is queued to it.

The following RPB fields must be set up before the call:

Bytes	Field Name	Set to...
00-03	RPLEN	56
04-05	REQUEST	14
06-07	RECOPT	as required
12-15	WORKADDR	address of 128 byte work area
16-23	SENDERID	a valid sender ID
24-31	RECVERID	the target receiver ID
32-35	BUFFLEN	length of the data buffer to send
36-39	BUFFADDR	address of the data buffer to send

The following RPB Field is returned after the call:

Bytes	Field Name	Set to...
08-11	RETCODE	see below

The following return codes are possible:

<b>Return Code</b>	<b>Description</b>
0	Request completed successfully
4	The specified receiver is not active—the buffer has been queued
22	The requestor is not in primary addressing mode
23	The sender program is not authorized
24	PPI is not active
26	The receiver program is not defined
28	This release of Management Services does not support PPI requests
32	No storage available
33	Invalid buffer length
35	The receiver buffer queue full
36	ESTAE could not be established as requested
40	Invalid sender ID
90	A processing error occurred

**Note**

The sender must be APF authorized if sending a buffer to a receiver defined as authorized.

After the call the data buffer is queued to the nominated receiver.

The PPI does not release the data buffer storage. Your program must do this if required.

## Allowing a Receiver to Receive a Data Buffer

To allow a defined, active receiver to receive a data buffer, use request code 22. The next buffer in the receiver buffer queue is made available in the user-provided area.

The following RPB fields must be set up before the call:

<b>Bytes</b>	<b>Field Name</b>	<b>Set to...</b>
00-03	RPLEN	56
04-05	REQUEST	22
06-07	RECOPT	as required
12-15	WORKADDR	address of 128 byte work area
16-19	ASCBADDR	the receiver ASCB address
20-23	ECBADDR	the receiver ECB address—this is only set when RETCODE 30 is returned
24-31	RECVERID	the target receiver ID
32-35	BUFFLEN	length of the data buffer to send
36-39	BUFFADDR	address of the data buffer to send

The following RPB Fields are returned after the call:

<b>Bytes</b>	<b>Field Name</b>	<b>Set to...</b>
08-11	RETCODE	see below
16-23	SENDERID	ID of sender of this buffer
32-35	BUFFLEN	actual data buffer length

The following return codes are possible:

<b>Return Code</b>	<b>Description</b>
0	Request completed successfully
22	The requestor is not in primary addressing mode
24	PPI is not active
25	The ASCB address is not correct
26	The receiver program is not defined
28	This release of Management Services does not support PPI requests
30	No data buffers in the receiver's buffer queue
31	The receiver buffer size is not large enough for the incoming data buffer
33	Invalid buffer length
35	The receiver buffer queue full
36	ESTAE could not be established as requested
40	Invalid sender ID
90	A processing error occurred

**Note**

The correct ASCB address is required. This is the ASCB address as provided when the receiver was defined.

One data buffer at a time can be received. They are provided first-in-first-out order. The sender-ID of the sending program is provided if the call is successful.

The length of the incoming buffer is provided in the BUFFLEN field after the call. If a return code 31 (buffer too small) is given, this is the required length needed to successfully receive the buffer. The call can be reissued after obtaining a large enough buffer.

If no data is queued, a return code of 30 is given and the ECBADDR field is set to the ECB address, as returned by DEFINE RECEIVER. The receiver can wait (using the WAIT macro or request code 24) until more data arrives.

## Purging the Data Buffer

To allow the caller to purge the front buffer on a receiver queue, use request code 23. It is equivalent to receiving the buffer and ignoring it, except that no receiver buffer is needed—this is useful for purging buffers that are too long.

The following RPB fields must be set up before the call:

Bytes	Field Name	Set to...
00-03	RPLEN	56
04-05	REQUEST	23
06-07	RECOPT	as required
12-15	WORKADDR	address of 128 byte work area
16-19	ASCBADDR	address of current ASCB
24-31	RECVERID	the target receiver ID

The following RPB Field is returned after the call:

Bytes	Field Name	Set to...
08-11	RETCODE	see below

The following return codes are possible:

Return Code	Description
0	Request completed successfully—the front data buffer has been purged
22	The requestor is not in primary addressing mode
24	PPI is not active
25	The ASCB address is not correct
26	The receiver program is not defined
28	This release of Management Services does not support PPI requests
30	No data buffers in the receiver's buffer queue
36	ESTAE could not be established as requested
40	Invalid sender ID
90	A processing error occurred

**Note**

The correct ASCB address is required—that is, the ASCB address provided when the receiver was defined.

Only one data buffer at a time can be purged.

Return code 30 is returned if no buffers are queued.

---

## Waiting On an ECB

To allow the caller to wait on an ECB, use request code 24. This allows receiver programs written in languages that do not support a WAIT service to wait for input.

The following RPB fields must be set up before the call:

Bytes	Field Name	Set to...
00-03	RPLEN	56
04-05	REQUEST	24
12-15	WORKADDR	address of 128 byte work area
20-23	ECBADDR	address of the ECB

The following RPB Field is returned after the call:

Bytes	Field Name	Set to...
08-11	RETCODE	see below

The following return codes are possible:

Return Code	Description
0	Request completed successfully—the ECB has been posted
18	The ECB was not 0 on entry to this function—it might have been already posted
22	The requestor is not in primary addressing mode
24	PPI is not active
28	This release of Management Services does not support PPI requests

**Warning**

This function should only be used if your programming language does not support a WAIT facility. Unpredictable results can occur if the PPI subsystem is terminated while you are waiting using this request.

**Note**

The ECB address is returned by a request code 4 (define a receiver).

You can wait using request code 24 after receiving a return code 30 from receive.

Remember to test the ECB post code in the last byte of the ECB for 0 (data available) or 99 (PPI shutting down).

---

## Obtaining a Unique Sender or Receiver ID

To obtain a unique sender or receiver ID, use request code 60. This is useful when establishing a bidirectional conversation with another program. The other program can be a globally known program, with a known ID. However, this program cannot use a reserved, unique ID. In this case it can use this service to obtain a valid, unique ID.

This service is only supported by the Management Services implementation of PPI (known as SOLVE PPI).

The following RPB fields must be set up before the call:

Bytes	Field Name	Set to...
00-03	RPLEN	56
04-05	REQUEST	24
12-15	WORKADDR	address of 128 byte work area

The following RPB Fields are returned after the call:

Bytes	Field Name	Set to...
08-11	RETCODE	see below
24-31	RECVERID	the returned unique ID

The following return codes are possible:

<b>Return Code</b>	<b>Description</b>
0	Request completed successfully—a unique ID has been allocated
20	Invalid function (not the SOLVE PPI)
22	The requestor is not in primary addressing mode
24	PPI is not active
28	This release of Management Services does not support PPI requests
90	A processing error has occurred— this also indicates that no more unique IDs are available

The returned ID is in the format: *pppp&nnn* where *pppp* is the 1 to 4 character PPI name prefix, as set by one of the PPI SSI JCL parameters. If less than 4 characters, it is padded to 4 characters with ampersand (&) characters. Position 5 is always an ampersand. Positions 6 to 8 are allocated from the characters: 0-9, A-Z, @, #, \$, and %. This allows up to 64000 unique IDs.

Unique IDs can be re-used. If an ID is obtained, defined, and then inactivated, and nothing is queued to it, then, subject to the PPIINATO and PPIREUSE SSI startup parameter values, the ID can be made available for later reuse.

If the PPI prefix is set to the same value as the associated Management Services domain ID, then these IDs are also unique across the connected network.

## Receiving Information from a Receiver Program

When you receive information from a receiver program after sending a PPI call, a number of return codes are possible. Table 10-2 is a full list of possible PPI return codes, a complete description of the possible causes, and all request codes that can cause that return code.

### Note

These are the RPB return codes. NCL interface return codes (in &RETCODE) are different. The NCL interface returns the PPI return code as described below in &ZFDBK for information purposes.

Table 10-2. Possible Return Codes from PPI and Their Causes (Sheet 1 of 3)

Return Code	Description	Returned on Requests
0	The PPI request has completed successfully. The requested function has been performed with no errors or warnings.	3, 4, 9, 12, 14, 22, 24, 60
4	The specified receiver is not presently active. The data buffer or generic alert has been queued. (The receiver buffer queue was not full).	12, 14
10	The PPI facility is active and might be used. This is a good return code.	1
14	The receiver program is active.	2
15	The receiver program is (already) inactive. It is defined but has been explicitly or implicitly deactivated.	2, 9
16	The receiver program is already active. It cannot be defined.	4
18	The ECB is not 0 (normally the receiver ECB). This is not necessarily an error condition, as the ECB might have been posted after it was last checked.	24
20	Invalid request type. The passed request code was not valid. This can occur with request code 60 if PPI is not being provided by Management Services. Otherwise, it is probably an error in formatting of the RPB.	any incorrect request
22	The program is not executing in primary addressing mode. Programs must not call the PPI in secondary mode (MVS, XA, ESA), or AR or home mode (ESA). They must be in primary mode, although they can be in cross-memory mode (that is primary ^= home).	1, 2, 3, 4, 9, 12, 14, 22, 24, 60
23	The program is not authorized. Attempt to send a buffer to a receiver defined as authorized.	14

Table 10-2. Possible Return Codes from PPI and Their Causes (Sheet 2 of 3)

Return Code	Description	Returned on Requests
24	PPI is not active. The SSI is not active or PPI is not running on a SOLVE SSI or NetView SSI. In the Management Services implementation, can also indicate that this system does not support PPI, as it has not built the relevant control block structure.	All
25	The ASCB address is not correct. To deactivate a receiver or receive data, the correct ASCB address must be supplied.	9,22
26	The receiver is not defined. The supplied receiver name has never been defined to this execution of PPI. Note that this could occur if the PPI-owning SSI is stopped and restarted.	2, 9, 12, 14, 22
28	This Management Services (or NetView) release does not support PPI. This return code cannot occur with the implementation of the SOLVE PPI. It can occur if NetView is providing PPI services.	All
30	No data buffers available in the receiver queue. There is no data to be received. Note that in this case, PPI clears the receiver ECB automatically.	22
31	The receiver data buffer length is too short to receive the next data buffer. The RPB buffer length contains the length of the pending buffer.	22
32	No storage available. Unable to obtain storage required to complete the requested function.	4, 12, 14
33	Invalid buffer length. The supplied RPB or data buffer length was not valid. (See page 10-5 for valid RPB lengths.) For a data buffer, the length must be less than 1 or greater than the PPI maximum buffer size JCL parameter.	All
35	The receiver buffer queue is full. As the queue is full, the new data buffer is not added to the queue.	12, 14
36	Unable to establish ESTAE protection as requested. Either the caller is not in home mode, or the ESTAE gave a non-zero return code.	All
40	The specified receiver or sender ID is invalid. It does not satisfy the documented rules for these IDs, or (when defining, deactivating, or receiving for a receiver), starts with NETV or NETM and the requesting task is not the SSI-connected Management Services.	4, 9, 12, 14, 22

Table 10-2. Possible Return Codes from PPI and Their Causes (Sheet 3 of 3)

Return Code	Description	Returned on Requests
90	A processing error has occurred. This is a catch-all return code that covers many things: 1. ESTAE-trapped ABENDs 2. Various internal errors	All

In addition to the above return codes, some fundamental errors can cause SOC4 ABENDs. These would include an RPB that cannot be referenced, or a bad work-storage address. A bad save area address (for example, a 31-bit address for a 24-bit mode caller) can also cause it.

---

## Tracing the Cause of a Processing Error

Return code 90 indicates that a processing error occurred. This return code has a trace facility that allows you to determine the cause of the processing error. This facility is enabled during NMSSI setup (see the *Management Services Administrator Guide* for details on setting up NMSSI).

When you issue a PPI call, processing messages from the receiver program are written as WTOs to your system console. If tracing is enabled, and a return code of 90 is recorded in register 15, register 0 records debugging information which is also sent to the system console. This additional information can be used by you to debug the processing error.

Register 0 contains the debugging information as follows:

`X'rrrrmm5A'`

where:

**rrrr**

Is the *reason code* of the debugging information, in signed hexadecimal, length 2 bytes. For example, a reason code of 10 would be X'000A' and -141 would be X'FF73'.

**mm**

Is the *module* identification of the debugging information in hexadecimal. For example, 35 would be X'23'.

**5A**

Is 90 in hex, which indicates that the debugging information has been set in R0.

Following is the resulting message format that you receive on the system console:

```
NS3580 PPI RC=90 MOD=aa REAS=bbbbbb - RPB FOLLOWS...
NS3581 RPB +nnn xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
NS3581 ... (for total RPB length)
NS3582 *END*
```

The fields in the messages are:

**MOD=aa**

Contains the *module* identification of the debugging information, in decimal. For example, MOD=35.

**REAS=bbbbbb**

Contains the (signed) *reason code* of the debugging information, in decimal. For example, REAS=-00121.

**+nnn**

Contains the offset, in hexadecimal, of the start of the hex dump of the RPB (up to 16 bytes is dumped per line).

**xxxxxxx**

8 hex digits representing RPB data.

## Debugging Codes

Table 10-3 is a list of all the most likely combinations of debugging module IDs and reason codes, with a brief description of the causes of each. If you receive any other module IDs, contact the help desk.

*Table 10-3. Possible Combinations of RC90 Trace Module IDs and Reason Codes*

<b>MOD</b>	<b>REASON</b>	<b>R0</b>	<b>Description</b>
35	1	0001235A	No work storage address or bad address
35	2	0002235A	Recovery option not 0 or 1
35	4	0004235A	ESTAE exit driven
36	4	0004245A	ESTAE exit driven
36	5	0005245A	Bad BUFQ-LIM value
36	6	0006245A	Bad RPB AUTH-IND option value (not 0 or 1)
37	1	0001255A	Define receiver TCB/ASCB not correct
37	2	0002255A	Redefine inactive receiver TCB/ASCB incorrect
37	4	0004255A	FRR driven during Send Buffer processing
37	5	0005255A	FRR driven during Receive Buffer proc
37	6	0006255A	All unique names in use (PPI func. 60)



---

# Issuing System Commands from Your Console

This chapter describes how you can use the SYSCMD facility to manage the system console.

**This chapter contains the following topics:**

- About the SYSCMD Facility
- Using the SYSCMD Facility in OS/390, z/OS, MSP, and VOS3
- Using the SYSCMD Facility in VM
- SYSCMD Command Summary

For detailed descriptions of any of the commands, verbs, or system variables discussed in this chapter, see the following manuals:

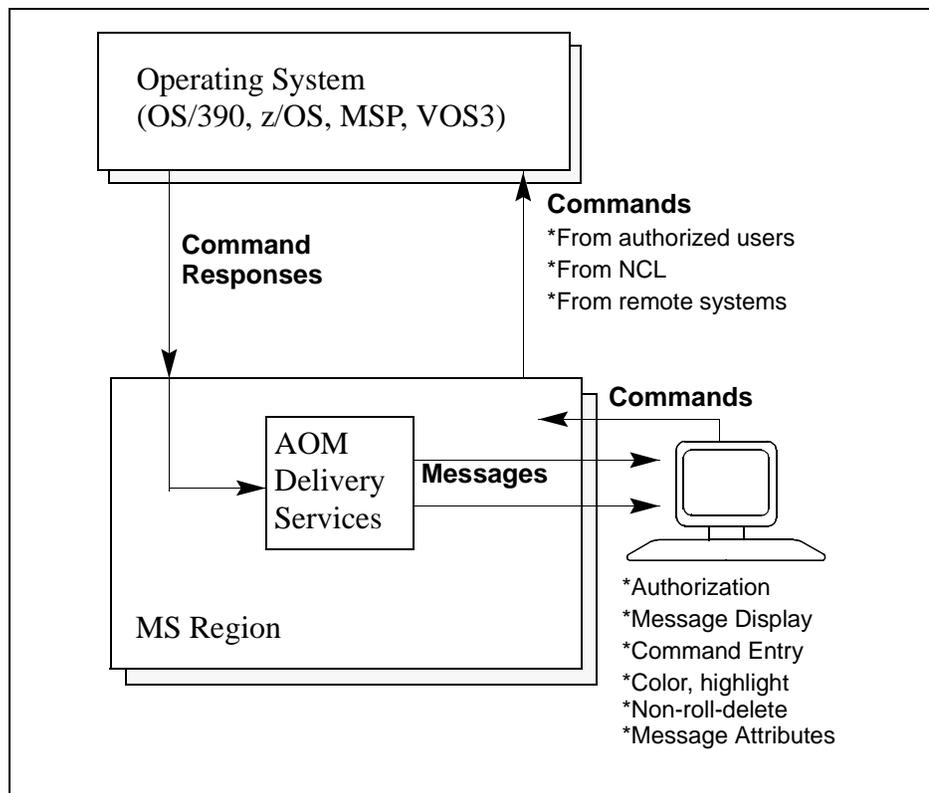
- The *Management Services Command Reference* for commands
- The *Management Services Administrator Guide* for SYSPARMS operands
- The appropriate volume of the *Network Control Language Reference* manual for verbs and system variables

## About the SYSCMD Facility

The SYSCMD facility gives you the ability to issue operating system commands and receive responses without having to use a *real* operating system console (see Figure 11-1 below); for example, to display the channel path or unit status of a local non-SNA terminal.

The SYSCMD facility is a subset of Advanced Operations Management (AOM) commands. This facility is available only if you have installed the NEWS component of NetMaster for SNA and are licensed for SYSCMD.

Figure 11-1. Overview of the SYSCMD Facility



### Note

You can use the SYSCMD facility in the OS/390, z/OS, MSP, and VOS3 operating system environments. In this chapter, references to specific environments are made only when it is necessary to distinguish between them. See the following section, *Using the SYSCMD Facility in OS/390, z/OS, MSP, and VOS3*.

You can also use the SYSCMD facility in the VM operating system environment. See the section, *Using the SYSCMD Facility in VM*, on page 11-5.

---

## Using the SYSCMD Facility in OS/390, z/OS, MSP, and VOS3

The SYSCMD command has several operands that you can use to enter master console commands, lock a console, or issue a command as if it came from a specific console. These operands are discussed over the following pages.

In its most basic form, the SYSCMD command is:

```
SYSCMD command-text
```

The *command-text* variable is the command to be entered.

### Note

You are restricted in your use of the SYSCMD facility by both your command authority and your user security profile. These are set by your systems administrator.

## Entering Master Console Commands

If the command to be entered is usually restricted to the master console, the CON=MASTER operand must be used with the SYSCMD command. For example:

```
SYSCMD CON=MASTER DATA=VARY CPU(0) OFFLINE
```

You must have MASTER authority for this.

### Note

This is not necessary if you are using Extended Multiple Console Support (EXTMCS) consoles.

## Locking a Console

To ensure that you can issue commands when you need to, you can lock a console to a specific environment. You should release the console when you no longer require it, so that it is made available to other SYSCMD users.

## Simulating Command Issue from a Specific Console

If you want to simulate the issue of a command from a specific console that you are not using, enter the following form of the SYSCMD command (where *n* is the console number):

```
SYSCMD CON=n DATA=command-text
```

This can be done from anywhere within the system.

As no console authority checks are made by the SYSCMD facility, the existing authority for the specified console is used.

### Note

The form of the SYSCMD command described in the example above is not supported if you are using EXTMCS consoles.

## Displaying the Status of the Console Pool

The SHOW CONSOLES command can be used to show the status of the console pool and various statistics for the console pool. The display (see Figure 11-2) provides two types of console information:

- SYSPARMS settings
- Statistics

Figure 11-2. Results of the SHOW CONSOLES Command

```
((16.26)----- Operator Control Services (PROD) -----  
show consoles  
N86E01 CONSOLE INFORMATION FOLLOWS...  
N86E10 SYSPARM SETTINGS...  
N86E11 CONSOLES AOMCTYPE AOMCMIGI AOMCUTOK AOMCTO1 AOMCTO2 AOMCTO3  
N86E12 (20,10) EXTMCS Y Y 10 20 5  
N86E13 AOMCMIGX AOMCOPTS AOMJESCH AOMSUBCH  
N86E14 NO 00 $ NO  
N86E20 STATISTICS...  
N86E21 #-LOG-AQ #-PHY-AQ %-PL-A AV-TM-PA #-LOG-RL #-PHY-RL %-PL-R AV-TM-PR  
N86E22 11 7 63.63 1.28 9 0 0.00 0.00  
N86E23 #-LA-MIG %-LA-M #-PA-MIG %-PA-M #-LA-FNC %-LA-F #-PA-FNC %-PA-F  
N86E24 5 45.45 3 42.85 0 0.00 0 0.00  
N86E30 C# ID NAME STATUS LOCK AUTH USERID ENV W T/O  
N86E31 1 224 ZD1ZZ010 IN-USE AOM MASTER DE1NAOMP AOM - -  
N86E31 2 - ZD1ZZ011 POOL - MASTER - - - -  
N86E31 3 - ZD1ZZ012 POOL - MASTER - - - -  
N86E31 4 - ZD1ZZ013 POOL - MASTER - - - -  
N86E31 5 225 ZD1ZZ014 POOL - MASTER - - - -  
N86E31 6 - ZD1ZZ015 POOL - MASTER - - - -  
N86E31 7 246 ZD1ZZ017 POOL - MASTER - - - -  
N11907 *END*  
-----NetMaster -----  
==>
```

For further information about the SYSPARMS settings, see the *SYSPARMS Operands* appendix of the *Management Services Administrator Guide*.

For further information about the statistics displayed, place your cursor on a line of statistics (for example, the line prefixed by message number N86E21, and press P1 (Help). This displays online help for the statistics on that line.

---

## Using the SYSCMD Facility in VM

In VM, the only form of the SYSCMD command that you can use is its basic form:

```
SYSCMD command-text
```

The *command-text* variable is the command to be entered.

### Note

You are restricted in your use of the SYSCMD facility by both your command authority and your user security profile. These are set by your systems administrator.

However, you can specify where this command is to be executed, by using the DEST operand:

```
DEST={ PROP | GCS | VMOP }
```

These destinations are as follows:

- PROP (the default) routes the command to the PROP virtual machine for execution there.
- GCS issues the command under the GCS environment of the virtual machine where the system is executing.
- VMOP routes the supplied command to the VMOPERATOR machine for possible execution.

### Note

You must be authorized in your user ID definition for the specified destination.

---

## **SYSCMD Command Summary**

### **AOM START**

Starts the local SYSCMD subset of the AOM operating system interface.

### **AOM STOP**

Stops the local SYSCMD subset of the AOM operating system interface.

### **PROFILE**

Displays a user profile

### **SHOW AOMABEND**

Displays diagnostic information if the SYSCMD OS/390, z/OS, MSP, or VOS3 subsystem interface code abends.

### **SHOW AOMSTAT**

Displays AOM statistics.

### **SHOW CONSOLES**

Displays the consoles currently allocated to your region for use by the SYSCMD facility.

### **STATUS**

Displays current system status information.

### **SUBMIT**

Passes a command to a background environment for processing.

### **SYSCMD**

Issues a command to the local operating system and returns associated response messages to your region.

### **SYSPARMS**

Initializes or modifies SYSCMD facility system parameter values.

For detailed information on the above SYSCMD facility commands, see your *Management Services Command Reference* manual.

# A

---

## Management Services Commands

This appendix provides a list and brief description of all the available Management Services commands.

## Summary Table

A quick summary of the commands available in Management Services is presented in the following table. The level of authority required to execute each command is also listed.

For a full description of all Management Services commands, see the *Management Services Command Reference*.

Command	Description	Auth
ABENDCMD	Sets the command to be issued if the NetMaster or SOLVE system terminates abnormally	9
ACT	Activates a VTAM network node	1
ACTLOGON	Activates previously suspended logon paths	3
ALLOCATE	Allocates a cataloged or sysout or VSAM dataset to management services	0/3
AOM GO	Restarts the local AOM operating system interface after a PAUSE	2
AOM NEWTAB	Compiles and (optionally) loads a new AOM Screening Table	2
AOM PAUSE	Suspends the local AOM operating system interface	2
AOM START	Starts the local AOM operating system interface	2
AOM STOP	Terminates the local AOM operating system interface	2
AT	Issues a command(s) or a message AT the specified time of day	0/2
ATF DEFINE	Defines a new transition name.	2
ATF LOAD	Loads translation tables for a specific translation name into storage.	2
ATF UNLOAD	Unloads translation tables for a specific translation name.	2
ATTACH	Attach a local non-SNA terminal to SOLVE SSI	3
AUTOHOLD	Determines the OCS screen display line mode	0
CANCEL	Cancels a nominated user or user region or window	0/1
CLEAR	Clears the current logical screen window	0
CLSDST	Closes the session(s) with the specified terminal(s)	1/0
CNM0	Starts and stops the VTAM CNM interface	3
CNMTRACE	Defines which CNM records are to be traced	3
CONNECT	Connects a terminal to NetMaster or SOLVE using XNF	1
CS-	Retrieves the command from the bottom of the command stack	0
CS+	Retrieves the command from the top of the command stack	0
D	Displays a specific VTAM resource	0
DEBUG	Controls the execution and debugging of NCL processes	0/3
DEFALIAS	Defines an alias entry for the Alias Name Translation Facility of NEWS	4
DEFCLASS	Defines RTM, SAW, Session or Resource classes	4

<b>Command</b>	<b>Description</b>	<b>Auth</b>
DEFLINK	Maintains the Dynamic Link Table, or DLT, used by LU6.2 services	3
DEFLOGON	Defines the logon information for the EASINET and MAI features	4
DEFMODE	Defines an entry in the Mode Control Table used by LU6.2 services	4
DEFMSG	Defines delivery options for PPO messages	4
DEFOPSET	Defines an entry in the OSCT table	4
DEFTERM	Defines terminal type (VOS3 only)	2
DEFTRANS	Defines an entry in the or TCT used by LU6.2 services	4
DELALIAS	Deletes an alias entry used by the Alias Name Translation Facility	4
DELCLASS	Deletes an NTS class definition	4
DELLINK	Deletes a dynamic link definition	3
DELLOGON	Deletes an entry form EASINET/MAI appl table	4
DELMODE	Deletes an APPC MCT table entry	4
DELOPSET	Deletes an APPC Option Set Control Table (OSCT) entry	4
DELTERM	Deletes terminal definition (VOS3 only)	2
DELTRANS	Deletes an APPC Transaction Control Table (TCT) entry	4
DETACH	Detaches a local non-SNA terminal from SOLVE SSI	3
DISCONN	Disconnects either the current or the nominated processing region	0/1
DNR	Defines or modifies parameters for the SOLVE Domain Name Resolver (DNR)	4
DOMAIN	Defines or deletes a domain	3
EDB	Defines, starts, stops and deletes an EDB connection	4
EDIT	Invokes panel maintenance from an OCS window or NCL procedure	0
END	Terminates a paused NCL process without further processing	0/2
ENTER	Defines the ENTER key	0
EQUATE	Assigns a text value to a unique string	0
EVERY	Issues a command or series of commands at a specified time frequency	0/2
EXEC	Schedules an NCL process for serial execution	0
F	Issues a VTAM modify (F) command	1
FLUSH	Terminates an NCL process without further processing	0/2
FORCE	Forcibly inactivates a VTAM network node	1
FSPROC	Executes an NCL procedure in OCS fullscreen mode	0
FSTOP	Forces an immediate shutdown of the system	3
FTS	Involves File Transmission Services	0
FTSINIT	Modifies the status of FTS initiators	0
FTSMOD	Modifies the status of incoming or outgoing FTS transmissions	0

<b>Command</b>	<b>Description</b>	<b>Auth</b>
GO	Resumes processing for a paused NCL process	0/2
INACT	Inactivates a VTAM network node	1
INTQUE	Passes data to an NCL procedure's &INTREAD statement	0/2
ISR	Changes the status of ISR (Inter System Routing) conversations	2
JOURNAL	Controls the Management Services journal dataset	2
K	Clears the current OCS window	0
LIBPATH	Controls library path definitions	4
LIBRARY	Controls library definitions	4
LINK	Defines or changes the status of the INMC/NVC/APPC links	3
LIST	Lists statements in a specific member of the procedure library	0
LOCK	Suspends current screen processing	0
LOG	Writes messages to the activity log	0
LOGSWAP	Swaps logging to the next available log	3
LSRPOOL	Sets attributes for the VSAM shared resource pool	2
LTITLE	Sets the title for the management services logo panel	4
LUTRACE	Traces session traffic to selected terminals	4
MAIDISC	Forces disconnection of an MAI-OC session	0
MAIINT	Interrupts an MAI-OC application	0
MAILOGON	Creates an MAI-OC session with another application	0
MAISEND	Sends data to an application connected by an MAI-OC session	0
MAI SESS	Provides functions for the control of MAI/FS sessions	0/4
MAXUSERS	Displays and limits the maximum number of concurrent users	3
MSG	Sends a message to the specified OCS Operator(s)	0
NCLCHECK	Tests syntax for an NCL procedure without execution	0
NCLTEST	Sets, resets, or displays NCL test status for this window	0
NCLTRACE	Dynamically alters the trace status of an executing NCL process	0/2
NDB ALTER	Builds, rebuilds or validates the key indexes for an NDB, or a field	2
NDB CREATE	Initializes a new \$NDB database	2
NDB FIELD	Allows a database field definition to be added, deleted, or updated	2
NDB PURGE	Frees up a locked or halted database	2
NDB RESET	Deletes all data from a \$NDB database	2
NDB START	Starts a \$NDB database	2
NDB STOP	Flags a \$NDB database as stopping	2
NDB UNLOAD	Unloads a copy of a \$NDB database	2
NETM	Passes a command to NETM for execution (VOS3 only)	2

<b>Command</b>	<b>Description</b>	<b>Auth</b>
NETMCNTL	Controls communication between NetMaster or SOLVE and NETM (VOS3 only)	2
NETSTAT	Invokes the TCP/IP NETSTAT command	–
NOTIFY	Sends a message to TSO/TSS users or CMS users	0
NOTRACE	Terminates a VTAM network trace	1
NPTAB	Changes the status of a user's NPF table	0/4
NRDRET	Restores all Non-Roll Delete messages for an OCS window	0
NSBRO	Creates and sends a general or specific broadcast	3
NSLOOKUP	Uses the name service to find the name or address of a host	–
NSPCONN DEFINE	Defines a NetSpy connection.	4
NSPCONN DELETE	Deletes a connection to a NetSpy system.	4
NSPCONN START	Starts a connection to a NetSpy system.	4
NSPCONN STOP	Stops a connection to a NetSpy system.	4
NTSDBMOD	Alters database records or session keep counts on the NTS database	4
NTSMOD	Alters session trace and logging parameters of active sessions	4
OBEYFILE	Invokes the IBM TCP/IP OBEYFILE command	–
OCSID	Sets or resets OCS window identifiers	0
OPNDST	Connects a specific terminal to management services	1/0
OPSYS	Passes a command to the operating system for execution	2
ORDER	Reorders your OCS window display from top to bottom	0
PAGE	Ensures that output messages start at the top of the OCS window	0
PF	Displays and sets terminal Function keys	0
PING	Sends echo requests to a remote host	–
PPO	Starts and stops the VTAM PPO interface	3
PROFILE	Displays or modifies a user profile	0/2
PROFILE EDS	Enables or disables event notification	0
PURGE	Purges and deletes current timer-initiated commands or NCL locks	0/2
RECONN	Reconnects the current terminal session with a disconnected region	0
REPALIAS	Replaces an alias name entry used NEWS	4
REPCCLASS	Replaces an existing SAW, RTM, Session or Resource class definition	4
REPLINK	Replaces or defines an DLT definition	3
REPLOGON	Replaces an existing application logon entry	4
REPLY	Issues a VTAM REPLY command	1
REPMODE	Replaces or defines an APPC Mode Control Table (MCT) entry	4
REPOPSET	Replaces or defines an APPC Option Set Control Table (OSCT) entry	4

<b>Command</b>	<b>Description</b>	<b>Auth</b>
REPTRANS	Replaces or defines an APPC Transaction Control Table (TCT) entry	4
REQMS	Sends data across the CNM interface	2
RETURN	Exits from any mode or function and returns to the primary menu	0
ROUTE	Sends a command string to a remote system	0
SAWARE	Controls NTS activity	4
SCRIPT	Starts or flushes an MAI-FS script procedure	0
SECUSER	Issues a command to a VM service machine	2
SHOW AIF	Displays AIF users	0
SHOW ALLOC	Displays datasets allocated by the ALLOC command	0
SHOW AOMABEND	Displays diagnostic information if AOM ABENDs	0
SHOW AOMSTAT	Displays AOM statistics	0
SHOW APPC	Displays the status of all or selected APPC conversations	0
SHOW ATF	Displays information about the ATF tables.	0
SHOW BRO	Displays the current general broadcast messages	0
SHOW BUFF	Displays the current system storage and buffer utilization	0
SHOW CNMTRACE	Shows active CNM trace requests	0
SHOW COMMANDS	Displays commands available to user or system	0
SHOW COMP	Displays 3270 datastream compression statistics	0
SHOW CONSOLES	Displays the consoles currently allocated for use by AOM	0
SHOW DEBUG	Displays NCL debug sessions	0/2
SHOW DEFALIAS	Displays one or more DEFALIAS entries	0
SHOW DEFCLASS	Displays NTS class definitions	0
SHOW DEFLINK	Displays current dynamic link definitions	0
SHOW DEFLOGON	Displays the current entries in the DEFLOGON table	0
SHOW DEFMODE	Displays APPC Mode Control Table (MCT) entries	0
SHOW DEFMSG	Displays the current DEFMSG delivery options	0
SHOW DEFOPSET	Displays APPC Option Set Control Table (OSCT) entries	0
SHOW DEFTERM	Displays terminal definitions (VOS3 only)	0
SHOW DEFTRANS	Displays APPC Transaction Control Table (TCT) entries	0
SHOW DNR	Displays parameters or statistics for the SOLVE Domain Name Resolver (DNR)	0
SHOW DOMAINS	Displays the domain information of connected systems	0
SHOW EDB	Displays information about external database connections	0
SHOW EDBSTAT	Displays statistics about currently defined EDB connections	0
SHOW EDBUSER	Displays information about EDB users	0

<b>Command</b>	<b>Description</b>	<b>Auth</b>
SHOW EDBUSTAT	Displays statistics about EDB users	0
SHOW EDS	Displays current Event Distribution Services PROFILE definitions	0
SHOW EPS	Displays a list of all endpoints known to this system	0
SHOW EQUATES	Displays the current EQUATE strings available to this user	0
SHOW EXEC	Displays the names of members in a procedure library (OS/VS only)	0
SHOW FTS	Displays the status of file transmissions	0
SHOW ISR	Displays ISR status information	0
SHOW ISRSTATS	Displays ISR statistics	0
SHOW LIB	Displays libraries which have been defined to the system	0
SHOW LICENSE	Displays the active licensing details and expiry dates	0
SHOW LINK	Displays the status of INMC or APPC links	0
SHOW LOCKS	Displays the status of all locks held within the system	0
SHOW LOGS	Displays the current status of the system activity logs	0
SHOW LSR	Displays LSR status information	0
SHOW LUTRACE	Displays the status of all LUTRACE requests	0
SHOW MAI	Displays information about MAI sessions for this user or all users	0
SHOW MAISTAT	Displays information about the status of MAI subtasks	0
SHOW MAP	Displays information about defined Mapping Services maps	0
SHOW MSGQ	Displays message queue depths	0
SHOW NCL	Displays the status of active NCL processes	0/2
SHOW NCLGLBL	Displays the names of any defined NCL global variables	2
SHOW NCLSTAT	Displays the status of NCL procedures currently in storage	0
SHOW NCLVARS	Displays information on variables in use by NCL procedures	0/4
SHOW NDB	Displays information about currently active or halted NDBs	0
SHOW NDBUSER	Displays a list of all users currently signed on to \$NDB databases	0
SHOW NETMCNTL	Displays the status of NETM connectivity (VOS3 only)	0
SHOW NETSPY	Displays the status of currently defined NetSpy connections.	0
SHOW NETSPY DEFINITIONS	Displays the owners of currently defined NetSpy connections.	0
SHOW NETSPY USERS	Displays the current users of the NetSpy interface.	0
SHOW NPF	Displays user's Network Partitioning Facility (NPF) tables	0
SHOW NPTAB	Displays the status of NPF resource tables	0
SHOW NRD	Displays the current queue of Non-Roll Delete Messages	0
SHOW NTS	Displays NTS resource or session information	0

<b>Command</b>	<b>Description</b>	<b>Auth</b>
SHOW NTSDBMOD	Displays currently executing NTSDBMOD & SHOW SKEEP processes	0
SHOW NTSSTATS	Displays NTS statistics	0
SHOW NTSUSER	Displays NTS users	0
SHOW OCS	Displays information about OCS users	0
SHOW PANELS	Displays management services panel queue information	0
SHOW PARM	Displays management services startup parameters	0
SHOW PATH	Displays current panel library path definitions	0
SHOW PAUSE	Displays the current PAUSE or WAIT status	0/2
SHOW PPIUSERS	Displays PPI user statistics	0
SHOW PPOSTAT	Displays PPO/SPO statistics	0
SHOW REPLY	Displays VTAM messages that require a reply	0
SHOW SCNT	Displays the current session count	0
SHOW SERVER	Displays the status of registered server processes	0
SHOW SESS	Displays the terminals that are in session	0
SHOW SKEEP	Displays the NTS session keep counts for historical sessions	0
SHOW SOCKETS	Displays information about the use of TCP/IP services	0
SHOW SSI EPS	Displays SSI EPS information	0
SHOW SNAMS	Displays SNA Management Services information	0
SHOW SSISTATS	Displays Subsystem Interface (SSI) statistics	0
SHOW SSITERMS	Displays a list of terminals attached to SOLVE SSI	0
SHOW SSIUSERS	Displays information about SSI users	0
SHOW STRACE	Displays NTS session trace activity	0
SHOW SUBSYS	Displays user subsystem status	0
SHOW SYSCONS	Displays a list of currently logged on operating system consoles	0
SHOW SYSPARMS	Displays the current SYSPARMS settings	0
SHOW TCPIP	Displays information about the use of TCP/IP services	0
SHOW TERM	Displays the terminals that are in session	0
SHOW TIMER	Displays current timer initiated commands	0
SHOW TIMEZONE	Displays current time zones and the system time zone offset	0
SHOW TNCTL	Displays a list of all defined TNCTL (TELNET) ports and their option settings	
SHOW TSO	Displays current TSO users	0
SHOW TSS	Displays current TSS users	0
SHOW UDB	Displays VSAM dataset information	0
SHOW UDBUSER	Displays NCL UDB user information	0
SHOW USERACCT	Displays status of user NCL cpu time accounting	0/4

Command	Description	Auth
SHOW USERS	Displays the current signed on users	0
SHOW VARTABLES	Displays information about VARTABLES	0
SHOW VMOP	Displays VMOPERATOR active sessions (VM only)	0
SHOW VSAM	Displays extended VSAM dataset information	0
SHOW XMIT	Displays the status of FTS Transmission Requests	0
SHOW XNFTRACE	Displays the status of all XNFTRACE requests (VOS3 only)	0
SHUTDOWN	Commences or cancels an orderly shutdown of the system	3
SIGNOFF	Signs off from a remote system	0
SIGNON	Signs on to a remote system	0/2
SPLIT	Opens or adjusts size of an OCS window	0
SPO	Starts and stops the VTAM Secondary Program Operator interface	3
SSI	Signs off or stops Subsystem Interface (SSI)	0/3
START	Starts executing an asynchronous NCL process	0
STATUS	Displays current general system status	0
STRACE	Starts and stops session trace activity	4
SUBMIT	Passes a command to a background environment for processing	0/2
SUBSYS	Defines, starts, stops and deletes subsystems	3
SUSLOGON	Suspends an entry or entries in the DEFLOGON table	3
SWAP	Swaps current logical windows	0
SYSCMD	Sends a command to the operating system	2
SYSLOG	Issues VMOPERATOR log browse commands (VM only)	2
SYSMON	Sends data to System Monitor in 3600/4700	1
SYSPARMS	Defines or changes system default values. This command is described in the <i>Management Services Administrator Guide</i> .	4/9
TCPIP MODIFY	Alters the current trace options setting	4
TCPIP QUIESCE	Stops TCP/IP services when all the sockets are closed	4
TCPIP START	Initiates TCP/IP services	4
TCPIP STOP	Terminates TCP/IP services	4
TELNET	Starts a Telnet connection	–
TERMINAL	Provides extended color and/or highlighting datastreams to terminals	0
TIME	Sets and displays the current date and time	0
TIMEZONE	Maintains time zone names and offsets	3
TITLE	Sets the title to be displayed on the top line of the OCS window	4
TNCMD	Sends a Telnet command on a connection to a remote host	–
TNCTL ADDPORT	Defines a TELNET port	

<b>Command</b>	<b>Description</b>	<b>Auth</b>
TNCTL DEFPORT	Defines a TELNET port	
TNCTL DELPORT	Deletes a TELNET port	
TNCTL REPPORT	Replaces a TELNET port	
TNDISC	Disconnects a Telnet connection	–
TNSEND	Sends data on a Telnet connection	–
TRACE	Initiates a VTAM network trace	1
TRACEROUTE	Traces a route taken by TCP/IP packets to a remote host	–
TRANSMIT	Requests a dataset transmission	0
UDBCTL	Controls the status of User DataBases (UDBs)	3/4
UNALLOC	Unallocates a closed dataset	0/3
V	Issues a VTAM VARY command	1
X	Exits from OCS screen mode	0
XLATE	Tests alias name translation	1
XNF	Removes all XNF connectivity (VOS3 only)	3
XNFTRACE	Initiates or terminates tracing of XNF connectivity (VOS3 only)	4
\$SPLC15U	Displays and modifies SNMP objects	

---

# Glossary

This glossary defines the terms and abbreviations commonly used with Management Services.

It also includes references to terms used in an IBM environment and any equivalent FUJITSU terms.

## **3270**

An IBM video display terminal. This is often used to refer to the entire range of 3270 terminals. When followed by a number (for example, 3270-5), a specific model is intended.

## **370/390**

This is an abbreviation for IBM's System 370 (S/370) or System 390 (S/390) architectures. It is often used to indicate any mainframe CPU that implements this architecture.

## **3705/3725/3745/3746**

An IBM front end communications processor (The Fujitsu equivalent is a CCP or 2806).

## **9526**

A Fujitsu video display terminal.

## **ACB (Access method Control Block)**

A control block that links an application program to an access method such as IBM's VTAM or VSAM.

## **ACB-sharing**

MAI's ability to use a single VTAM ACB for multiple sessions.

**Access Security Exit**

An installation-provided routine that may be used to replace the Management Services UAMS functions, partially or completely, allowing logon, logoff, and password maintenance requests to be passed to an external security system.

**ACF/VTAM (Advanced Communication Facility/VTAM)**

IBM's product implementation of SNA's SSCP or CP.

**Activity Log**

A system-maintained log that records all important activity for use in later problem determination.

**Alternate Index**

An alternative view of the data contained within a VSAM keyed dataset. The alternate index allows data to be retrieved using an alternate key in addition to the usual access through the primary key.

**AOM (Advanced Operation Management)**

A facility of SOLVE:Operations that manages and controls local and remote operating systems.

**AOMPROC**

The name given to an NCL procedure used to intercept messages from the screening table component of the SOLVE:Operations AOM facility to provide extended message processing.

**APF (Authorized Program Facility)**

Describes the special authorization level required within the operating system for certain applications.

**APPC (Advanced Program to Program Communications)**

An IBM-defined application level protocol which makes use of SNA's LU 6.2. It is an accepted industry standard for transaction processing between peer systems.

**APPL (Application Program)**

A VTAM term used to describe the definition that allows an application to use VTAM facilities.

**APPN (Advance Peer-to-Peer Networking)**

IBM's data communications support that routes data in a network between two or more APPC systems that do not need to be adjacent.

**ASN.1**

Abstract Syntax Notation One, defined by ISO 8824, is an abstract syntax used to describe data structures. It is used by Mapping Services to define data structures within Management Services.

**BCI (Batch Command Interface)**

A subcomponent of EIP that allows commands to be issued from batch jobs into a Management Services system.

**BER (Basic Encoding Rules)**

The transfer syntax used by Mapping Services to serialize data for transmission. It is defined by ISO 8825.

**BIND**

A VTAM term describing the action of logically linking one network resource with another network resource.

**Broadcast Services**

The message broadcasting function provided by Management Services.

**Build/Verify**

A semi-automatic method of adding or verifying a series or group of resource records, by retrieving data from the hardware and software in the live configuration.

**CAS (Common Application Services)**

CAS functions are a collection of NCL routines designed to facilitate program development.

**CICS (Customer Information Control System)**

An IBM licensed program that enables transactions entered at remote terminals to be processed concurrently by user-written application programs.

**Client**

A functional unit that receives shared services from a server.

**CNM (Communications Network Management)**

IBM term for its SNA management facilities.

**CNMPROC**

The name given to an NCL procedure used to intercept CNM records received across the VTAM CNM interface by the NEWS component of NetMaster for SNA.

**Command Partition**

A term associated with network partitioning that describes the group of network resources a user ID is authorized to reference with VTAM commands.

**Control Member**

A term associated with network partitioning that describes the list of resource table names applying to a user ID. This control member is referenced in the definition of USERID.

**CP (Control Point)**

A collection of tasks which provide directory and route selection functions for APPN.

**Cross-domain Resource (CDRSC)**

A VTAM term describing the definition of a network resource that is owned by VTAM in another domain.

**DBCS (Double Byte Character String)**

Refers to a mode of representation of data where each byte of data requires 16 bits rather than 8 bits as required by Single Byte Character String. DBCS is used for the implementation of Asian languages such as Japanese.

**Deferred Write**

A performance option for use with UDBs to minimize I/O by deferring the writing of records.

**DEFLOGON**

The term used to describe an application entry path to be supported by SOLVE:Access. The DEFLOGON command is used to define application access paths and their associated text strings.

**Dependent LU**

Any logical unit that is made active by a command from the host system over a data link.

**Dependent Processing Environment**

An NCL processing environment which is a child process to another NCL process and hence has its output delivered as input to some other NCL procedure.

**DOM (Delete Operator Message)**

A non-roll deletable message (NRD) can be deleted from a window only when a DOM is issued.

**Domain**

1. An SNA term describing a domain that consists of the set of SNA resources controlled by one common control point called an SSCP. In terms of implementation, an SSCP is the host access method (VTAM). An SNA network consists of one or more domains.
2. A VTAM term that describes a logical division of a network. Networks are divided into domains that are associated with the way they are controlled.
3. A term that describes any instance of Management Services that is running.

**Domain ID**

A 1 to 4 character mnemonic used as a unique identifier for a domain.

**Dynamic Allocation**

Assignment of datasets to a program at the time the program is executed rather than at the time the job is started.

**EASINET**

A component of SOLVE:Access. EASINET allows idle terminals to be brought under the control of SOLVE:Access and to be operated by installation-written NCL procedures that can provide a wide range of *front end* facilities to end-users of the network.

**EDBS (External Database Support)**

Facility allowing NCL to use DB2 databases.

**EDS (Event Distribution Services)**

A Management Services facility for notifying NCL procedures of events.

**EIP (External Interface Package)**

A facility that allows you to connect to, and issue commands on, a Management Services system from external sources such as TSO and BATCH jobs.

**ER (Explicit Route)**

The physical path between two network nodes. (SNA)

**ESDS (Entry Sequenced Data Set)**

A non-keyed VSAM dataset whose records are stored and retrieved in sequential order, and new records added to the end of the data set.

**Exit**

An installation-written routine that can be driven from a point within a program to provide data to the program, or perform additional processing relevant to that installation's specific requirements.

**Extended Datastream**

A 3270 datastream containing fields that utilize color and/or extended highlighting capabilities of the terminal.

**External Database Connection**

A term used to refer to connections from Management Services to the database which use the Call Attach Facility (CAF) to connect to DB2. NCL connections are connections to DB2 that utilize the Management Services connection. See also *Management Services Connection* and *NCL Connection*.

**External Database ID**

The ID of the external database as it is known to the operating system.

**FTS (File Transmission Services)**

A feature of Management Services which is used to transmit datasets between CPUs.

**Function Key**

A key on a terminal's keyboard which causes a panel to be completed. In the case of 3270, this term also applies to the ENTER key (the same behavior can be achieved on a 6530).

Also called Program Function (or PF) keys.

**ID**

Identification

**IMS (Information Management System)**

IBM's database/data communication (DB/DC) system that provides a hierarchical database manager and transaction processing system.

**Independent LU**

A logical unit that does not receive an active LU over a link. Can act as a primary LU or secondary LU, and can have one or more LU-LU session at a time.

**Initiator**

The component of FTS which schedules transmission of a dataset.

**INMC (Inter-Management Services Connection)**

This facility allows systems running in a network to communicate with each other, providing general-purpose data transfer within the network.

**Internet**

A wide area network connecting networks all over the world. Uses TCP/IP as the standard for information transmission.

**I/O**

Input/Output.

**IS**

Information System.

**ISR (Inter-System Routing)**

Provides centralized control at the system level through INMC.

**KSDS (Key Sequenced Data Set)**

A VSAM dataset whose records are directly accessed by a user-supplied key.

**LAN (Local Area Network)**

A computer network within a limited geographical area. Is not subject to external regulations.

**Link**

A term used to describe a logical connection between two peer communications systems such as two Management Services systems. See also *INMC (Inter-Management Services Connection)*.

**LOGMODE**

A VTAM term used to describe a set of characteristics and protocols of a logical unit.

**Logon-path**

A path through which users of SOLVE:Access gain access to other VTAM application programs. Paths are defined and controlled by the DEFLOGON command.

**LOGPROC**

The name given to an NCL procedure used to process messages destined for the Management Services activity log.

**LSR (Local Shared Resources)**

A technique for buffering I/O to VSAM files called LSR pools. NCL supports this type of processing for User Databases (UDBs).

**LU (Logical Unit)**

SNA introduced the concept of the logical unit (LU). The LU is a type of SNA network-addressable unit (NAU) that provides protocols for end users to gain access to the network and to the functional components of the LUs.

**LU0**

An unconstrained SNA protocol that allows implementers to select any set of available protocol rules, as long as the two LUs are able to communicate with each other successfully according to the rules chosen. Therefore, all LU types are an implementation of LU Type 0.

**LU1**

A line-by-line or typewriter type terminal (for example 3767, 3770), using SNA protocols.

**LU2**

A 3270 type terminal using SNA protocols.

**LU3**

LU Type 3 was implemented to support printers with a different data stream format. LU Type 3 is used by printers attached to an IBM display cluster controller.

**LU4**

LU Type 4 was implemented so that office system products could transfer documents.

**LU6.2**

A protocol that serves as a port into an SNA network. LU6.2 defines a specific set of services, protocols, and formats for communication between logical processors. LU6.2 provides presentation services for presentation of data to the end user, transaction services for performing transaction processing on behalf of the end user and LU services for managing the resources of the LU.

**LU7**

An SNA protocol that is used by word-processing devices.

**MAI (Multiple Application Interface)**

A facility of SOLVE:Access which is used to provide sessions with any number of other VTAM application programs from one terminal.

**MAI/EF (MAI/Extended Function)**

A SOLVE:Access facility which provides an extension to NCL to support session scripts which allow an NCL procedure to control the application and terminal session flow. MAI/EF also includes the Session Replay Facility (SRF) which allows recording and replay of session scenarios, and Screen Image Services (SIS) which allows recording of screen images for later retrieval or to send to another user.

**MAI-FS (MAI Full Screen)**

A SOLVE:Access facility that allows a single terminal to be used to provide full screen access to any number of other applications. The user may 'jump' from one application to another using designated 'jump' keys on the keyboard, or special command strings.

**MAI-OC (MAI Operator Control)**

A Management Services facility that allows an operator in OCS to have LU Type-1 sessions with many other applications from an OCS window. When used in conjunction with MSGPROC NCL procedures this can provide automated central monitoring and operation of multiple applications from the one operator console.

**Management Services**

This the central core of functions and service routines within the system. It supports all of the NetMaster, NetSpy, and SOLVE products.

**Management Services Connection**

A Management Services connection is a communication link from Management Services to the external database. It is started, stopped, defined, and deleted using the EDB command. A Management Services connection must be defined and started before opening an NCL connection. See also *NCL Connection*.

**Mapping Services**

A facility of Management Services that enables programmers to define complex data structures for use by applications.

**MDS-MU (Multiple Domain Support-Message Unit)**

The message unit used in data transmission between management applications in SNA networks.

**MDO (Mapped Data Object)**

Any data item that can be represented as a continuous string of bytes in storage.

**Message Partition**

A term associated with network partitioning that describes the group of network resources for which a user ID will receive unsolicited (PPO) VTAM messages.

**MIB (Management Information Database)**

Any database that provides information about the structure and capabilities of a management application.

**Modify Interface**

A means of communicating with an application program from the system console in OS/VS systems. The MODIFY command, abbreviated to F, avoids having an outstanding REPLY at the system console. Management Services supports the use of the MODIFY command.

**MSGPROC**

An NCL procedure used to intercept and process messages destined for a user's Operator Console Services (OCS) window.

**MSP**

An operating system for large scale Fujitsu systems.

**NAU (Network Addressable Unit)**

In SNA, a logical unit, a physical unit, or a system services control point. The NAU is the origin or destination of information transmitted by the path control network.

**NCL (Network Control Language)**

The interpretive language that allows logical procedures (programs) to be developed externally to Management Services and then executed by Management Services on command. NCL contains a wide range of logic, built-in functions and arithmetic facilities which can be used to provide powerful monitoring and automatic control functions.

**NCL Connection**

An NCL connection is a communication link from an NCL procedure to the external database. An NCL connection is opened and closed with the &EDB verb. A Management Services connection must be defined and started before opening an NCL connection. See also *Management Services Connection*.

**NCL Procedure**

A member of the procedures dataset comprising NCL statements and Management Services commands. The NCL statements and other commands are executed from an EXEC or START command specifying the name of the procedure.

**NCL Process**

The NCL task that is invoked, usually by a START command to execute one or more associated procedures. Each NCL process has a unique NCL process identifier.

**NCL Processing Environment**

Provides the internal services and facilities required to execute NCL processes for the user, from its associated Management Services window.

**NCL Processing Region**

All users (real or virtual) have an NCL Processing Region associated with their user ID while logged on. This region provides all of the internal services needed to allow the user to have processes executed on their behalf.

**NCLID**

A 6-digit NCL process identifier which is unique within the system. It is used to identify a process for the purpose of communicating with that process.

**NCP (Network Control Program)**

This resides within and controls the operation of a communications controller. The NCP communicates with VTAM.

**NCPView**

A component of NetMaster for SNA that allows monitoring of NCP configuration.

**NCS (Network Control Services)**

A facility of NetMaster for SNA that allows display and control of SNA network resources.

**NDB (NetMaster Database)**

NDBs are field-oriented databases in which data is stored and retrieved in named fields. They are designed for environments that have complex, high volume data storage and retrieval requirements.

**NEWS (Network Error Warning System)**

A facility of NetMaster for SNA which is used to provide network error and traffic statistics and error alert messages.

**NMINIT**

The NCL procedure automatically executed after system initialization has completed. It cannot contain commands that require VTAM facilities as it is executed before the primary ACB is opened. The procedure name can be changed by the installation.

**NMREADY**

The NCL procedure automatically executed once the primary ACB is open. It can contain commands that require VTAM facilities. The procedure name can be changed by the installation.

**NMVT (Network Management Vector Transport)**

A request/response unit (RU) that flows over an active session between a physical unit (PU) and a control point (CP).

**Node**

A connection point in a communications network.

**NPF (Network Partitioning Facility)**

A facility of Management Services that allows the range of resources which an operator can influence to be denied.

**NPF Control Member**

A member of the NPF dataset which defines a list of member names that are to be the resource tables for the associated user ID.

**NPF Resource Table**

A member of the NPF dataset that defines a group of network resource names. The resource names can be defined specifically or generically using wildcard characters. A resource table is addressed via a control member.

**NRD (Non-Roll Delete) Message**

A message that will not roll off an OCS window display until explicitly deleted. See *DOM*.

**NT 2.1**

Node Type 2.1. A node in an SNA network. It implements a peer-to-peer protocol and allows greater dynamics in network configuration, greater independence in session set up between partner LUs and reduced definitions. Same as PU type 2.1.

**NTS (Network Tracking System)**

A facility of NetMaster for SNA used to provide SNA session monitoring, dynamic online network tracing, accounting, and response time information in conjunction with diagrammatic representations of session partners.

**Object Services**

An object-oriented development environment used to define and maintain the application data and methods of SOLVE:Central products.

**OCS (Operator Console Services)**

A facility of Management Services that provides general operational control and an advanced operator interface to VTAM for network management.

**OS/390**

An IBM operating system.

**OSI (Open Systems Interconnection)**

A set of ISO standards for communication between computer systems.

**Packet**

The unit of data used in transmission.

**Panel Maintenance**

A facility of Management Services which allows users to generate and modify panel definitions used for presentation purposes by NCL procedures. In releases prior to Version 3.0, this function was known as Edit Services.

**Panel Services**

A facility of Management Services for displaying full-screen panel definitions.

**Panel Skip**

The ability to chain menu selection requests together without having to display intermediate selection panels.

**Password**

A 1- to 8-character string chosen by a user and linked to their user ID for security purposes. To gain access to the system a user must enter both their defined user ID and its associated password.

**PDS (Partitioned DataSet)**

A type of dataset format that supports named data segments in the one physical dataset.

**PFK (Program Function Key)**

See *Function Key*.

**PIU (Path Information Unit)**

An SNA packet.

**PLU (Primary Logical Unit)**

Relates to SNA. A type of LU that is usually used by the application programs in a host. It refers to the BIND sender for a session. See also *Primary and Secondary*.

**PPI (Program-to-Program Interface)**

PPI is a general-purpose facility which allows programs, written in any language, to exchange data.

**PPO (Primary Program Operator)**

A VTAM term that describes a facility of VTAM that allows unsolicited network messages to be delivered to an application program, such as Management Services, for processing.

**PPOPROC**

The name given to the NCL procedure used to process unsolicited VTAM (PPO) messages.

**Preload**

A term applied to NCL procedures which are loaded into the system before being required, to improve system performance.

**Primary Menu**

The first menu of an application.

**Primary and Secondary**

Primary and secondary are SNA terms for describing the LU's role when the session is established. The primary LU sends the BIND request that causes the session to be established, and the secondary LU receives the BIND request. Rules defined in the BIND request determine which of these is the first speaker in the exchange of information.

**PSM (Print Services Manager)**

PSM is a facility of Management Services which simplifies the control of the physical printing of reports on JES or network printers.

**PU (Physical Unit)**

The part of a control unit or cluster controller which fulfils the role of an SNA-defined physical unit. Each node (a logical grouping of hardware) in an SNA network is addressed by its PU. There are 4 types of nodes or PU in an SNA network: PU-T5, PU-T4, PU-T2, PU-T1. A PU is a type of NAU. (See *NAU (Network Addressable Unit)*).

**PU Type 1**

A type of Physical Unit or Node in an SNA network. Consists of a terminal (such as an IBM 3278).

**PU Type 2**

A type of Physical Unit or Node in an SNA network. Consists of a cluster controller (such as an IBM3274, 3276, 3770 or 3790).

**PU Type 4**

A type of Physical Unit or Node in an SNA network. Consists of a communications controller (such as an IBM 3704, 3705, 3725 or 3745).

**PU Type 5**

A type of Physical Unit or Node in an SNA network. Consists of a host computer system (such as an IBM30xx, S/370 or 43xx, running VTAM).

**PVC**

X.25 Permanent Virtual Circuit.

**Report Writer**

A facility of Management Services which allows the creating and customizing of report definitions.

**Request Unit (RU)**

A message unit in an SNA network that contains control information such as a request code, or function management headers, end-user data, or both.

**Reserved word**

The term given to a token that will terminate an input expression if found unquoted outside the topmost parenthesis level. In the context of a particular verb statement the verb keywords are reserved words. A reserved word has special meaning for the current statement only, and different statements have different reserved words.

**Resource Table**

A term associated with NPF that describes a list of resource names or generic resource names that define a command or message partition.

**Response Unit (RU)**

A message unit in an SNA network that acknowledges a request unit.

**Return Code**

A code returned from the system that indicates the success or failure of the task performed.

**ROF (Remote Operator Facility)**

A facility of Management Services that allows an operator to sign on to a remote location, execute commands and have the results returned.

**RTM (Response Time Monitor)**

A facility provided by IBM's 3x74 control units to monitor end-user response times. NEWS can interpret this data .

**SAW Data (Session Awareness Data)**

Network management data supplied by VTAM and processed by NTS.

**SDLC (Synchronous Data Link Control)**

A discipline for managing information transfer over a communications link.

**Sequence Number**

A number assigned to each message exchanged between a VTAM application program and a logical unit. Values increase by one throughout the session, unless reset by the application program using an STSN or CLEAR command.

**Server**

A process designed to serve the data to a client, or request process, for one or more users.

**Session Name**

A name assigned to a workstation or session to permit it to receive messages or share resources.

**SIS (Screen Image Services)**

A part of the MAI/EF facility of SOLVE:Access which provides the ability to record screen images for later retrieval or to send to another user.

**SIS (Sequential Insert Strategy)**

A technique that governs the insertion rule for data in VSAM KSDS. Normally used when ascending keys are being added to a dataset, to help in efficient use of space within the dataset.

**SLU (Secondary Logical Unit)**

(SNA) A type of LU that is usually used by the end-users at the terminals or by programs which reside in the peripheral node. See also *Primary and Secondary*.

**SMF (System Management Facility)**

An optional control feature of OS/VS that provides the means for gathering and recording information that can be used to evaluate system usage.

**SMP (System Modification Program)**

An IBM program used to install software on OS/VS1 and OS/VS2 systems.

**SNA (Systems Network Architecture)**

This term describes the logical structure, formats, protocols, and operational sequences for transmitting communication data through the communication system (Fujitsu equivalent is FNA). A set of standards that allows the integration of all the different IBM hardware/software products into a universal network. Introduced in 1974.

**SNI (SNA Network Interconnection)**

The connection of independent SNA networks using gateways.

**SNMP (Simple Network Management Protocol)**

An Internet standard for network management.

**SPO (Secondary Primary Operator)**

A VTAM facility that allows solicited network messages to be delivered to an application program.

**SRF (Session Replay Facility)**

A part of the MAI/EF facility of SOLVE:Access which provides the ability to record and playback terminal session scenarios.

**SSCP (System Services Control Point)**

A part of VTAM and the focal point of SNA networks. It controls general management of each domain.

**Structured field**

Representation of user ID attribute information exchanged between Management Services and its security exit.

**Subtask**

A unit of work that is established by a main task and is displaceable by the operating system.

**SVC**

X.25 Switched Virtual Circuit.

**SYSPARMS**

System parameters—values that affect Management Services system capabilities. Most SYSPARMS can be modified dynamically.

**TCP/IP (Transmission Control Protocol/Internet Protocol)**

A set of communications protocols that support peer-to-peer connectivity functions for both LANs and WANs.

**TSO (Time Sharing Option)**

An IBM product that allows terminal operators to interact directly with computer resources and facilities. Used mainly by application and system programmers. (Fujitsu equivalent is TSS).

**UAMS (Userid Access Maintenance Sub-system)**

The security component of Management Services that supports the definition of authorized users and their associated function and privilege levels.

**UCS (Universal Character Set)**

A printer feature that permits the use of a variety of character sets.

**UDB (User Data Base)**

1. UDB file access method layer allowing file access from NCL.
2. A term used to identify VSAM datasets to which NCL procedures may have access using the &FILE verb (GET, PUT, ADD, and DEL options).

**User ID**

Defines the function and privilege level to which a specific user is entitled when they sign on to the system. It is associated with a secret password to prevent use by unauthorized personnel. This definition is stored in the UAMS dataset or on an external security system.

**User Services**

A facility of Management Services that allows the creation of a range of specific procedures for different users, or classes of user, if required.

**USS (Unformatted System Services)**

A VTAM term that describes a facility that translates an unformatted command such as LOGON or LOGOFF, into a field formatted command for processing by formatted system services. Applies to terminals before connection to an application.

**Verb**

The term given to a stand-alone statement in an NCL program. NCL *verbs* cause actions to occur. There are different types of verbs, some that dictate the flow of processing and logic, others that fetch information for the procedure to process and others that cause data to flow to external targets.

**VFS (Virtual File Services)**

The VSAM dataset, used by many facilities as a database.

**VM (Virtual Machine)**

A superset operating system that allows other operating systems to run as if they each had their own machine.

**VOS3**

A Hitachi operating system comparable to IBM's MVS.

**VR**

(Session) Virtual Route.

**VSAM (Virtual Storage Access Method)**

A method for processing data files that utilizes relative, sequential, and addressed access techniques.

**VTAM (Virtual Telecommunications Access Method)**

A suite of programs that control communication between terminals and application programs.

**VTAM-G**

Fujitsu's functional equivalent of IBM's ACF/VTAM.

**WAN (Wide Area Network)**

A network that provides communication services to a large area, for example, a telephone network.

**Wildcard**

The term used to describe the character used (usually an asterisk) when defining resources generically—no specific matching character is required in the wildcard character position.

**X.25**

An international recommendation regarding the connection of computer equipment to public data networks.

**XNF**

A Hitachi network access method for OSI networks.

**XSP**

A Fujitsu operating system.

**z/OS**

An IBM operating system.

---

# Index

## Symbols

\$BSCALL 7-3  
\$CMDENT 5-6  
\$PSCALL 9-2  
&INTCMD facility 5-2  
&INTCMD verb 4-14  
&PPI verb 10-2

## A

abbreviating commands 3-9  
    in MAI-OC 5-7  
acknowledging receipt of broadcast 7-15  
activity log, using with OCS 4-9  
Advanced Program-to-Program  
    Communication. *See* APPC  
AOM START command 11-6  
AOM STOP command 11-6  
APPC links  
    displaying status 8-7  
    starting 8-7  
    stopping 8-8  
    using with Management Services  
        to communicate 8-2  
        to link 8-7  
ASCB address, using PPI 10-11  
AT command 4-11  
AUTOHOLD command 4-3

## B

background processes  
    issuing commands in 4-10  
    logger 4-10  
    monitor 4-10  
    server 4-10  
    system 4-10  
broadcast services 7-2  
    accessing 7-3  
    broadcasts  
        acknowledging receipt 7-15  
        entering text 7-14  
        listing 7-4  
        receiving 7-15  
        reviewing 7-13  
        types 7-2  
    dynamic broadcasts  
        fields  
            Retain Broadcast? 7-13  
        sending 7-13  
    system groups  
        adding 7-5  
        resource definitions 7-5  
broadcast services panels  
    Group Definition 7-5  
    List Broadcasts 7-4  
    Primary Menu 7-3  
    Resource Definition 7-7  
    Resource List 7-6  
    Review Broadcasts 7-13  
    Send Menu 7-14

- broadcasts
  - listing 7-4
  - receiving 7-15
  - receiving 7-13
  - text 7-14

## C

- categories, NETINFO 2-15
- changing your password 2-5
- CLEAR command 3-9, 4-4
- CNMNETM module 10-5
- CNMNETV module 10-5
- command line in OCS window 3-3
- commands
  - abbreviating 3-9
    - MAI-OC 5-7
  - authority levels 3-9, A-2
  - concatenated 3-9
    - preventing 3-10
  - execution, simplifying 6-4
  - issuing
    - from a remote system 6-4
    - in background processes 4-10
    - in IMS applications 5-8
    - in OCS 4-10
    - using MAI-OC 5-7
    - using ROF 6-4
  - list A-2
  - partitioning 4-17
  - renaming 3-11
  - restricting 4-17
  - retaining on the command line 3-11
  - routing 4-11
  - setting authority levels 3-9
  - stack 3-10
  - summary table A-2
  - summary, SYSCMD 11-6
  - timer-initiated 4-11
    - concatenating 4-14
    - deleting automatically 4-13
    - deleting manually 4-12
    - displaying status 4-12
    - limiting execution 4-13
    - redirecting control 4-13
    - routing 4-14
    - using in OCS 3-8
  - commands, specific
    - AOM START 11-6
    - AOM STOP 11-6
    - AT 4-11

- AUTOHOLD 4-3
- CLEAR 3-9, 4-4
- CS- 3-10
- CS+ 3-10
- EQUATE 3-11, 5-7, 6-4
- EVERY 4-11
- EXEC 4-14, 4-16
- K 4-4
- LINK 8-3
- LINK RESET 8-4
- LOCK 2-7
- MAINT 5-5
- MAILOGON 5-2
- MAISEND 5-6, 5-8
- OCSID 3-4
- ORDER 4-4
- PROFILE 3-4, 4-3, 4-18, 11-6
- PROFILE CMDKEEP 3-11
- PURGE 4-8, 4-12
- REPLY 4-6
- ROUTE 4-19, 6-4
- SHOW AOMABEND 11-6
- SHOW AOMSTAT 11-6
- SHOW CONSOLES 11-4, 11-6
- SHOW MAI 5-3, 5-8
- SHOW NCL 3-3
- SHOW NP 4-17, 4-19
- SHOW NPTAB 4-17
- SHOW TIMER 4-12, 4-13
- SIGNOFF 4-8, 6-6
- SIGNON 6-3, 6-5
- START 4-14, 4-16
- STATUS 11-6
- SUBMIT 4-10, 11-6
- SYSCMD 11-6
- SYSPARMS 11-6
- TITLE 3-4
- communicating between systems
  - using APPC 8-2
- concatenating commands 3-9
  - timer-initiated 4-14
- confirming printing 9-6
- consoles
  - displaying status of console pool 11-4
  - locking 11-3
  - master console commands 11-3
  - SHOW CONSOLES display 11-4
  - simulating command issue 11-4
- contention delay interval, changing 4-4
- control characters (SCS) 5-9
- conventions, user actions 2-2
- conversation function keys 3-6

copying display lines to command line  
3-11  
CS- command 3-10  
CS+ command 3-10

## D

data buffers  
controlling 10-19  
purging 10-23  
receiving 10-21  
sending 10-19  
datastreams, SCS control characters 5-9  
debugging codes, PPI 10-31  
default function keys 3-6  
DEFMSG table 4-5  
displaying status of console pool 11-4  
dynamic broadcasts  
fields  
    Retain Broadcast? 7-13  
sending 7-13

## E

ECB, waiting 10-24  
ENTER key, redefining 3-8  
EQUATE command 3-11, 5-7, 6-4  
errors  
    correcting, NPF 4-18  
    tracing cause, PPI 10-29  
EVERY command 4-11  
EXEC command 4-14, 4-16

## F

function keys  
    conversational 3-6  
    default 3-6  
    defining as NCL procedures 3-8  
    immediate 3-6  
    prefix 3-6  
    setting as ENTER keys 3-8  
    suffix 3-6  
    using in OCS 3-5  
functions  
    Management Services 2-9

## G

general broadcasts 7-2  
getting started 2-1

## H

holding limit, changing 4-3

## I

immediate function keys 3-6  
information database, using in OCS 4-9  
INMC links 8-3  
    domain information 8-5  
    resetting 8-4  
    starting 8-3  
    status 8-4  
    stopping 8-4  
    troubleshooting 8-6  
    using with Management Services 8-3  
Inter-Management Services  
    Communication. *See* INMC

## J

JES2, MAI-OC session 5-8  
JES3, MAI-OC session 5-8

## K

K command 4-4  
keyboard  
    lock 5-8  
    locked condition, MAI-OC 5-7  
    unlock 5-8

## L

LINK command 8-3  
LINK RESET command 8-4  
listing  
    broadcasts 7-4  
    resource definitions 7-5  
LOCK command 2-7

- locking
    - a console 11-3
    - your terminal 2-7
  - logging off
    - MAI-OC 5-4
    - Management Services 2-8
  - logging on
    - Management Services 2-3
    - multiple sessions 2-4
    - to another application using MAI-OC 5-2
  - logical unit (LU)
    - pool 5-3
    - selecting 5-3
    - specifying a terminal 5-3
  - LU.1 protocol for MAI-OC session 5-2
- M**
- MAIDISC command 5-4, 5-11
  - MAIINT command 5-5
  - MAILOGON command 5-2
  - MAI-OC 5-2
    - issuing commands 5-7
      - abbreviating 5-7
      - IMS applications
        - multi-segment messages 5-8
        - in IMS applications 5-8
        - keyboard locked condition 5-7
      - logging off 5-4
      - logging on to another application 5-2
      - LU.1 protocol 5-2
      - receiving
        - data from an application 5-6
        - messages 5-6
      - sending data to an application 5-6
        - new line character 5-6
      - session
        - acting as master console 5-2
        - creating an identifier 5-2
        - establishing 5-2
        - interrupting 5-5
        - JES2 or JES3 5-8
        - listing 5-3
        - lost terminal condition 5-4
        - ownership 5-6
        - terminating 5-4
        - SNA LU-Type 1 5-8
    - MAISEND command 5-6, 5-8
    - Managed Object Development Services.
      - See* MODS
    - Management Services 1-2
      - accessing 2-2
      - functions 2-9
      - getting started 2-1
      - locking your terminal 2-7
      - logging off 2-8
      - logging on 2-3
        - multiple sessions 2-4
      - online help 2-12
      - opening and closing windows 2-12
      - operating environments 1-6
      - PPI facilities 10-2
      - security, changing user details 2-7
      - selecting functions 2-9
      - services
        - application development
          - services 1-4
        - broadcast services 1-4
        - MODS 1-4
        - NCL 1-4
        - OCS 1-2
        - report writer 1-4
        - security 1-3
        - splitting windows 2-11
        - supported terminals 1-6
        - swapping windows 2-12
        - working in two windows 2-11
    - master console commands, entering 11-3
    - messages
      - controlling presentation speed 4-2
      - holding limit 4-3
      - network warning 4-5
      - NRD
        - deleting 4-8
        - hiding 4-7
        - receiving 4-7
        - restoring hidden 4-8
      - PPO
        - intercepting and processing 4-6
        - receiving 4-5
        - undeliverable 4-5
      - receiving in ROF 6-5
      - ROF message ID 6-5
      - stopping flow in OCS 4-2
      - tables, changing status 4-18
      - unsolicited
        - changing severity level 4-18
        - receiving 4-5
      - unwrapping 4-4
      - VTAM
        - replying to 4-6
        - restricting 4-18
    - monitoring restricted resources 4-17

Multiple Application Interface-Operator Console. *See* MAI-OC

multiple session logon 2-4

multi-segment messages, sending to IMS applications using MAI-OC 5-8

## N

NCL procedures

accessing PPI facilities from 10-3

defining to function keys 3-8

executing 4-14

concurrently 4-15

from another NCL procedure 4-16

serially 4-15

nesting 4-16

slave procedures 4-16

starting 4-14

advantages 4-16

NETINFO

Browse Utility File 2-14

information categories 2-15

NetMaster and SOLVE products 1-5

Network Control Language. *See* NCL

network partition tables, displaying 4-17

Network Partitioning Facility. *See* NPF

network warning messages 4-5

Non-Roll Delete messages. *See* NRD messages

NPF

errors, correcting 4-18

restricting

commands 4-17

resource monitoring 4-17

unsolicited VTAM messages 4-18

using with ROF 4-19

NRD messages

associated with ROF sessions 4-8

deleting 4-8

hiding 4-7

NRD queue 4-7

receiving 4-7

restoring hidden 4-8

## O

OCS

accessing 3-2

activity log 4-9

clearing the OCS window 4-4

command

authority levels 3-9

help 2-13

stack 3-10

commands 3-8

issuing 4-10

contention delay interval 4-4

controlling message presentation speed 4-2

copying display lines to command line 3-11

cursor-sensitive help 2-13

executing NCL procedures 4-14

fullscreen mode 3-4

function keys 3-5

redefining as ENTER 3-8

information database 4-9

message presentation speed

AUTOHOLD option 4-2

HOLD option 4-2

message queue holding limit 4-3

NETINFO help 2-13

NRD queue 4-7

online help 2-13

receiving unsolicited messages 4-5

redefining ENTER key 3-8

renaming commands 3-11

restricting resource monitoring 4-17

ROF 6-2

routing commands 4-11

running multiple windows 3-4

setting window IDs 3-4

splitting the screen 3-4

timer-initiated commands 4-11

unwrapping messages 4-4

window layout 3-2

command line 3-3

operating mode indicator 3-3

roll delete area 3-3

roll-delimiter line 3-4

time display 3-4

title line 3-4

OCS commands

MAIDISC 5-11

OPSYS 5-11

- OCSID command 3-4
- online help
  - accessing 2-12
  - in OCS 2-13
  - types 2-12
- operating
  - environments 1-6
  - mode indicator, OCS window 3-3
- Operator Console Services. *See* OCS
- OPSYS command 5-11
- ORDER command 4-4

**P**

- panel skipping 2-10
- panels
  - broadcast services
    - Group Definition 7-5
    - List Broadcasts 7-4
    - Primary Menu 7-3
    - Resource Definition 7-7
    - Resource List 7-6
    - Review Broadcasts 7-13
    - Send Menu 7-14
  - NETINFO
    - Browse Utility File 2-14
  - PSM
    - Browse Output 9-4
    - Confirm Printer 9-6
    - Output Queue 9-4
    - Primary Menu 9-3
    - Print Request 9-5
    - Printer List 9-7
  - UAMS
    - Primary Menu 2-5
    - User Password Maintenance 2-6
- partitioning commands 4-17
- passwords
  - changing 2-5
  - expired 2-6
  - forgotten 2-6
- PPI 10-2
  - accessing
    - from Management Services 10-2
    - from NCL procedures 10-3
    - from other programs 10-5
  - checking status 10-9
  - CNMNETM module 10-5
  - CNMNETV module 10-5
  - controlling
    - data buffers 10-19
    - receiver programs 10-10
  - data buffers 10-19
    - controlling 10-19
    - purging 10-23
    - receiving 10-21
  - debugging codes 10-31
  - making calls 10-5, 10-8
  - obtaining
    - ASCB and TCB addresses 10-11
    - unique sender or receiver ID 10-25
  - receiver programs
    - checking status 10-10
    - controlling 10-10
    - deactivating 10-14
    - defining 10-12
    - deleting active 10-16
    - initializing 10-12
    - receiving information from 10-27
  - request codes 10-5
  - sender and receiver IDs 10-7
  - sending a generic alert to Management Services 10-17
  - tracing cause of error 10-29
    - debugging codes 10-31
  - variables
    - system 10-3
    - user 10-4
  - waiting on an ECB 10-24
- PPO messages
  - intercepting and processing 4-6
  - receiving 4-5
  - undeliverable 4-5
- PPOPROC 4-5
- PPOPROC, PPO messages 4-6
- prefix function keys 3-6
- preventing command concatenation 3-10
- primary menu broadcasts 7-2
- Primary Program Operator. *See* PPO
- print
  - queue 9-3
  - request output 9-4
- Print Services Manager. *See* PSM
- printer
  - entries
    - listing 9-3
    - modifying 9-5
- printing, SCS control characters 5-9
- problem determination, INMC 8-6
- PROFILE command 3-4, 4-3, 4-18, 11-6
  - CMDKEEP operand 3-11

Program to Program Interface. *See* PPI

## PSM

- accessing 9-2
  - confirming printing 9-6
  - displaying
    - print request output 9-4
  - facilities 9-2
    - print control 9-2
    - print spooling 9-2
    - printer definitions 9-2
  - listing printer entries 9-3
  - modifying a printer entry 9-5
  - panels
    - Browse Output 9-4
    - Confirm Printer 9-6
    - Output Queue 9-4
    - Primary Menu 9-3
    - Print Request 9-5
    - Printer List 9-7
  - selecting a printer 9-6
- PURGE command 4-8, 4-12

## R

receipt of broadcast, acknowledging 7-15

receiver

ID

- specifying in PPI 10-7
- unique, using PPI 10-25

programs

- checking status 10-10
- controlling, using PPI 10-10
- deactivating 10-14
- defining 10-12
- deleting 10-16
- initializing 10-12
- receiving information from 10-27

Remote Operator Facility. *See* ROF

renaming commands 3-11

REPLY command 4-6

request codes, PPI 10-5

Request Parameter Block. *See* RPB

resource definitions

- adding 7-5
- types 7-5

resources, monitoring restricted 4-17

restoring NRD messages 4-8

restricting commands 4-17

retaining commands on the command line 3-11

## ROF

- benefit, maximum 6-2
- inactive link 6-3
- issuing commands 6-4
- receiving messages 6-5
- restarting a session 6-3
- signing off 6-6
- signing on 6-3
- using
  - in OCS 6-2
  - NRD messages 4-8
  - with NPF 4-19

roll delete area, OCS window 3-3

roll-delimiter line, OCS window 3-4

ROUTE command 4-19, 6-4

routing timer-initiated commands 4-14

RPB, constructing 10-5

## S

screens

- opening and closing 2-12
- splitting 2-11
- swapping 2-12

SCS character support 5-9

security

- changing user details 2-7
- locking your terminal 2-7
- passwords
  - changing 2-5
  - expired 2-6
  - forgotten 2-6

selecting functions 2-10

sender ID

- specifying in PPI 10-7
- unique, using PPI 10-25

sending 10-19

- data buffers using PPI 10-19
- data to an application using MAI-OC 5-6
- dynamic broadcasts 7-13
- generic alert to Management Services PPI 10-17

- services
  - Management Services
    - application development
      - services 1-4
    - broadcast services 1-4
    - OCS 1-2
    - report writer 1-4
    - security 1-3
- session
  - identifier, creating 5-2
  - protocols 5-8
  - specifying a terminal 5-3
- sessions
  - concurrent 2-4
  - JES 5-11
  - multiple 2-4
- setting
  - command authority levels 3-9
  - window IDs 3-4
- SHOW AOMABEND command 11-6
- SHOW AOMSTAT command 11-6
- SHOW CONSOLES command 11-4, 11-6
- SHOW MAI command 5-3, 5-8
- SHOW NCL command 3-3
- SHOW NP command 4-17, 4-19
- SHOW NPTAB command 4-17
- SHOW TIMER command 4-12, 4-13
- signing off, ROF 6-6
- signing on, ROF 6-3
- SIGNOFF command 4-8, 6-6
- SIGNON command 6-3, 6-5
- simulating command issue 11-3
- skipping panels 2-10
- splitting
  - OCS window 3-4
  - screens 2-11
  - windows 2-11
- START command 4-14, 4-16
- starting
  - APPC links 8-7
  - INMC links 8-3
  - NCL procedures, advantages 4-16
- STATUS command 11-6
- stopping
  - APPC links 8-8
  - INMC links 8-4
  - message flow, in OCS 4-2
- strike-over masks 5-11
- SUBMIT command 4-10, 11-6
- suffix function keys 3-6
- supported terminals 1-6
- swapping between windows 2-12
- SYSCMD command 11-6
- SYSCMD facility
  - AOM command summary 11-6
  - entering master console commands
    - 11-3
    - in OS/390, z/OS, MSP, and VOS3
      - 11-3
      - in VM 11-5
    - locking a console 11-3
    - overview 11-2
    - simulating command issue 11-4
    - status of console pool 11-4
- SYSPARMS command 11-6
- system groups, broadcast services
  - adding 7-5
  - resource definitions 7-5

## T

- tables
  - changing message status 4-18
  - displaying network partitioning 4-17
- TCB address, using PPI 10-11
- terminals, locking 2-7
- terminating sessions
  - JES, using MAIDISC 5-11
  - MAI-OC 5-4
- time display, OCS window 3-4
- timer commands, displaying status 4-12
- timer-initiated command executions 4-13
- TITLE command 3-4
- title line, OCS window 3-4
- tracing cause of error, PPI 10-29, 10-31

## U

### UAMS

- changing
  - user details 2-7
  - your password 2-5
- panels
  - Primary Menu 2-5
  - User Password Maintenance 2-6
- passwords
  - changing 2-5
  - expired 2-6
  - forgotten 2-6

underscore characters, changing 3-4

unwrapping OCS messages 4-4

User Access Maintenance Subsystem. *See*  
UAMS

user action conventions 2-2

user broadcasts 7-2

## V

### verbs

- &INTCMD 4-14
- &PPI 10-2

### VTAM messages

- replying to 4-6
- restricting 4-18

## W

waiting on an ECB 10-24

wildcard character (\*) 4-17

### windows

- opening and closing 2-12
- splitting in OCS 3-4
- swapping 2-12
- working in two 2-11

