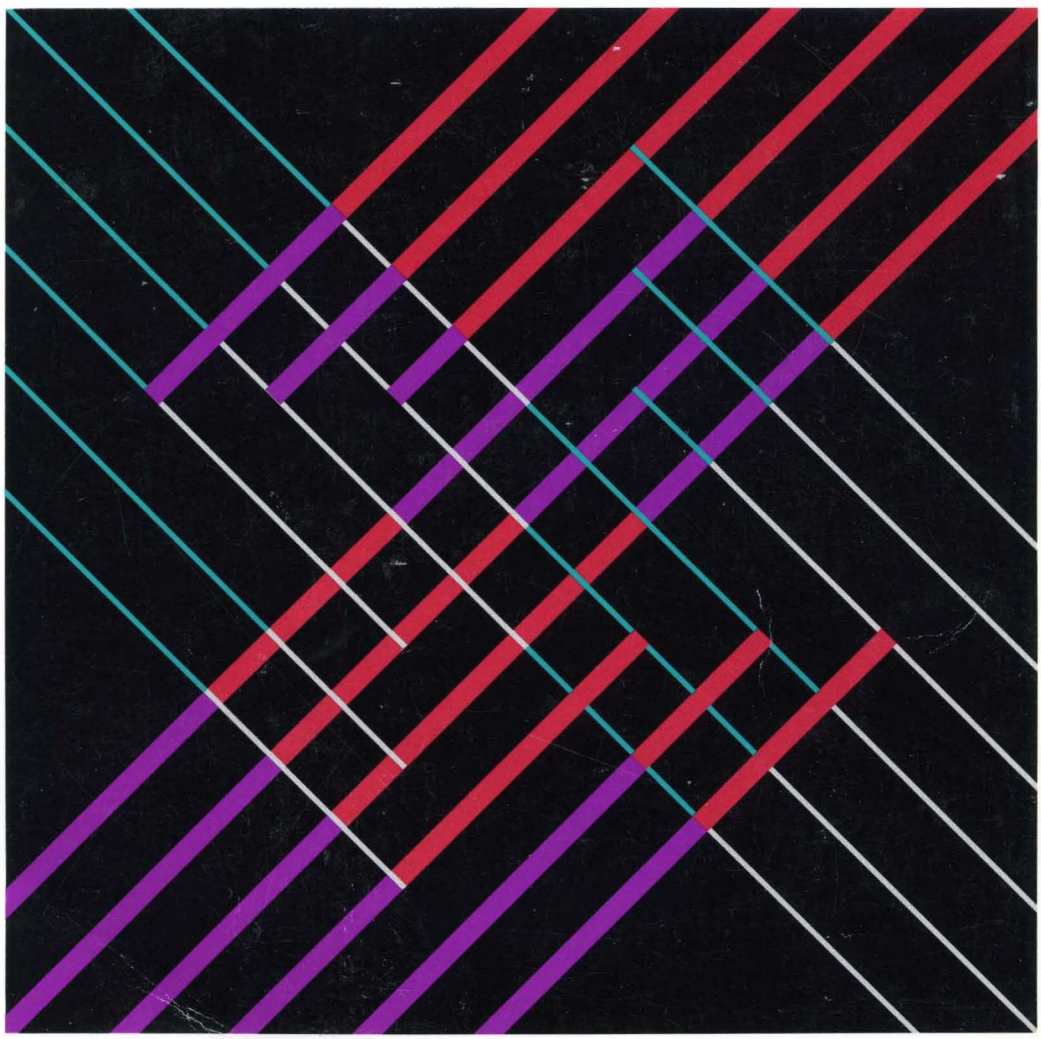
Multiprotocol Network Program

SC31-6692-01

Operations and Problem Management

Version 1 Release 3



Multiprotocol Network Program

SC31-6692-01

Operations and Problem Management

Version 1 Release 3

Note

Before using this document, read the general information under "Notices" on page xvii

Second Edition (September 1994)

This edition applies to:

Version 1, Release 3 of the IBM Multiprotocol Network Program
Models 120, 125, 140, 145, 170, and 175 of the IBM 6611 Network Processor

and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters. See the Summary of Changes for the changes made to this manual. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change. Make sure you are using the correct edition for the level of the product.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address below.

IBM welcomes your comments. A form for readers' comments is provided at the back of this publication. If the form has been removed, you may address your comments to:

International Business Machines Corporation
Department E15
P.O. Box 12195
Research Triangle Park, North Carolina 27709-9990
U.S.A.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Abbreviations, Glossary, Bibliography, and Index

Figures

Tables

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make them available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of the intellectual property rights of IBM may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
208 Harbor Drive, Building 1
Stamford, CT 06904 USA

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement.

This document is not intended for production use and is furnished as is without any warranty of any kind, and all warranties are hereby disclaimed including the warranties of merchantability and fitness for a particular purpose.

Trademarks

The following terms, denoted by an asterisk (*) at their first occurrence in this publication, are trademarks or registered trademarks of the IBM Corporation in the United States, other countries, or both:

AIX	NetView
Advanced Peer-to-Peer Networking (APPN)	Operating System/2
AIXwindows	OS/2
BookManager	Personal System/2
IBM	PS/2
Micro Channel	RISC System/6000

The following terms, denoted by two asterisks (**) at their first occurrence in this publication, are trademarks of other companies:

AppleTalk	Apple Computer, Inc.
Banyan	Banyan Systems, Inc.
Cylink	Cylink Corporation
DEC	Digital Equipment Corporation
DECnet	Digital Equipment Corporation
Digital	Digital Equipment Corporation
Intel	Intel Corporation
Internetwork Packet Exchange (IPX)	Novell, Inc.
Microsoft	Microsoft Corporation
Microsoft Windows	Microsoft Corporation

MS-DOS	Microsoft Corporation
UNIX	Novell Corporation
VINES	Banyan Systems, Inc.
VT100	Digital Equipment Corporation
Xerox	Xerox Corporation
Xerox Networking Systems (XNS)	Xerox Corporation
80386	Intel Corporation

About This Book

This book describes how to use the IBM* System Manager component of the Multiprotocol Network Program Version 1 Release 3. The Multiprotocol Network Program (*5648-016*) is the operating system that provides the bridging and routing functions for the IBM 6611 Network Processor (*6611*). The Multiprotocol Network Program is preloaded on the disk of the 6611. There are three components of the Multiprotocol Network Program:

- The base operating system performs routing and bridging, and supports the Simple Network Management Protocol (SNMP) network manager agent.
- The IBM Multiprotocol Network Program Configuration Program (*Configuration Program*) allows you to customize the 6611 functions and how the 6611 communicates with the network.
- The IBM Multiprotocol Network Program System Manager (*System Manager*) is a user interface that performs operation and system management tasks.

The *Operations and Problem Management* is comprised of the following information:

- **Chapter 1** provides an introduction to System Manager and shows an hierarchical flow of the System Manager panels.
- **Chapter 2** explains the different screen types, and contains information on understanding and working with the System Manager screens, and on using System Manager helps. This chapter also includes a description of the System Manager log and how to use it.
- **Chapter 3** explains how to access the 6611 locally and remotely and describes the access commands that are supported by the 6611.
- **Chapter 4** explains the operating tasks that can be performed using the System Manager. Examples of these tasks include performing file and diskette operations and requesting network statistical information.
- **Chapter 5** provides information on running system diagnostics. It includes instructions for obtaining traces, dumps, and performance data that you may need to generate for the IBM service personnel.
- **Chapter 6** explains how to use the System Manager to perform configuration.
- **Chapter 7** explains how to install software changes on the 6611 using the System Manager. It discusses how to initiate remote installation to one or multiple 6611s from a single control point. It also contains information about software vital product data.
- **Chapter 8** provides information about hardware vital product data.
- **Chapter 9** describes the commands available in the fast-path environment. It also explains the fast-path environment, the structure of the commands, and how to obtain help for the commands.
- **Appendix B** provides the License Program Specification (LPS) for the IBM Multiprotocol Network Program.
- A list of abbreviations, a glossary, a bibliography, and an index follow the appendixes.

Summary of Changes

Since the first edition of the *IBM Multiprotocol Network Program Operations and Problem Management* was published, technical changes include, but are not limited to:

- Fast-path command equivalents for the **Clear the Error Log** menu item
- Menu item equivalents for these fast-path commands:
  - **files (transfer) checksum**
  - **files (transfer) compress**
  - **files (transfer) uncompress**
  - **files system view**
  - **hardware model update**
  - **hardware serial update**
- Limited access to AIX* commands
- New functions supported through both System Manager and the fast-path environment:
  - Display the protocol trace status
  - List the processes that protocols are running
  - Report network statistics on the transparent bridge protocol and the transparent bridge spanning tree
  - Send IP echo requests continuously from the 6611 to a remote node
  - Provide support for translational bridge protocol with:
    - Translational bridge network statistics
    - Translational bridge spanning tree network statistics
    - Translational bridge spanning tree trace
  - Display transparent bridge filter information
  - Display source route bridge filter information
- New functions supported only through the fast-path environment:
  - View or modify APPN class-of-service (COS) files
  - Send IPX echo requests
  - Turn DLSw negative cache parameter to on or off
  - Turn DLSw TCP delay parameter to on or off
- New adapter support
- Protocol debug information collection facility

Technical changes are marked with revision bars (I) in the left margin of the page.

This edition contains miscellaneous corrections and clarifications of information that appeared in the first edition of the *Multiprotocol Network Program IBM Multiprotocol Network Program Operations and Problem Management.*

For the sake of brevity, we will refer to equivalent adapters by one generic name. Table 0-1 lists the adapters supported by each model of the 6611 and the generic name used in this publication.

Table 0-1. 6611 Adapter Names

Shortened Name	Full Adapter Name	
	Model 120 and Model 125	**Model 140, Model 145, Model 170, and Model 175**
token-ring network 16/4 adapter	6611-A25 1-Port Token-Ring Network 16/4 Adapter	6611-A47 1-Port Token-Ring Network 16/4 Adapter
	6611-A25 2-Port Token-Ring Network 16/4 Adapter	6611-A47 2-Port Token-Ring Network 16/4 Adapter
Ethernet adapter	6611-A25 1-Port Ethernet Adapter	6611-A47 1-Port Ethernet Adapter
		6611-A47 2-Port Ethernet Adapter
serial adapter	6611-A25 2-Port Multi-Interface Serial Adapter	6611-A47 2-Port Multi-Interface Serial Adapter
	6611-A25 4-Port Multi-Interface Serial Adapter	6611-A47 2-Port Multi-Interface Serial Adapter
serial/token-ring combination adapter	6611-A25 Multi-Interface Serial/Token-Ring Combination Adapter	6611-A47 Multi-Interface Serial/Token-Ring Combination Adapter
serial/Ethernet combination adapter	6611-A25 Multi-Interface Serial/Ethernet Combination Adapter	6611-A47 Multi-Interface Serial/Ethernet Combination Adapter
SDLC adapter	6611 4-Port SDLC Adapter	6611 4-Port SDLC Adapter
X.25 adapter	6611 X.25 Adapter	6611 X.25 Adapter

Who Should Use This Book

This book is intended for the customer who will operate and manage the 6611. The users include the network planner, system programmer, network administrator, and network operator.

6611 Network Processor and Multiprotocol Network Program Information

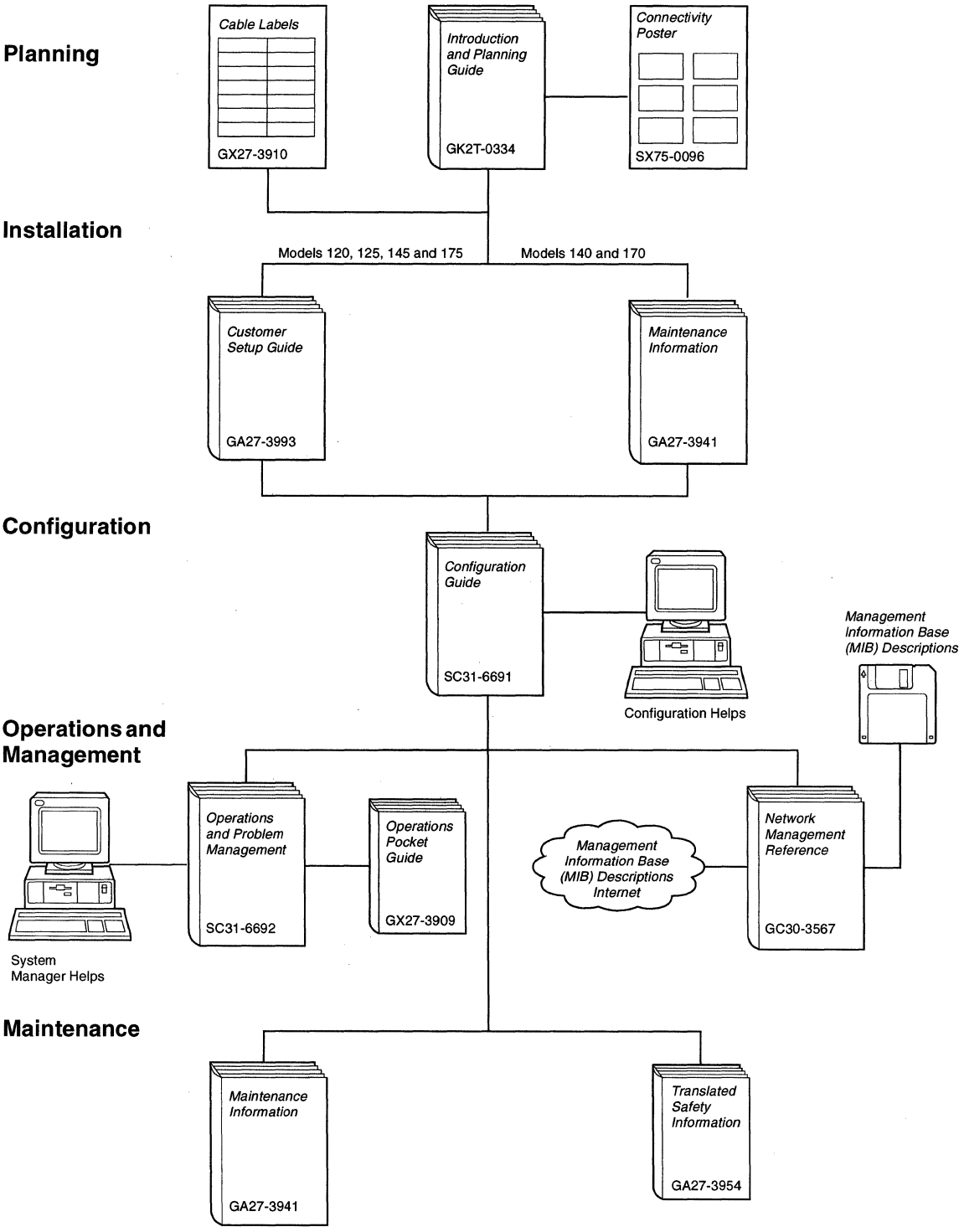


Figure 0-1. The 6611 Library

Library Overview

Table 0-2 shows the IBM 6611 Network Processor and the IBM Multiprotocol Network Program library, arranged according to tasks.

Table 0-2 (Page 1 of 2). Release 3 Library

Planning

GK2T-0334 — *IBM 6611 Network Processor Introduction and Planning Guide*

Part I of this book provides information needed to understand the functions of the 6611, how to order it, and how to plan and to prepare for its installation. Part II is an overview of networking concepts and designs. Part III is a protocol reference that includes details about each of the protocols that the 6611 supports. The *IBM 6611 Network Processor Connectivity* poster is packaged with this book.

SX75-0096 — *IBM 6611 Network Processor Connectivity* poster

This poster illustrates some of the connectivity options for Models 120, 125, 140, 145, 170 and 175.

Note: This poster is shipped with the *Introduction and Planning Guide* and can also be ordered separately.

GX27-3910 — *IBM 6611 Network Processor Cable Labels*

These labels, when completed, provide information about the:

- 6611 adapters and the network devices to which the cables will be connected
- Network to which the adapter will be attached
- Network management support, if any, for that network

Note: In previous releases, the cable labels had been included in the *Introduction and Planning Guide*; you can now order them separately.

Installation and Maintenance

GA27-3993 — *IBM 6611 Network Processor Customer Setup Guide*

This book, shipped with Models 120, 125, 145, and 175, explains how to:

- Prepare each model for installation
- Install each model
- Verify the successful installation of each model
- Install the available features for each model
- Setup an ASCII terminal and a modem so that they can communicate with the 6611
- Perform an orderly shutdown of the 6611

Note: GA88-6199 is the Japanese version of this book.

GA27-3941 — *IBM 6611 Network Processor Maintenance Information*

This book provides maintenance information for Models 120, 125, 140, 145, 170 and 175. It also provides installation instructions for Models 140 and 170. It shows how to remove and replace field replaceable units and it identifies adapters and cables that are used with the 6611.

Table 0-2 (Page 2 of 2). Release 3 Library

GA27-3954 *IBM 6611 Network Processor Translated Safety Information*

This book provides translations for caution and danger notices and other safety information found in the *IBM 6611 Network Processor Maintenance Information* and the *IBM 6611 Network Processor Customer Setup Guide.*

Configuration

SC31-6691 *IBM Multiprotocol Network Program Configuration Guide*

This book explains how to install and use the Configuration Program. It also provides instructions, examples, and scenarios that enable you to customize your 6611 configuration.

Operations and Management

SC31-6692 *IBM Multiprotocol Network Program Operations and Problem Management*

This book describes how to use the System Manager component of the IBM Multiprotocol Network Management Program to perform these tasks:

- Operate the 6611 and monitor its status
- Perform software problem determination
- Install and maintain software
- Maintain hardware
- Use System Manager helps, including the fast-path
- Use the fast-path commands

GX27-3909 *IBM 6611 Network Processor Operations Pocket Guide*

This book shows how to operate the 6611 and explains error and status codes. It provides brief descriptions of the System Manager menus and fast-path commands.

GC30-3567 *IBM 6611 Network Processor Network Management Reference*

This book provides:

- Information on the network management facilities provided by the IBM 6611.
- A high-level overview of the Simple Network Management Protocol (SNMP) as well as complete descriptions of the SNMP traps and SNA alerts supported.
- A description of how the IBM LAN Network Manager manages token-ring networks that are remotely or locally attached to the IBM 6611.

The *IBM Multiprotocol Network Program MIB Diskette* is packaged with this book.

Library Ordering Information

All IBM 6611 publications can be ordered separately.

These publications are shipped with the IBM 6611:

IBM 6611 Network Processor Customer Setup Guide (shipped with Models 120, 125, 145, and 175)

IBM 6611 Network Processor Maintenance Information

IBM 6611 Network Processor Operations Pocket Guide

IBM 6611 Network Processor Translated Safety Information

These publications are shipped with the IBM Multiprotocol Network Configuration Program:

IBM Multiprotocol Network Program Configuration Guide
IBM Multiprotocol Network Program Operations and Problem Management
IBM 6611 Network Processor Introduction and Planning Guide

The *IBM Multiprotocol Network Program MIB Diskette* is packaged with the *IBM 6611 Network Processor Network Management Reference*. The MIBs are also available over the Internet. Internet retrieval instructions are included in the *IBM 6611 Network Processor Network Management Reference*.

Obtaining Softcopy Information

Softcopy BookManager* READ library information will be available for many of the IBM 6611 publications on the *IBM Networking Systems Softcopy Collection Kit.* To place a single order for the CD-ROM, use form number SK2T-6012. To place a single order for the 3480 cartridge, use form number SK2T-6013.

Yearly subscriptions for the *IBM Networking Systems Softcopy Collection Kit*, product number 5636-PUB, are available through your branch office representative. Order feature code 2003 and media code 5003 for CD-ROM format. Order feature code 2004 and media code 5004 for 3480 cartridge format.

Note: The *Customer Setup Guide*, *Maintenance Information*, *Translated Safety Information*, *Connectivity* poster, and *Cable Labels* are not available in softcopy format.

Chapter 1. Using the System Manager

About This Chapter

This chapter describes what System Manager is and provides a hierarchical flow of the System Manager menus.

Introduction to System Manager

The IBM Multiprotocol Network Program System Manager (*System Manager*) is a menu-driven user interface that is designed to simplify system management and operation tasks. The System Manager supports tasks for performing change management, network management, and problem determination, and many system operations. System Manager is invoked automatically whenever you access the 6611. For more information about accessing the 6611, see Chapter 3.

Using the System Manager Main Menu

Figure 1-1 shows the main menu of System Manager. Each menu item represents one area of operations available through System Manager. Use the up and down arrows to highlight your selection and the Enter key to register your selection. If you are on a System Manager screen other than the main menu, you may press **F10 (Esc+0)** to return to the System Manager main menu.

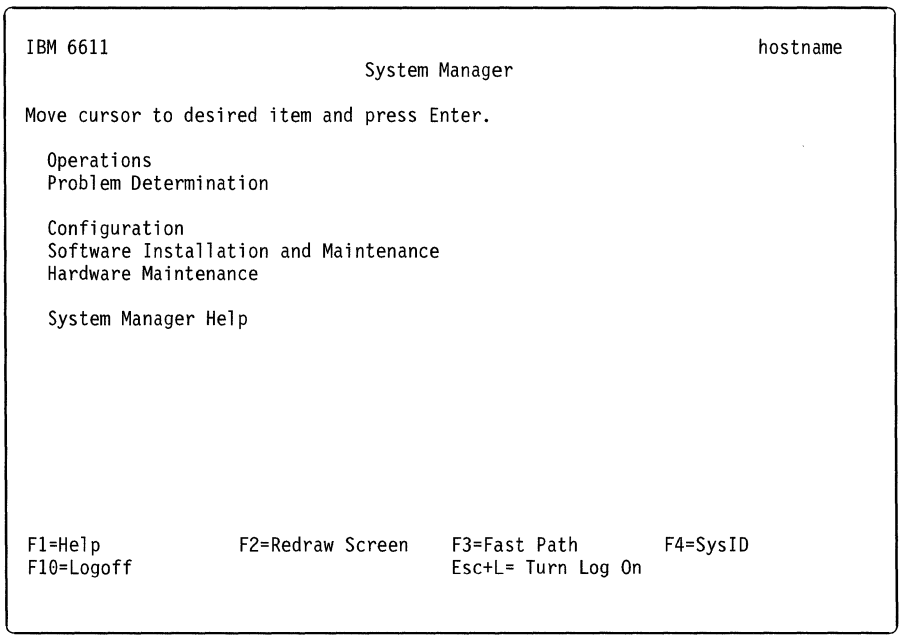


Figure 1-1. System Manager Main Menu

To go to the fast-path environment from System Manager, press **F3 (Esc+3)** on the main menu. To go to the System Manager from the fast-path environment, type **exit** or **quit** at the fast-path environment prompt and press **Enter**. See "Using the Fast-Path Environment" on page 2-15 for more information about using commands in the fast-path environment.

Press **F10 (Esc+0)** from the System Manager main menu to exit (or logoff from) the System Manager. When you access the 6611 through the S1 or S2 serial port locally or using a modem, you exit to the login prompt by pressing **F10 (Esc+0)**.

When you access the 6611 using the **telnet** or **rlogin** command, your remote connection is closed. To return to the System Manager, you are required to issue the **telnet** or **rlogin** command again. For more information about how to access the System Manager, see Chapter 3.

Another way to exit the System Manager is to press **Ctrl+C**. This takes you to the fast-path command environment.

Note: You cannot return to the System Manager when you enter the fast-path environment by this method. If you enter **exit**, you are logged out of the 6611.

Refer to "Using the Function Keys in the System Manager" on page 2-11 for explanations of System Manager function key designations.

Maps of the System Manager Menu Screens

Table 1-1 through Table 1-6 on page 1-7 show the navigation of the System Manager screens. Use these tables as references to locate System Manager task information.

There is a table for each of the System Manager main menu items. Where applicable, the choices available on a lower-level menu are shown. A page reference for more information is given for each item.

Operations Menu Items

For operations tasks, see Chapter 4 for details.

Table 1-1 (Page 1 of 2). Operations Menu Map

Operations menu item	Items on next menu	Page reference
Protocol and Interface Monitor		4-4
Routing Information	**Route Tables**	4-9
	AppleTalk Zones Information Table**	4-11
	VINES Neighbor Table**	4-12
	DLSw Partners	4-13
	DECnet Routing Information**	4-13
	OSPF Routing Information	4-14
Remote Host Echo (Ping)/Route Trace		4-18
Network Statistics	**Connection**	4-22
	Interface Status	4-23
	Interface Utilization Monitor	4-25
	Packet Traffic	4-26
	Protocol	4-27
	Bridge	4-29

Table 1-1 (Page 2 of 2). Operations Menu Map

Operations menu item	Items on next menu	Page reference
ARP Table Management	View IP ARP Table	4-32
	Add IP ARP Entry	4-33
	Delete IP ARP Entry by Hardware Address	4-34
	Delete IP ARP Entry by Host Name	4-33
	Delete All IP ARP Entries	4-34
	View AppleTalk ARP Table	4-35
Filters		4-36
Network Management Information (MIBs)		4-37
File Systems		4-40
File and Diskette Operations	View Transfer Directory File	4-42
	Rename Transfer Directory File	4-43
	Delete Transfer Directory Files	4-43
	Send Transfer Directory File	4-43
	Receive Transfer Directory File	4-45
	Checksum Transfer Directory Files	4-46
	Compress/Uncompress Transfer Directory Files	4-46
	Scan Transfer Directory Files	4-46
	Clear Log Files	4-47
	View Static Directory File	4-47
	Send Static Directory File	4-48
	List Diskette Files	4-49
	Format Diskette	4-50
Remote Access to Other Nodes		3-2
Login Information		4-51
System Activity Report		4-53
EIA 232 Serial Ports		4-54
System Shutdown		4-58
Date and Time		4-61

Problem Determination Menu Items

For problem determination tasks, see Chapter 5 for details.

Table 1-2 (Page 1 of 2). Problem Determination Menu Map

Problem Determination menu item	Items on next menu	Page reference
Process Information	Processes	5-4
	Process Commands	5-6
	Process Information	5-7
	Process Status and Resource Utilization	5-9
	Processes by Protocol	5-11
	Process Table Information	5-12
System Statistics	Virtual Memory	5-15
	Input/Output	5-16
	Memory Management	5-18
	Paging Space	5-19
	System Socket	5-20
	Active Internet Connection	5-21
Three-Digit LED Display		5-21
Error Logs and Reports	View an Error Report	5-24
	View Error Log Continuously	5-27
	View an Error Report for a Single Sequence Number	5-28
	Copy Error Log to Transfer Directory	5-30
	Clear the Error Log	5-31
System Dump	Start	5-32
	View Dump Information	5-34
	Copy to Diskette or Transfer Directory	5-34
	Format	5-35
	Extract Error Log Records	5-36
	Extract Trace Log Records	5-37
Protocol and Process Dumps	Start Nondisruptive	5-38
	View Nondisruptive	5-39
	Start Disruptive	5-39
	View Disruptive	5-40
System Trace	Start	5-42
	Stop	5-43
	Format	5-43
Protocol and Process Traces	Start	5-46
	Stop	5-47
	View	5-48
	Status	5-49

Table 1-2 (Page 2 of 2). Problem Determination Menu Map

Problem Determination menu item	Items on next menu	Page reference
Adapter Debug	Read Memory	5-51
	View Registers	5-52
	Start Line Trace	5-53
	Dump Memory	5-54
Protocol Debug	Source Route Bridge Adapter Table	5-55
	Network Management Subsystem Information	5-57
	DLSw General Information	5-58
	Protocol Debug Collection	5-59
	X.25 Traffic Monitor	5-59
Concurrent Hardware Diagnostics		5-81

Configuration Menu Items

For configuration tasks, see Chapter 6 for details.

Table 1-3. Configuration Menu Map

Configuration menu item	Items on next menu	Page reference
System Manager Configuration Utility		6-7
User IDs and Passwords	List All Users	6-18
	Add a User	6-18
	Delete a User	6-19
	Change User Password	6-19
	Change Your Password	6-20
Apply Changes		6-20
Commit Changes		6-21
Reject Uncommitted Changes		6-22
Configuration Reports		6-22
Receive and Apply Configuration		6-24
Send Configuration		6-26
Reinstate a Saved Configuration		6-26

Software Installation and Maintenance Menu Items

For software installation and maintenance tasks, see Chapter 7 on page 7-1 for details.

Table 1-4. Software Installation and Maintenance Menu Map

Software Installation and Maintenance menu item	Items on next menu	Page reference
Receive Installation File(s)		7-25
List Installation Files		7-26
List All Problems Fixed by Software Updates		7-27
Apply Software Updates		7-27
Clean up After a Failed Installation		7-28
List All Applied but Not Committed Software		7-29
Commit Applied Updates		7-29
Reject Applied Updates		7-31
View Software Vital Product Data		7-32

Hardware Maintenance Menu Items

For hardware maintenance tasks, see Chapter 8 on page 8-1 for details.

Table 1-5. Hardware Maintenance Menu Map

Hardware Maintenance menu item	Items on next menu	Page reference
Installed Devices		8-4
Device Characteristics		8-5
Hardware Vital Product Data		8-6
Configuration Change VPD Update		8-7
Serial Number		8-8
Model Number		8-9

System Manager Help Menu Items

For System Manager help information, see Chapter 2 on page 2-1.

Table 1-6. System Manager Help Menu Map

System Manager Help menu item	Items on next menu	Page reference
Menu Screens		2-3
Selector Screens		2-6
Dialog Screens		2-7
Command Status Screens		2-8
Function Keys		2-11
Selecting Choices from a List		2-14
Fast Path		2-15

Chapter 2. System Manager Help

About This Chapter

This chapter describes the different screen types within the System Manager and the different types of help that are available throughout the System Manager. It includes help for the fast-path environment, using the fast-path log, and how to execute the fast-path command environment. Figure 2-1 shows the System Manager Help menu.

```
IBM 6611                                                          hostname
                            System Manager Help

Move cursor to desired item and press Enter.

  Menu Screens
  Selector Screens
  Dialog Screens
  Command Status Screens

  Function Keys
  Selecting Choices from a List

  Fast Path









F1=Help             F2=Redraw Screen    F3=Return           F4=SysID
F10=Main Menu                           Esc+L=Turn Log On
```

Figure 2-1. System Manager Help

Refer to the following for information about the individual menu items:

- "Menu Screens" on page 2-3.
- "Selector Screens" on page 2-6.
- "Dialog Screens" on page 2-7.
- "Command Status Screens" on page 2-8.
- "Using the Function Keys in the System Manager" on page 2-11.
- "Selecting Choices from a List" on page 2-14.
- "Using the Fast-Path Environment" on page 2-15.

Understanding the System Manager Screens

The System Manager has these four major types of screens:

- Menu screens
- Selector screens
- Dialog screens
- Command status screens

Other supporting screens in the System Manager include:

Contextual help screens
: Describe specific help information for a given field. On menu screens, the help information describes the task that the menu item performs. On selector screens, the help information describes the list of items to select. On dialog screens, the help information gives instructions for data entry in a field. On command status screens, the help information describes the function performed and the output provided. To get help, position the cursor beside the item on which help is desired and press **F1 (Esc+1)**.

General help screens
: Contain help information either for the entire System Manager or for a specific screen type. General help for the entire System Manager is invoked from the System Manager main menu, and from within each contextual help screen, information message screen, and error message screen. General help for screen types is available on pop-up list screens, field edit screens, and command status screens.

  To get help, position the cursor beside the item on which help is desired and press **F1 (Esc+1)**.

Information message screens
: Give status information when attempting to execute a task.

Error message screens
: Identify problems that occur when attempting to execute a task.

Pop-up list screens
: Appear when **F4 (Esc+4)** is pressed on an entry field of a dialog screen that contains a list of options that can be selected for the given dialog item. These dialog items contain a "+" on the right side of the screen.

Field edit screens
: Appear when **F6 (Esc+6)** is pressed on a field of a dialog screen that can be edited.

For information about function keys and key sequences, see Table 2-1 on page 2-12.

Menu Screens

Each menu screen has a list of items that can be selected to perform a specific task or group of tasks that are described by the menu item. In the top right corner of the menu screen, the host name that is associated with this 6611 appears, if configured. The host name is only updated when the user logs in. If the host name changes during the login session and you want the new name to appear on the screen, you need to exit the 6611 and log in again. The menu title appears on the second line of the menu screen.

Many menu paths lead to dialog screens, which provide a means of interactive dialog.

Figure 2-2 shows the main menu screen of the System Manager.

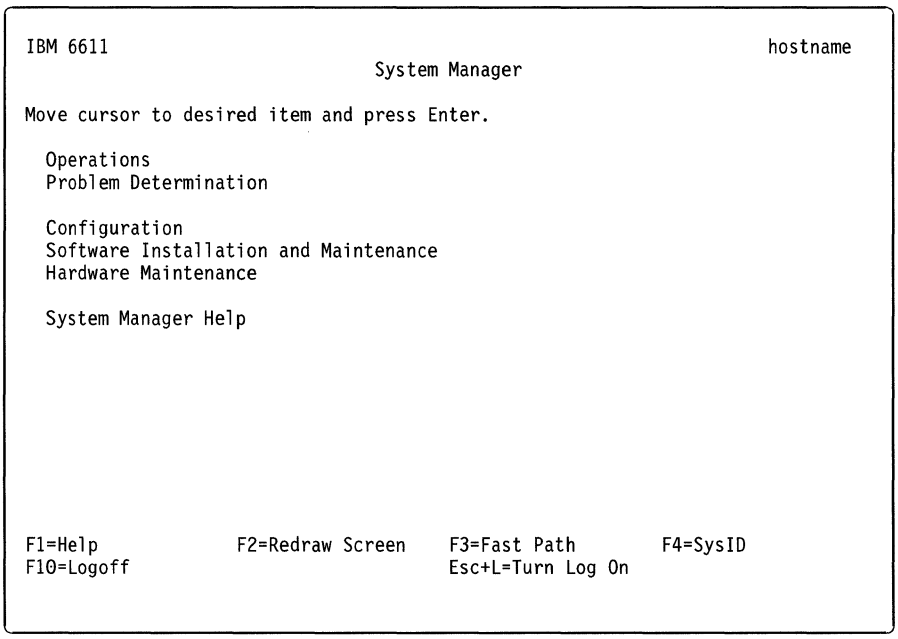


Figure 2-2. System Manager Main Menu

To select a menu item, move the cursor beside that menu item and press **Enter**. With some terminal types, the selected menu item is shown in reverse video. One of the following screens appears:

- Another menu screen
- A command status screen
- A selector screen
- A dialog screen

From each of the menu screens, press **F4 (Esc+4)**, labeled SysID, to view high-level system configuration information. This information can be viewed only when it is configured. The configuration information includes:

- Host name

  The host name must be configured using either the Configuration Program or the System Manager. (Using the Configuration Program rather than System Manager is *highly recommended*.)

- Model number

  The model number is added to the hardware vital product data during the manufacturing process. If you replace your hard disk, it may be necessary to update the hardware vital product data with the model number.

  You can update the model number with the System Manager function, **Model Number** from the Hardware Maintenance menu, or with the fast-path command:

  hardware model update *model_number*

- Serial number

  The serial number is added to the hardware vital product data during the manufacturing process. If you replace your hard disk, it may be necessary to update the hardware vital product data with the serial number.

  You can update the serial number with the System Manager function, **Serial Number** from the Hardware Maintenance menu, or with the fast-path command:

  hardware serial update *serial_number*

- Configuration name

  The configuration name is the name of the configuration currently running in the IBM 6611. If the current configuration was sent from the Configuration Program, this name is the one that was specified when you saved the configuration. If the current configuration was updated last with the System Manager, the name has the format: `localhost(userid) date time`. The userid is the user name that was used to update the current configuration at the date and time specified. Any configuration change made from the System Manager must be applied or committed for it to become the current configuration.

  Refer to Chapter 6 for details on using the System Manager for updating configuration parameters. It is *highly* recommended that you use the Configuration Program for all your configuration needs, except for setting user IDs and passwords.

- Configuration status

  The System Manager configuration status presented is from the perspective of the user who has pressed **F4 (Esc+4)=SysID** to view this information. The configuration status can be:

  `current`: all configuration changes made from the user ID that you are logged into have been committed. However, there may be unapplied or applied configuration changes made from a different user ID. If another user has some applied (but not committed) changes, the configuration name will have the localhost format. The user ID will contain the name of the user who has applied, but not committed, the last configuration changes. The only way to determine if there are unapplied configuration changes is to login with each controlling user ID and press **F4 (Esc+4)=SysID** to view its configuration status.

  `applied`: the user ID that you are logged into has some applied, but not committed, configuration changes.

  `unapplied`: the user ID that you are logged into has some unapplied configuration changes. These changes are unnamed. Thus, the configuration name is not associated with these changes.

  `partially applied`: the user ID that you are logged into has some applied and unapplied configuration changes.

- Adapter slot list

  A list of the adapter slots and the type of adapter contained in each slot is displayed along with the adapter and interface names associated with the adapter.

When viewing the System Configuration Information screen, press **Enter** to return to the System Manager menu screen.

Selector Screens

A selector screen displays a list of options from which a selection must be made to complete the task. This screen appears between menu screens and dialog or command status screens throughout the System Manager.

Figure 2-3 is an example of a selector screen in the System Manager.

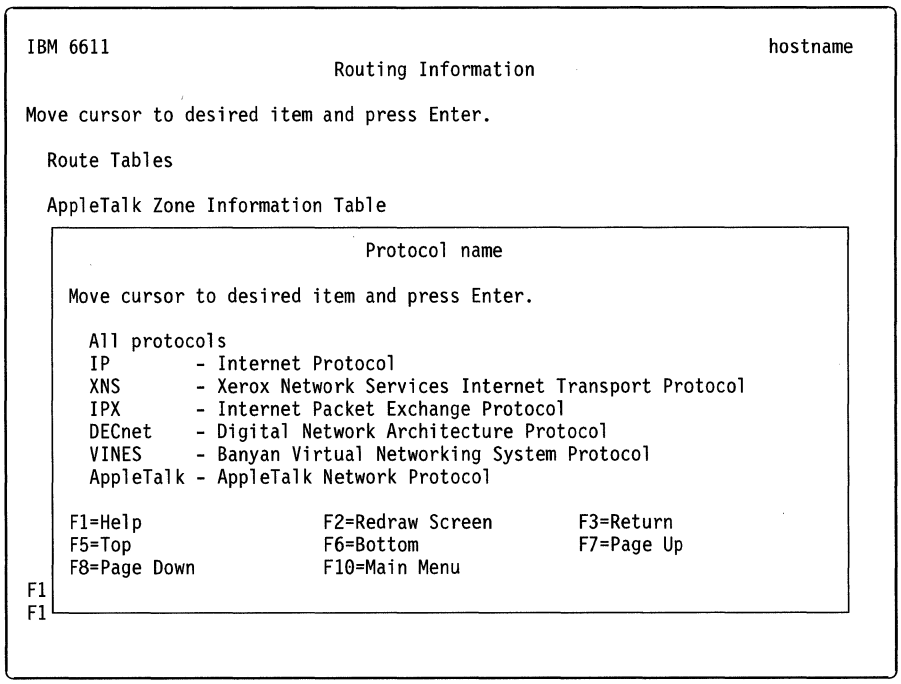


Figure 2-3. Example of a Selector Screen

To select an option on a selector screen, use the up and down arrow keys to place the cursor beside the item in the selection list.

For lists that are too long to be displayed on one screen, the following indications appear at the top or bottom of the list:

[TOP]	Indicates the top of the list
[BOTTOM]	Indicates the bottom of the list
[MORE...nn]	Indicates that nn items in the list are not displayed on the screen.

Place the cursor on the item to be selected and press **Enter** to select the item. One of the following screens appears:

- Another selector screen
- A command status screen
- A dialog screen

Contextual help is available for the group of items on the selection list.

For information about function keys and key sequences, see Table 2-1 on page 2-12.

Dialog Screens

In a dialog, you provide details about the task you selected. Values are placed into the entry fields on the dialog screen by selecting an item from an *option ring*, from a pop-up list, or by typing in the value for dialog items that do not have a list.

In the top right corner of the menu screen, the host name that is associated with this 6611 appears, if configured. The host name is only updated when the user logs in. If the host name changes during the login session and you want the new name to appear on the screen, you need to exit the 6611 and log in again.

Figure 2-4 is an example of a dialog screen in the System Manager.

```
IBM 6611            Issue IP Echo (Ping) to Any IP Node          hostname

Type or select values in entry fields.
Press Enter after making all desired changes.

                                                    [Entry Fields]
* Host name or IP address                          []
* Packet size                                      [64]                  #
* Number of echoes                                 [3]                   #









F1=Help             F2=Redraw Screen    F3=Return           F4=List
F5=Undo             F6=Edit             F7=Page Up          F8=Page Down
F10=Main Menu                           Esc+L=Turn Log On
```

Figure 2-4. Example of a Dialog Screen

To select a dialog item, use the up and down arrow keys to move the cursor to the entry field.

The following symbols indicate the various types of entry fields on the dialog screens:

Symbol	Meaning
[ ]	Indicates an entry field
< >	Indicates more text to the left or right of the visible entry field. Use the right and left arrow keys to scroll the field.

The following symbols appear at the left side of the screen:

Symbol	Meaning
*	Indicates that this dialog item requires a value.

The following symbols appear at the right side of the screen:

Symbol	Meaning
+	Indicates that a list of choices or an option ring is available. A list of choices is a pop-up list with the selections available for a particular entry field. An option ring allows you to tab through each selection available for a particular entry field. Press **F4 (Esc+4)** to display the list of choices. You will see a screen of your option list. Use the up and down arrow keys to place the cursor on an option in the list that you want to select. Press **Enter** to select the option for a single selection list when one choice is allowed. Press **F9 (Esc+9)** to select items for a multiple selection list and press **Enter** to indicate all choices that are selected. When an option ring is available, the entry field is not enclosed in brackets in most instances. Press **Tab** to display and make a selection from the option ring. For an explanation of option rings, single and multiple selection lists, refer to "Selecting Choices from a List" on page 2-14.
#	Indicates that a numeric value must be supplied.
X	Indicates that a hexadecimal value must be supplied.

When dialog items are too long to be displayed on one screen:

[TOP]	Indicates the top of the list of dialog items.
[BOTTOM]	Indicates the bottom of the list of dialog items.
[MORE...nn]	Indicates that nn dialog items are not displayed on the screen.

Contextual help is available for each entry field on the dialog screen.

For information about function keys or key sequences, see Table 2-1 on page 2-12.

Command Status Screens

The command associated with a selected task is invoked when you press **Enter** on a:

- Dialog screen
- Selector screen
- Menu screen that does not lead to a dialog screen

A command status screen is displayed as a result of issuing most commands. While the command is executing, the `Command: running` message is displayed in the upper left side of the screen. The function key designations are not displayed. As the output is formatted for the screen, a `Processing data ...` message is displayed at the bottom the screen. When the command completes, the `Command: OK` message or `Command: failed` message is displayed in the upper left side of the screen. The first screen of the output is displayed on the screen and the function key designations appear at the bottom of the screen.

In the upper right corner of the menu screen, the host name that is associated with this 6611 appears, if configured. The host name is only updated when the user logs in. If the host name changes during the login session and you want the new name to appear on the screen, you need to exit the 6611 and log in again.

Press **F1 (Esc+1)** for contextual help describing the function just performed and the output produced.

Figure 2-5 is an example of a command status screen in the System Manager.

```
IBM 6611                          COMMAND STATUS                        hostname

Command: OK            stdout: yes           stderr: no
Function name: Protocol Interface Statistics
Fast Path: [at | dec | ip | ipx | vines | xcs] stat (view) -intf "intf"

------------------------------------------------------------------------

[TOP]
ip:
        ocIpForwarding = 1
        ocIpDefaultTTL = 255
        ocIpInReceives = 87
        ocIpInHdrErrors = 0
        ocips_toosmall = 0
        ocips_badver = 0
        ocips_badhlen = 0
        ocips_badsum = 0
        ocips_badlen = 0
        ocips_tooshort = 0
        ocips_badttl = 0
[MORE...27]

F1=Help             F2=Refresh Data     F3=Return           F5=Top
F6=Bottom           F7=Page Up          F8=Page Down        F10=Main Menu
```

Figure 2-5. Example of a Command Status Screen

When the output cannot be displayed on one screen:

[TOP] Indicates the top of the list

[BOTTOM] Indicates the bottom of the list

[MORE...nn] Indicates that nn items of the list are not displayed on the screen.

For information about function keys or key sequences, see Table 2-1 on page 2-12.

With some commands, the command status screen is not used for output. The System Manager clears the screen and gives control of the screen to the command being invoked. When the command finishes, control is returned to the System Manager. This is used mainly in situations requiring interactive dialog between you and the command being issued (for example, changing passwords).

There are also situations when the System Manager gives control of the screen to the command being invoked and then exits. (Examples of these situations are for configuration changes or when issuing a system dump.) When the command is completed, System Manager does not regain control of the screen. Therefore, you will have to log in again to the 6611 to restart System Manager.

Whenever this situation occurs, you will see an

```
ARE YOU SURE?
```

message. You are given a chance to cancel the command which would cause System Manager to exit.

Getting System Manager Help

Help is available for System Manager screens. The type of help displayed is determined by the cursor location when you request help or by the task you are doing when you request help.

Contextual Help

Contextual help is available for dialog entry fields, selector screens, menu items, and command status screens. To get contextual help, position the cursor on the entry field, list item, or menu item and press **F1 (Esc+1)**.

On dialog screens, the help information gives instructions for data entry in a field. On selector screens, the help information describes the list of items to select. On menu screens, the help information describes the task that the menu item performs. On command status screens, the help information describes the function performed and the output produced.

General Help

General help is available for the entire System Manager interface. This general help describes how to use the System Manager and the different screen types. This help is invoked from the System Manager main menu and from each of the contextual help screens, information screens, and error message screens. To access this general help from the contextual help screen, the information message screen, and the error message screen, press **F1 (Esc+1)**.

There are three ways of obtaining general System Manager help from the main menu, as shown in Figure 2-6 on page 2-11:

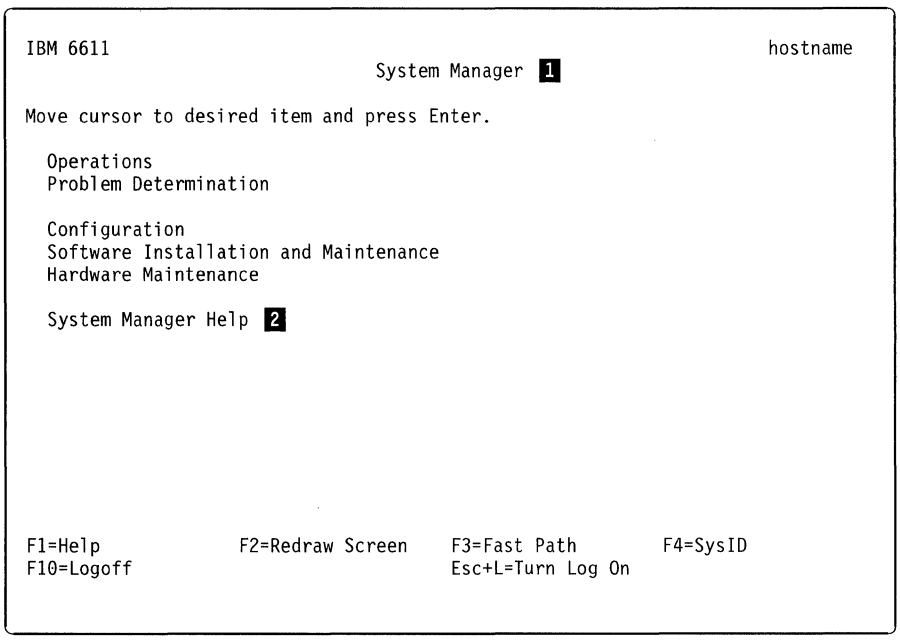


Figure 2-6. System Manager Main Menu

- Position the cursor on the title of the System Manager main menu, **1**, and press **F1 (Esc+1)**.
- Position the cursor on the System Manager Help menu item, **2**, and press **F1 (Esc+1)**.
- Position the cursor on the System Manager Help menu item, **2**, and press **Enter**. There is another menu from which you can select from one of five general help topics. See Figure 2-1 on page 2-2.

To access general help on a dialog entry field, press **F4 (Esc+4)** to bring up a pop-up list. To get help, press **F1 (Esc+1)** while viewing the list of choices.

To access general help on the field edit screen, press **F6 (Esc+6)** on a dialog entry field. To get this help, press **F1 (Esc+1)** while viewing the field edit screen.

Using the Function Keys in the System Manager

In the System Manager, function key designations appear at the bottom of the screens. Only the function keys that are valid for the specific screen type are displayed. Table 2-1 describes these function keys.

The key sequences function according to the way the first key functions. All keys are designated by a plus sign (+) separating the keys.

- If the first key is the Esc key, it is pressed and released. The second key is pressed shortly after the Esc key.
- If the first key is the Ctrl or Shift key, it is pressed and held down while the second key is pressed.

Note: The following functions are valid only when your keyboard has not been remapped.

Table 2-1 (Page 1 of 2). System Manager Function Keys

Function Key	Meaning	Description
F1 or Esc+1	Help	Gives more information about the item selected. In some areas of the System Manager, you can move to the next level for more information.
F2 or Esc+2 menu, dialog, and selector screens	Redraw Screen	Redraws the screen. Use if the console messages overwrite the screen.
F2 or Esc+2 command status screens	Refresh Data	Reexecutes the function described by the Function name.
F3 or Esc+3	Return	From the main menu, F3 (Esc+3) will take you to the fast-path command environment. From other screens, F3 (Esc+3) returns one level to the previous screen.
F4 or Esc+4 dialog screens	List	Presents a list of possible choices for an entry field. A scrollable pop-up list is displayed.
F4 or Esc+4 menu screens	SysID	Displays a screen with high-level system configuration parameters, such as host name, serial number, model number, and configuration file name.
F5 or Esc+5 dialog screens	Undo	Resets the entry field to the original setting.
F5 or Esc+5 selector and command status screens	Top	Scrolls to the top of the list or command output.
F6 or Esc+6 dialog screens	Edit	Allows editing of an entry field. Use this key if a larger entry field is needed.
F6 or Esc+6 selector and command status screens	Bottom	Scrolls to the bottom of the list or command output.
F7 or Esc+7	Page Up	Scrolls to the previous page.
F8 or Esc+8	Page Down	Scrolls to the next page.
F9 or Esc+9	Select	Makes individual selections on multiple selection lists.
F10 or Esc+0 on Main Menu	Logoff	Exits the System Manager. Log in again to return.
F10 or Esc+0 on other screens	Main Menu	Returns to the System Manager Main Menu.
Enter	Do	Performs the selected function.
Ctrl+C	Interrupt	When used on System Manager continuous display output screens, exits the command. When used on other System Manager screens, exits System Manager into the fast-path environment. If a file is viewed from the fast-path environment using the More Facility, it exits the file. Refer to "The More Facility" on page 9-7 for more information.
Home or Esc+<	Top	Scroll to the top of the command output.

Table 2-1 (Page 2 of 2). System Manager Function Keys

Function Key	Meaning	Description
End or Esc+>	Bottom	Scroll to the bottom of the command output.
Esc+L	Turn log on or off	It serves as a toggle switch for the System Manager log. If the System Manager log is off, this turns the log on. If the System Manager log is already on, this turns the log off.
Page Up or Esc+V	Page up	Scrolls backward to the previous page.
Page Down or Ctrl+V	Page down	Scrolls forward to the next page.
Tab	Forward the list of options	Moves forward through a list of choices associated with a dialog item. A list of choices is denoted by a plus (+) symbol located to the right of the entry field and the absence of brackets ([ ]) surrounding the entry value.
Arrow keys	Moves the cursor up one line or down one line	Scrolls through the information. Moves between entry fields on dialog screens. Moves the cursor beside menu items on the menu screens.
Backspace	Delete character	Deletes the character at the left of the screen.

Selecting Choices from a List

In the System Manager, you can make selections from one of three types of lists:

Single selection lists:

Appear on selector screens.

Are available with most dialog items when you use the list option, F4 (Esc+4). Are denoted by the plus (+) symbol on a dialog screen.

Multiple selection lists:

Appear with a few dialog items when you use the list option, F4 (Esc+4).

When multiple selection lists are available, the select option, F9 (Esc+9), is available on the selector screen.

Option rings:

Appear on some dialog items.

Are denoted by the plus (+) symbol and the absence of brackets surrounding the entry field.

To select an item from a single selection list:

1. Move the cursor to the correct item.
2. Press **Enter** to select the item.

To select more than one item from a multiple selection list:

1. Move the cursor to the first item to be selected.
2. Press **F9 (Esc+9)** to select the individual item. Press **F9 (Esc+9)** a second time to undo the selection.
3. Continue selecting until all desired items are highlighted.
4. Press **Enter** to confirm choices.

To select an item from an option ring:

1. Press **Tab** to move forward through the list of choices.
2. Press **Shift+Tab** key sequence to move backward through the list of choices.
3. Press **Enter** to select the item.

Using the System Manager Log

The Multiprotocol Network Program maintains a System Manager log which began with Version 1 Release 2. Output is always directed to the screen, if it is less than 512 K bytes long. (If it is longer than 512 K bytes, you can view it from the fast-path environment.) You can select to have the output of all functions that are directed to the screen to also be sent to a single log file in the transfer directory.

To request that output be sent to the log, you must turn on the log. This is done by pressing the **Esc+L** keys. This key combination serves as a toggle switch. The key description at the bottom of each menu reminds you of the log's status. A statement of **Turn Log On** means the log is off. **Turn Log Off** means the log is currently turned on.

Output is appended to the log file. It does not overwrite information that is already there.

There can be a separate System Manager log for each user ID. The System Manager log name has the form:

`sysman.log.userid`

where `userid` is the user who is logged into the System Manager. Each System Manager log is monitored when a user logs into the System Manager.

If the file is longer than 512 K bytes, it is renamed to:

`sysman.log.userid.old`

A new log is created when data is directed to the log. The previous `sysman.log.userid.old` is overlaid.

Using the Fast-Path Environment

The fast-path environment is a *command line interface* that enables you to execute most of the same functions provided in the System Manager screens. The fast-path environment uses commands to execute 6611 functions without having to navigate through the System Manager screens to perform the tasks.

Fast-Path Command(s)

Throughout this manual, this box is used to show command alternatives to System Manager menu paths. Where applicable, this command equivalent is shown under the set of menu steps needed to complete a task.

For almost any command, the `-log` option can also be specified, although it is not shown in the examples. This will send command output to the fast-path log.

For each command, the long form is given. Defaults and abbreviations can be specified. Refer to Chapter 9 on page 9-1 for command details and a description of command syntax, or the *IBM 6611 Network Processor Operations Pocket Guide* for a summary.

Note: The fast-path commands perform error checking on most, but not all, of the entered parameters.

Refer to Chapter 9 on page 9-1 for:

- General information about the commands (such as output)
- Executing commands
- Use of the fast-path log
- Use of global and object-specific fast-path help
- Use of the More facility to view help text
- Details on the commands themselves

The commands can be used in the fast-path environment, with the rexec or rsh command, or in rsh scripts. Information on the commands needed to execute the tasks in this book are listed under Chapter 9. For more information on the commands, use the fast-path help provided with System Manager.

Chapter 3. Accessing the 6611

About This Chapter

This chapter describes the methods used to access the 6611. The 6611 can be accessed locally and remotely through either of the EIA 232 serial ports, S1 and S2 (labeled S1 and S2 on the Model 120 and Model 170, and labeled Serial 1 and Serial 2 on the Model 140).

Unless specific reference is made to the Model 140, the EIA 232 serial ports are referred to as S1 and S2 throughout.

Users who configure the S2 serial port to support network management of the Cylink** 4201 cannot use the S2 serial port for local or remote access to the 6611 as described in Chapter 3 on page 3-1. See the *IBM Multiprotocol Network Program Configuration Guide* for information on configuring Cylink. For more information on accessing the 6611, including terminal attachment, see the *IBM 6611 Network Processor Introduction and Planning Guide*.

Accessing a Local 6611

Local access to the 6611 is needed only in isolated situations, such as to replace hardware components or to replace remote service when there is no modem access and the 6611 cannot be reached through the IP network.

Most service procedures require an ASCII terminal (or terminal emulating an ASCII device). For local access, it is attached to the 6611 through one of the EIA 232 serial ports. Attaching the terminal does not disrupt the operation of the 6611.

When the terminal is connected to the serial port, the login screen appears. Enter a configured user ID and password. After password verification, a prompt for the terminal type appears. After the correct terminal type is entered, control is passed to the System Manager. See the *IBM 6611 Network Processor Introduction and Planning Guide* for more information about the supported ASCII terminal types. Refer to "Logging In to a 6611" on page 3-13 for more information about logging into the 6611.

Accessing a Remote 6611

Remote access is the method both you and IBM service personnel use to access the 6611 most of the time. All management and operation tasks can be performed over the IP network connection from your network management station. Access by modem is the best for IBM service personnel.

If IBM service personnel are given access to the 6611, you do not need to know how to issue dumps and traces or retrieve problem, performance, or configuration information. IBM service personnel can perform all the problem determination tasks and gather all the data they need.

Using an IP Network Connection

Using the IP network, the following TCP/IP remote access commands can access the 6611:

- Telnet (**telnet**)
- Remote login (**rlogin**)
- File Transfer Protocol (**ftp**)
- Remote shell (**rsh**)
- Remote execution (**rexec**)

When you use each of these commands depends on the specific situation and location at which the command is being issued. If you are located at an IP node on your IP network that is not a 6611, you can issue any of the commands listed above to your 6611, provided the IP node supports the command. The same commands can also be issued from the System Manager or from the fast-path environment of any 6611 to another 6611 with the exception of **rexec**. Rexec is no longer valid *from* a 6611. Each of the above commands, except **rsh** and **rexec**, can be issued from the System Manager or from the fast-path environment of a 6611 to another node on the IP network that is not a 6611.

In the remainder of this chapter, each of the remote access commands is discussed in detail with explanations of how they are issued to and from a 6611. There are fast-path commands that are used with the **rsh** and **rexec** remote access commands. You may refer to Chapter 9 or use online help from the fast-path environment to get detailed information on the commands.

When you use the System Manager to execute these remote access commands, there is a specific menu item for the telnet, rlogin, and rsh functions that are accessed from the Operations menu, called the Remote Access to Other Nodes menu. See Figure 3-1 for the functions available on the Remote Access to Other Nodes selector screen.

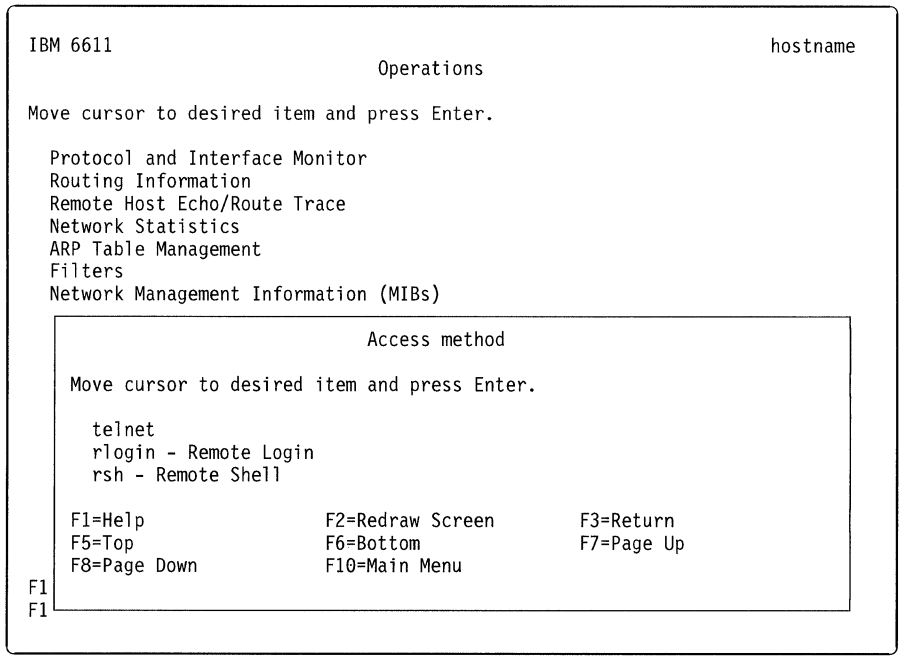


Figure 3-1. Remote Access Selector Screen

Using Telnet

Telnet is the most widely used method for one node on an IP network to reach another node. A user at a remote station can log in and interactively execute multiple commands at the destination station. Both IP stations must support Telnet for the session to be established. When a Telnet session is established to a 6611, all the same tasks can be performed with the remote session as with the local attachment of the ASCII terminal to the EIA 232 serial ports.

Two Telnet session initiation procedures are outlined below:

- From a remote IP station to access a 6611
- From one 6611 to access any other IP station (including another 6611)

Remote IP Station to a 6611: The 6611 can be accessed from any station on the IP network using Telnet. The Telnet protocol requires you to know the host name or IP address, a user ID, and a password configured for the 6611. User IDs and passwords must be configured using the Configuration Program, by a controlling user using the System Manager, or a fast-path environment command. Refer to "Logging In to a 6611" on page 3-13 for more information about 6611 users.

The following steps show the details of a Telnet session's initiation from a remote station to a 6611. You must have the host name registered with the name server for the host name to be recognized, or the host name can be mapped to its IP address in the 6611 using the Configuration Tool or the fast-path command **hostname map add** *host_name IP_address*. What you are expected to input from the remote station is provided under **"Type in"**. What you should expect to find displayed on the screen is provided under **"Output displayed"**.

Type in:

telnet hostname

The IP address of the 6611 can be used in the place of the host name.

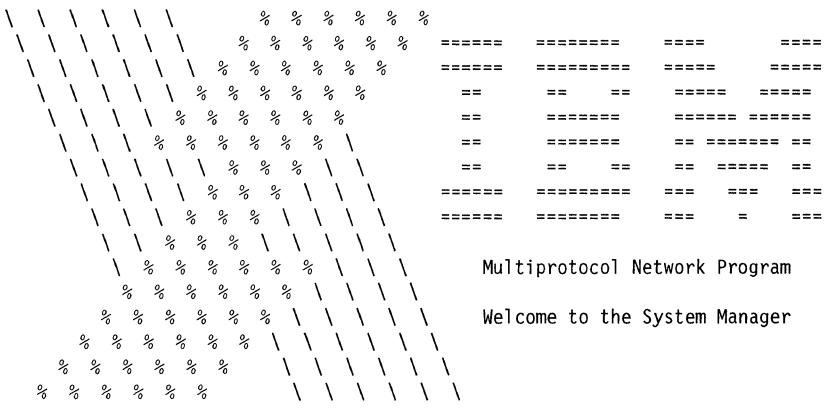
Output displayed:

```
Trying...

Connected to hostname.domainname.

Escape character is '^T'.


6611 telnet (hostname)
```




```
(c)Copyrights by IBM and by others 1992, 1994

hostname Login:
```

Type in:

userid

Output displayed:

```
userid's password:
```

Type in: (Enter the password. It will not be displayed.)

Output displayed:

```
The current terminal type is [sun].
Press the ENTER key to accept this value or
type NO to see a list of supported terminals.
```

Type in:

no

Output displayed:

```
                    SUPPORTED TERMINALS
                    --------- ---------
 1. ibm3101      2. ibm3151     3. ibm3161     4. ibm3162      5. ibm3163
 6. ibm3164      7. sun         8. vt100       9. vt320       10.  vt330
11. vt340       12. hft        13. vt100-am

     Type the number corresponding to your choice:
```

Type in:

```
12 (for example)
```

Output displayed: The main menu of the System Manager.

The last four steps can be eliminated if the remote station and the 6611 negotiate the correct terminal type. At the completion of the login process, control is passed to the System Manager. If you exit the System Manager using **F10 (Esc+0)** from the System Manager main menu, the remote connection is closed. To access the System Manager again, you are required to reenter the **telnet** command.

Refer to Chapter 1 and Chapter 2 for details about using the System Manager. If you want to execute 6611 functions that require controlling user privileges, you must log in with a controlling user ID. For more information about controlling user privileges, refer to "Tasks Restricted to Controlling Users" on page 3-16.

6611 to Any IP Station: A Telnet session can also be initiated from the 6611. This is accomplished with the System Manager or a fast-path environment command.

To initiate a Telnet session from a 6611 to another IP station using the System Manager:

1. Select **Operations** on the System Manager main menu.
2. Select **Remote Access to Other Nodes** on the next menu.
3. Select **telnet** on the selector screen.

A dialog screen appears requesting the host name or IP address of the remote IP station being accessed. After entering the host name, you are prompted for a user ID and password defined in the remote IP node. When you enter the password correctly, control is passed to the login environment of the remote station.

To initiate a Telnet session from the fast-path environment to another IP station, type:

telnet *dest_host_name*

where *dest_host_name* is the host name or IP address of the remote station. After issuing that command, you are prompted for a user ID and password defined in the remote IP node. When the password is entered correctly, control is passed to the login environment of the remote station.

Using Remote Login

There is an alternate method for one node on an IP network to reach another node on the IP network. It is called remote login, or rlogin. Using remote login, as with Telnet, a user at a station remote from another station can log in and interactively execute multiple commands at that station. Both stations must support rlogin to use this method. When a remote login session is established with a 6611, all the same tasks can be performed from the remote session as with the local attachment of the ASCII terminal to the EIA 232 serial ports.

Two rlogin session initiation procedures are outlined below:

- From a remote IP station to access a 6611
- From a 6611 to access any other IP station (including another 6611).

Remote IP Station to a 6611: The 6611 can be accessed from any station on the IP network using the **rlogin** command, provided the station supports rlogin. The remote login requires you to know the host name or IP address and a user ID and password configured for the 6611. User IDs and passwords must be configured using the Configuration Program, or by a controlling user using the System Manager. Refer to "Logging In to a 6611" on page 3-13 for more information about 6611 users.

The following steps show the details of a remote login session initiation from a remote station to a 6611. What you are expected to input from the remote station is provided under **"Type in"**. What you should expect to find displayed on the screen is provided under **"Output displayed"**.

Type in:

rlogin hostname (or IP address) -8 -l 6611_userid

The *-8* instructs the **rlogin** command to use eight bit communication for data transfer. This is necessary when data is transferred over multiple nodes. The *-l* tells the **rlogin** command that the user ID follows.

Output displayed:

```
userid's Password:
```

Type in: (Enter the password. It will not be displayed.)

Output displayed:

```
The current terminal type is [sun]. Press the ENTER key to
accept this value or type NO to see a list of supported terminals.
```

Type in:

no

Output displayed:

```
                    SUPPORTED TERMINALS
                    --------- ---------
 1. ibm3101     2. ibm3151     3. ibm3161     4. ibm3162      5. ibm3163
 6. ibm3164     7. sun         8. vt100       9. vt320       10.  vt330
11. vt340      12. hft        13. vt100-am

Type the number corresponding to your choice:
```

Type in:

12 (for example)

Output displayed: The main menu of the System Manager.

At the completion of the login process, control is passed to the System Manager. If you exit the System Manager using **F10 (Esc+0)** from the System Manager main menu, the remote connection is closed. To access the System Manager again, you must reenter the **rlogin** command.

6611 to Any IP Station: You can also initiate a remote login from the 6611. This is accomplished with the System Manager or a fast-path command.

To issue the **rlogin** command from a 6611 to another IP station on the same IP network using the System Manager:

1. Select **Operations** on the System Manager main menu.
2. Select **Remote Access to Other Nodes** on the next menu.
3. Select **rlogin–Remote login** on the selector screen.

A dialog screen appears requesting:

- Host name (or IP address) of the remote IP node
- User name (ID)

After you have completed these required fields, you are prompted for the password of the user ID given in the dialog. When you enter the password correctly, control is passed to the login environment of the remote station. If the remote IP station is another 6611, control is passed to the 6611's System Manager.

To initiate a remote login session from the fast-path environment to another IP station, type:

rlogin hostname userid

Where:

- hostname is the host name or IP address of the remote station
- userid is any configured user in the 6611 specified by the host name

After issuing that command, you are prompted for the password of the user ID. When you enter the password correctly, control is passed to the login environment of the remote station.

Using Rlogin for Extended Modem Connection

There are more IP stations supporting telnet than rlogin. The 6611 supports both methods. It is recommended that you use telnet for most of your remote session needs. However, the following scenario shows a particular situation in which an rlogin session is needed because a telnet session cannot work.

Scenario: A file needs to be transferred from one 6611 (referred to as 6611 A) to a station with an ASCII terminal that is modem-attached to another 6611 (6611 B).

Procedure:

1. The user at the ASCII terminal initiates the call to 6611 B and logs in to the 6611, specifying user ID, password, and terminal type when prompted.
2. From the System Manager main menu of 6611 B that is displayed automatically at login completion:
   a. Select **Operations** on the System Manager main menu.
   b. Select **Remote Access to Other Nodes** on the next menu.
   c. Select **rlogin–Remote login** on the selector screen.
3. A dialog screen appears on which the user types in the host name and a user ID at the 6611 A.
4. The user enters the password when prompted and control passes to the System Manager of the 6611 A.

5. From the System Manager main menu on IBM 6611 A:
    a. Select **Operations** on the System Manager main menu.
    b. Select **File and Diskette Operations** on the next menu.
    c. Select **Send Transfer Directory File** on the next menu.
    d. Select **modem connected host** on the selector screen.
    e. Supply the name of the file to send to the remote host on the next selector screen.
6. Return to the remote host connected to IBM 6611 B to receive the selected transferred file.

If in Step 2 on page 3-8, you prefer to use Telnet instead of rlogin, the transfer cannot be made directly to the ASCII terminal. A technical difference between Telnet and rlogin is that rlogin allows data transfer across many nodes, but Telnet does not. This is the only situation in which rlogin is preferred over Telnet. Refer to "Transferring Files" on page 4-62 for further details on file transfer.

Using Remote Execution

With the **telnet** and **rlogin** commands, you can have access to the full function of a 6611. However, there are scenarios when this is not needed. If you only need to execute a single command at a remote 6611, you can use **rexec**. To use the **rexec** command, it must be supported by the IP station issuing the command.

The 6611 supports the **rexec** command with a large number of commands. The commands and the parameters needed to execute them are listed under Chapter 9. They are summarized in the *IBM 6611 Network Processor Operations Pocket Guide*. Refer to "Using the Fast-Path Environment" for general information on using these commands, which are also supported in the fast-path environment. You may use online help from the fast-path environment to get detailed information on the commands. Most functions that can be performed from the System Manager can also be performed using the **rexec** command and the fast-path commands without logging into the 6611.

Each **rexec** command can execute one fast-path command at the 6611 to which the command is directed. The output from the fast-path command is displayed at the station that issued the **rexec** command. The station that issues the command can be any station on the same IP network as the 6611 to which the command is sent that supports remote execution.

Remote execution requires you to know the host name or IP address and a user ID and password configured for the 6611. User IDs and passwords must be configured using the Configuration Program or by a controlling user using the System Manager or a fast-path environment command. If you want to execute commands that require controlling user privileges, you are required to specify a controlling user ID when prompted. For more information about the commands that require controlling user privileges, refer to "Logging In to a 6611" on page 3-13.

The **rexec** command can be issued to the 6611 from a remote IP station. The following steps show the details of a remote execution scenario from a remote station to a 6611. Your input from the remote station is provided under **"Type in"**. The output that you should expect to see on the screen is provided under **"Output displayed"**.

Type in:

rexec hostname command-object subobject action -option parameters

The IP address of the 6611 can be used in place of the host name.

Output displayed:

```
Name (hostname:local_userid):
```

Type in:

remote_userid

Output displayed:

```
Password (hostname:remote_userid):
```

Type in: (Enter the password. It will not be displayed.)

Output displayed: Command output follows, if any.

Many of the commands place the command output in the transfer directory of the 6611 to which the command is directed. If these commands are issued from an RSH or REXEC environment, the **rsh** or **rexec** commands should be followed by an **ftp** to retrieve the output file. Refer to "Transferring Files" for information on using **ftp**.

Using Remote Shell

The remote shell (**rsh**) command can be used in a similar way to the **rexec** command. To use the **rsh** command, it must be supported by the IP station issuing the command. The 6611 supports the **rsh** command with a large number of commands. The commands and the parameters needed to execute them are listed under Chapter 9. They are summarized in the *IBM 6611 Network Processor Operations Pocket Guide*. Refer to "Using the Fast-Path Environment" for general information on using the commands. You may use online help from the fast-path environment to get detailed information on the commands. Most functions that can be performed from the System Manager can also be performed with **rsh** and the fast-path command without logging in to the 6611.

The rsh command executes fast-path commands one at a time at the 6611 to which the command is directed. The output from the command is displayed at the station at which the **rsh** command is issued. The station that issues the command can be any station on the same IP network as the 6611 to which the command is sent.

As with the rexec command, rsh requires you to know the host name or IP address, and a user ID and password configured for the 6611. If you want to execute 6611 functions that require controlling user privileges, you must specify a controlling user ID. For more information about the commands that require controlling user privileges, refer to "Logging In to a 6611" on page 3-13.

Two **rsh** command procedures are outlined below:

- From a remote IP station to access a 6611
- From a 6611 to access another 6611

Remote IP Station to a 6611: A typical situation for using a **rsh** command is within a script. A typical **rsh** command for the script is entered as follows:

rsh hostname -l userid passwd object subobject action -option parameters

Where:

- Hostname is the host name of the 6611 to which the command is sent. The IP address of the 6611 can be used in place of the host name.
- Userid is a user ID defined at the 6611 to which the command is sent.
- Passwd is the password for the user ID.
- Object subobject ... represent one of the supported commands.

The output of the command is displayed at the station issuing the **rsh** command.

6611 to Another 6611: To issue an **rsh** command from a 6611 to another 6611:

1. Select **Operations** on the System Manager main menu.
2. Select **Remote Access to Other Nodes** on the next menu.
3. Select **rsh–Remote Shell** on the selector screen.

A dialog screen appears requesting:

- Host name or IP address of the 6611
- User name
- Password
- Command
- Parameters for the command

Each of these fields can be edited using **F6 (Esc+6)**. A pop-up edit screen is displayed with a long line on which to type the input. This is especially helpful when typing in a long command.

Comparing REXEC and RSH

Remote execution and remote shell perform the same tasks using the fast-path commands. The main difference is in how you issue the commands. When the **rsh** command is sent to the 6611, you are not prompted for the user ID and password. The user ID and password must be typed on the command line. This allows the **rsh** command and fast-path commands to be combined in a user-written script containing more than one **rsh** command with or without the **ftp** command. This allows you to perform several functions while only issuing one script.

IBM suggests that you use the **rexec** command when you need to execute a 6611 command outside of a user-written script. This is because the password is not displayed as it is typed in after the prompt. With the **rsh** command, the password must be typed on the command line with the password in full view. If the screen output is saved, the password is also visible in the saved data.

Some of the commands place the command output in the transfer directory of the 6611 to which the command is directed. If these commands are issued from an RSH or REXEC environment, the **rsh** or **rexec** commands should be followed by an **ftp** command to retrieve the output file. Refer to "Transferring Files" on page 4-62 for further details on using **ftp**.

The fast-path log option on commands is not available in the RSH or REXEC environments.

Using a Modem

Remote access to the 6611 can also be reached through a modem that is connected to an EIA 232 serial port. The modem should be 2400 baud and compatible with the Attention (AT) Command Set. When the terminal is connected through the modem to the port, a login procedure is initiated. You are asked to supply the terminal type you are using immediately after login verification. After you have supplied the correct terminal type, the main menu of the System Manager is displayed.

When a connection is made using a modem, it is possible for you to access any 6611 on the IP network using the network connection commands (**telnet, rlogin, rsh, and ftp**). You can have full remote modem access to any 6611 on the network using only one modem connection. For most purposes, the single modem can be attached to an IP workstation instead of a 6611 as long as the station supports **rlogin**.

When the modem connection is established, the call must be initiated from a station that is not a 6611. The 6611 does *not* support connection initiation. It can only receive the switched call.

There are three tasks you may need to perform to set up the modem connection physically:

1. Plug the modem into one of the EIA 232 serial ports.
2. If necessary, change the line speed (baud rate) of the serial port for a modem connection.

   The S1 or Serial 1 serial port is initially configured with a baud rate of 9600 bps.

   The S2 or Serial 2 serial port is initially configured for use with a modem with a baud rate of 2400 bps.

   You can change the baud rate of the serial port with the Configuration Program or from the fast-path environment. To change the baud rate of the serial port using a fast-path command, use:

   serialport baud set -s1 *baud_rate*
   serialport baud set -s2 *baud_rate*

   Use online help from the fast-path environment for more details about this command.
3. Enable auto-answer mode for the modem.

   The method for enabling auto-answer mode for the modem you purchased depends on the modem. Some modems may contain a physical switch for this function. Others require an AT command to be sent to the modem over the EIA 232 serial port. Please read the documentation that accompanies the modem to see which method to use.

Refer to "EIA 232 Serial Ports" on page 4-54 for information using the EIA serial ports to send AT commands.

To establish a modem connection, you initiate the call from a remote station that supports CALLOUT. If you want to transfer files, this station must also support the Xmodem Protocol. Xmodem is available with many communication packages for personal computers and workstations and is used to access the 6611's

asynchronous serial line. Read the documentation sent with the communication package to understand the details of establishing the connection.

To establish a connection, you are required to know the telephone numbers and serial line parameters of the phone line of the modem you are calling. Refer to "Transferring Files between a RISC System/6000 and a 6611" on page 4-70 for information about the procedure for transferring files from a RISC System/6000 workstation using a modem connection.

When the connection to the 6611 is established, you are prompted for a user ID and password that have previously been configured for the 6611 on the receiving end of the switched connection. Refer to "Logging In to a 6611" for further discussion about the login procedure.

To access a 6611 that is on the IP network but not equipped with a modem, it is necessary to establish an rlogin session between the 6611 that needs to be accessed and the IP station on the network equipped with the modem. The remote login is initiated from the 6611 or another IP node in the network equipped with the modem. If a node other than a 6611 has the modem, it must support rlogin and Xmodem commands for transferring files. Refer to "Using Remote Login" on page 3-6 for details of the remote login procedure.

Verifying a Link Connection

You may need to determine if you can reach another node in your network. These protocols provide an echo facility that you can use to verify connection to another node:

- IP
- AppleTalk
- XNS
- VINES
- IPX**

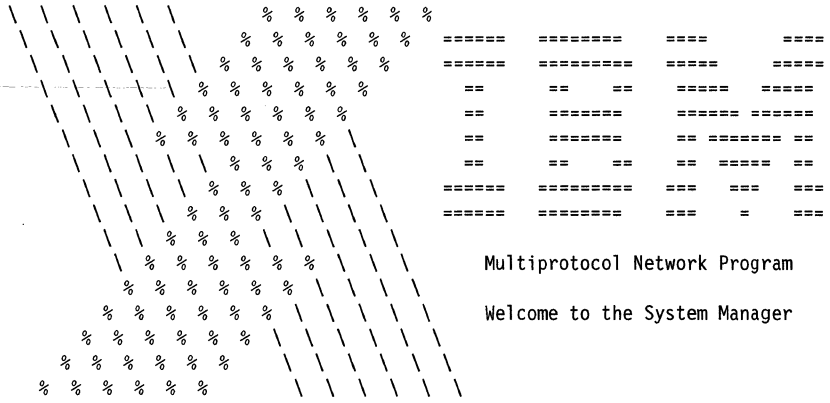
In addition, the IP protocol has a route trace facility. For information on using the echo facilities with the various protocols, or using the route trace facility, refer to "Remote Host Echo (Ping)/Route Trace" on page 4-18.

Logging In to a 6611

If you are local or remote and using a network connection or a modem connection, the login procedure for the 6611 is the same. You are prompted for a user ID, password, and terminal type. The login scenario for remote access using the Telnet command is found in "Using Telnet" on page 3-4. The login scenario for remote access using the rlogin command is found in "Using Remote Login" on page 3-6.

The following steps show the details of the login procedure from a terminal connected to the S1 or S2 serial port, either directly or through a modem. Your input from the ASCII terminal is provided under **"Type in"**. The output that you should expect to see displayed on the screen is provided under **"Output displayed"**.

Output displayed:




```
(c)Copyrights by IBM and by others 1992, 1994
hostname Login:
```

Type in:

userid

Output displayed:

```
userid's password
```

Type in: (Enter the password. It will not be displayed.)

Output displayed:

```
The current terminal type is [vt100].
Press the ENTER key to accept this value or
type NO to see a list of supported terminals.
```

Type in:

no

Output displayed:

```
                    SUPPORTED TERMINALS
                    --------- ---------
 1. ibm3101     2. ibm3151    3. ibm3161    4. ibm3162     5. ibm3163
 6. ibm3164     7. sun        8. vt100      9. vt320      10.  vt330
11. vt340      12. hft       13. vt100-am

Type the number corresponding to your choice:
```

Type in:

6 (for example)

Output displayed: The main menu of the System Manager.

When logging in through the EIA 232 serial ports, the terminal type chosen on the previous login is presented as the default type. It is assumed that the terminal type used for this connection is normally the same from login to login.

At the completion of the login process, control is passed to the System Manager. If you exit the System Manager using **F10 (Esc+0)** from the System Manager main menu, you will return to the login prompt.

User IDs and Passwords

To log into the 6611, you are required to have a user ID and password. There are two classes of users:

- Controlling

  Controlling users have access to and can perform all System Manager functions.

- Viewing

  Viewing users have limited access to System Manager functions.

You can configure multiple controlling and viewing users. Up to 10 users, either controlling or viewing, can be logged into the 6611 simultaneously. However, IBM recommends that you only allow up to five users at one time to improve system performance.

User IDs and passwords are defined using either the Configuration Program, the System Manager, or commands in the fast-path environment. Both the user ID and the password must be defined together.

Two default user IDs are preconfigured with the 6611:

- `ibm6611c`–a controlling user ID
- `ibm6611v`–a viewing user ID

The password for each user ID is the user ID itself. The default user IDs are to be used during initial configuration of the 6611, if performed using the System Manager. Refer to "Initial Configuration without Using a Diskette" on page 6-11 for details about using the System Manager for initial configuration.

IBM recommends that you delete these user IDs or change the passwords immediately after receiving the 6611. Refer to "User IDs and Passwords" on page 6-17 for details of setting user IDs and passwords.

Tasks Restricted to Controlling Users

Many of the System Manager functions require controlling user privileges. If you attempt to execute a System Manager function from a viewing user ID that requires controlling user privileges, you will receive a message similar to the one shown here:

```
Only a controlling user can perform this function.
```

The following list shows all the functions that only a controlling user can perform. Each of the menu items is listed under the main menu item under which it appears. Menu items are listed as they appear on System Manager menu screens, except for the text within parentheses. This text is added to provide context for the functions.

- Operations
  - Protocol and Interface Monitor
  - Add IP ARP Entry
  - Delete IP ARP Entry by Host Name
  - Delete IP ARP Entry by Hardware Address
  - Delete All IP ARP Entries
  - Rename Transfer Directory File
  - Delete Transfer Directory Files
  - Compress/Uncompress Transfer Directory Files
  - Clear Log File
  - Login Information
  - System Activity Report
  - EIA/232 Serial Ports
  - System Shutdown
  - Date and Time
- Problem Determination
  - Process Table Information
  - Virtual Memory (System Statistics)
  - Input/Output (System Statistics)
  - Three-Digit LED Display
  - Clear the Error Log
  - Start (System Dump)
  - View Dump Information (System Dump)
  - Copy to Diskette or Transfer Directory (System Dump)
  - Format (System Dump)
  - Extract Error Log Records
  - Extract Trace Log Records
  - Start Nondisruptive (Process Dumps—IP, VINES, APPN*)
  - Start Disruptive (Process Dumps)
  - Start (System Trace)
  - Stop (System Trace)
  - Start (Process Traces)
  - Stop (Process Traces)
  - Read Memory (Adapter Debug)
  - View Registers (Adapter Debug)
  - Start Line Trace (Adapter Debug)
  - Dump Memory (Adapter Debug)
  - DLSw General Information (Protocol Debug)
  - X.25 Traffic Monitor (Protocol Debug)

- Protocol Debug Collection Facility (Protocol Debug)
- Concurrent Hardware Diagnostics

- Configuration
  - System Manager Configuration Utility
  - List All User IDs
  - Add a User ID
  - Delete a User ID
  - Change Any Password
  - Change Your Password
  - Apply Changes
  - Commit Changes
  - Reject Uncommitted Changes
  - Receive and Apply Configuration
  - Reinstate a Saved Configuration
- Software Installation and Maintenance
  - Receive Installation File(s)
  - List Installation Files
  - List All Problems Fixed by Software Updates
  - Apply Software Updates
  - Clean Up after a Failed Installation
  - List All Applied but Not Committed Software
  - Commit Applied Updates
  - Reject Applied Updates
- Hardware Maintenance
  - Configuration Change VPD Update
  - Serial Number
  - Model Number

Chapter 4. Operations

About This Chapter

This chapter provides information about logging into the 6611 and about using the Operations facilities provided by the System Manager. Operations tasks may be selected from the Operations menu. Tasks are presented so that those that may have to be done more often are at the top of the list.

Figure 4-1 shows the Operations menu.

```
IBM 6611                                                          hostname
                                  Operations

Move cursor to desired item and press Enter.

  Protocol and Interface Monitor
  Routing Information
  Remote Host Echo (Ping)/Route Trace
  Network Statistics
  ARP Table Management
  Port Filters
  Network Management Information (MIBs)

  File Systems
  File and Diskette Operations
  Remote Access to Other Nodes
  Login Information
  System Activity Report
  EIA 232 Serial Ports
  System Shutdown
  Date and Time


F1=Help            F2=Redraw Screen    F3=Return          F4=SysID
F10=Main Menu                          Esc+L=Turn Log On
```

Figure 4-1. Operations Menu

Refer to the following for information about the individual menu items:

Using the 6611 Operations Facilities

To gather the operations data, select **Operations** from the System Manager main menu, and the menu in Figure 4-1 on page 4-3 is displayed.

Making selections from the Operations menu lets you gather information about the performance of many of the components in the 6611, including:

- Main operating system
- Running user processes
- Installed adapters
- Configured protocols
- Hard disks
- Network, as viewed from both the adapters and the main system

The Simple Network Management Protocol (SNMP) Management Information Base (MIB) variables can also be viewed from this menu.

Most output is displayed on the screen if it is less than 512 kilobytes long. If it is more than 512 K bytes, you can view it from the fast-path environment.

Output can also be sent to the System Manager log in the transfer directory. To start this, you must turn the log on (**Esc+L**). When the notation at the bottom of each System Manager menu shows **Esc+L=Turn Log Off**, the log is on.

When the output is placed in the transfer directory, it can be sent to a diskette or transferred to a remote node. When the remote node is attached through the Internet Protocol (IP) network, the output must be sent using the File Transfer Protocol (FTP). When the 6611 is accessed using a modem, the output must be sent using the Xmodem Protocol.

Protocol and Interface Monitor

The protocol and interface monitor displays the number of packets sent and received for each protocol or installed adapter. The monitor periodically updates the packet traffic information screen until you press **Ctrl+C** to stop it.

To monitor protocol or interface packet traffic using the System Manager:

1. Log in using a controlling user ID.
2. Select **Operations** from the System Manager main menu.
3. Select **Protocol and Interface Monitor** from the next menu.

   Figure 4-2 on page 4-5 shows the dialog screen that appears.

```
IBM 6611                  Protocol and Interface Monitor          hostname

Type or select values in entry fields.
Press Enter after making all desired changes.

                                                          [Entry Fields]
* Number of seconds between displays                    [60]                  #
* Display protocols or interfaces?                       protocols            +

  This is a continuous display.









F1=Help             F2=Redraw Screen    F3=Return           F4=List
F5=Undo             F6=Edit             F7=Page Up          F8=Page Down
F10=Main Menu                           Esc+L=Turn Log On
```

Figure 4-2. Protocol and Interface Monitor Dialog Screen

4. Enter the number of seconds between information updates on the output screen. The number of seconds has a minimum value of 10 and a maximum value of 60. The default is 60 seconds. IBM recommends you accept the default to minimize the monitor's use of system resources.
5. Select **protocols** or **interfaces** to determine where to monitor packet throughput. The default is **protocols**.
6. Press **Enter** to start monitoring packet traffic.

   Figure 4-3 on page 4-6 shows an example of the output produced when you select **protocols**.

```
                PACKET TRAFFIC INFORMATION FOR PROTOCOLS

Protocol      rcv       xmt    Status| Protocol      rcv       xmt    Status
ip           1135       330      up |
tcp           261       226      up |
udp           802        99      up |
snmp           59        50      up |
ppp             4        23      up |
decnet          0         0    down |
dls             0         0    down |
FmRl            0         0    down |
Brdg            0         0    down |
ipx             0         0    down |
xns             0         0    down |
APPN            0         0    down |
AppTk           0         0    down |
TBrdg           0         0    down |
Vines           0         0    down |

                Press Ctrl+C  to return to System Manager
```

Figure 4-3. Sample Protocol Monitor Output

The output contains these fields:

Protocol Name of the protocol

rcv Number of packets received

xmt Number of packets transmitted

Status Protocol status

If the status is `up`, the protocol is enabled and running. If the status is `down`, the protocol is either not enabled or has stopped.

Figure 4-4 on page 4-7 shows an example of the output produced when you select **interfaces**.

```
                PACKET TRAFFIC INFORMATION FOR INTERFACES

Interface    rcv         xmt Status| Interface    rcv         xmt Status
lo0          386         386    up
tk0        13592         146    up
do0            0           0  down
do1            0           0  down
do2            4          36    up
ct0            0           0  down

                Press Ctrl+C  to return to System Manager
```

Figure 4-4. Sample Interface Monitor Output

The output contains these fields:

Interface Interface name.

Refer to Table 4-1 for a description of the possible interface names. The monitor only lists installed adapters.

rcv Number of packets received

xmt Number of packets transmitted

Status Interface status.

If the status is `up`, the interface is installed and configured. If the status is `down`, the interface is physically installed but not configured.

7. Press **Ctrl+C** to end this command.

Table 4-1 (Page 1 of 2). Adapter Interface Name Table

Interface Name	Adapter or Interface
tk#	1-port token-ring network 16/4 adapter
to?	2-port serial adapter
te#	1-port Ethernet adapter
xt%	X.25 adapter
mpq&	SDLC adapter
ce+	Serial or Ethernet interface on the serial/Ethernet combination adapter
ct+	Serial or token-ring interface on the serial/token-ring combination adapter
de?	2-port Ethernet adapter

Table 4-1 (Page 2 of 2). Adapter Interface Name Table

Interface Name	Adapter or Interface
do@	4-port serial adapter
dt?	2-port token-ring network 16/4 adapter
lo$	Internal wrap test network interface, loopback

Legend:

#	A number from 0 to 6
?	A number from 0 to 13
%	A number from 0 to 3
&	A number from 0 to 23
$	Either 0 or 1
+	A number from 0 to 20
@	A number from 0 to 27

Fast-Path Command(s)

system statistics monitor [(-protocol)|-interface] *number_seconds*

Routing Information

From the Routing Information menu (as shown in Figure 4-5), you can display the route table and request specific routing information on supported protocols. You can also display the complete route table or only the portion pertaining to a specific protocol. You can access the Routing Information menu from the Operations menu of the System Manager.

```
IBM 6611                                                          hostname
                              Routing Information

Move cursor to desired item and press Enter.

  Route Tables

  AppleTalk Zone Information Table
  VINES Neighbor Tables
  DLSw Partners
  DECnet Routing Information
  OSPF Routing Information









F1=Help            F2=Redraw Screen    F3=Return           F4=SysID
F10=Main Menu                          Esc+L=Turn Log On
```

Figure 4-5. Routing Information Menu

The following sections explain how to accomplish the tasks presented on the Routing Information menu using the System Manager.

Route Tables

The route tables contain the routes for lists of valid paths through which hosts or a network can communicate with other hosts in that network. Route tables are supported for most of the configured protocols in the 6611.

To view a route table using System Manager:

1. Select **Operations** on the main System Manager menu.
2. Select **Routing Information** on the next menu.
3. Select **Route Tables** on the next menu.
4. Select a protocol or All protocols from the selector screen (refer to Figure 4-6). The supported protocols are:
   - IP
   - XNS**
   - IPX
   - DECnet
   - VINES
   - AppleTalk
5. A COMMAND STATUS screen will display the output. The display format indicates the available routes and their states.

```
IBM 6611                                                          hostname
                              Routing Information

Move cursor to desired item and press Enter.

  Route Tables

  AppleTalk Zone Information Table
    ┌──────────────────────────────────────────────────────────────────┐
    │                            Protocol name                         │
    │                                                                  │
    │ Move cursor to desired item and press Enter.                     │
    │                                                                  │
    │   All protocols                                                  │
    │   IP         - Internet Protocol                                 │
    │   XNS        - Xerox Network Services Internet Transport Protocol│
    │   IPX        - Internet Packet Exchange Protocol                 │
    │   DECnet     - Digital Network Architecture Protocol             │
    │   VINES      - Banyan Virtual Networking System Protocol         │
    │   AppleTalk - AppleTalk Network Protocol                         │
    │                                                                  │
    │ F1=Help                F2=Redraw Screen       F3=Return          │
    │ F5=Top                 F6=Bottom              F7=Page Up         │
    │ F8=Page Down           F10=Main Menu                             │
F1  │                                                                  │
F1  └──────────────────────────────────────────────────────────────────┘
```

Figure 4-6. Route Tables Selector Screen

Fast-Path Command(s)

system routes view {-log}
ip routes view -system
xns routes view -system
ipx routes view -system
decnet routes view -system
vines routes view -system
appletalk routes view -system

For IP, IPX, XNS, VINES, and DECnet, each route consists of a destination host or network and a gateway to use when forwarding packets. Direct routes are created for each interface attached to the local host. These routing tables contain the fields:

Destination Provides the IP address or host name at the end of the route.

Gateway Provides the address of the outgoing interface.

Flags Shows the state of the route:

- U Up
- H The route is to a host rather than to a network.
- G The route is to a gateway. (This is an indirect route.)
- D The route was created dynamically by a redirect.
- M The route has been modified by a redirect.
- L The link-level address is present in the route entry.

Refcnt Gives the current number of active uses for the route. Connection-oriented protocols hold on to a single route for the duration of a connection, while connectionless protocols obtain a route while sending to the same destination.

Use Provides a count of the number of packets sent using that route.

Interface Indicates the network interfaces used for the route. Refer to Table 4-1 on page 4-7 for a description of the interface names used to identify the adapters.

Figure 4-7 shows an example of an IP route table.

```
Routes for the Internet Protocol Family:
Destination      Gateway                 Flags  Refcnt      Use  Interface
-------------------------------------------------------------------------
1.1.1            1.1.1.4                 U          2    18172  tk0
9.67             1.1.1.2                 UG         0    14519  tk0
127              127.0.0.1               U          0        0  lo0
127.0.0.1        127.0.0.1               UH         5    80900  lo0
224.0.0.9        127.0.0.1               UH         0        0  lo0
```

Figure 4-7. Example of Route Table for IP

For AppleTalk, the route tree contains one entry for each network that the 6611 Each entry is composed of these fields:

Network Identifies the destination network

Hop Cnt Distance to the destination network, measure in hops

Next Net.Next Hop Node address of the next router in the path to the destination network

Interface Indicates the network interfaces used for the route Refer to Table 4-1 on page 4-7 for a description of the interface names used to identify the adapters.

Rte State Identifies the current state of the route, either good, suspect, or bad

```
Route Tree for AppleTalk:

   Network      Hop Cnt     Next Net.Next Hop   Interface         Rte State
     5            1               0           tk0               good
    31-36         3              11           do1               good
     84           2              11           do1               good

Total number of AppleTalk networks: 8
```

Figure 4-8. Example of Route Table for AppleTalk

AppleTalk Zone Information Table

An AppleTalk zone is an administrative grouping of networks. This table lists the zone name and ranges of network addresses contained within each AppleTalk zone.

To view AppleTalk zone information using the System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **Routing Information** from the next menu.
3. Select **AppleTalk Zone Information Table** from the next menu.
4. A COMMAND STATUS screen will display with the table information. An example of the output for an AppleTalk zone table is in Figure 4-9.

Fast-Path Command(s)

appletalk zones view

```
Zone: myZone  contains these nets:
 1234-1245   1255-1267   1300-1399   1450-1455   1460-1465
 1477-1477
Zone: herZone  contains these nets:
  222-225       5-6

Total number of zones: 2
```

Figure 4-9. AppleTalk Zone Output

VINES Neighbor Tables

This table contains information on neighboring VINES nodes.

In some cases, neighboring VINES nodes may go off-line or change their VINES network numbers, and the 6611 might not be aware of changes. If this occurs, you must manually delete the obsolete neighbors' entries from the 6611 VINES neighbor table by using System Manager.

Using System Manager to delete the obsolete addresses is necessary only if the Enable periodic full routing updates parameter is not enabled on the 6611 interface to which the VINES neighbors are connected. If the Enable periodic full routing updates parameter is enabled, then the 6611 will automatically remove these addresses after not hearing from them after approximately six minutes.

To view VINES neighbor table information using the System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **Routing Information** from the next menu.
3. Select **VINES Neighbor Tables** from the next menu.
4. Select one of these choices from the selector screen:
   - **view system**–to view the entire VINES neighbor table
   - **view interface**–to view the VINES neighbor table entries pertaining to a specified interface

     Refer to Table 4-1 on page 4-7 for a description of the interface names used to identify the adapters.
   - **delete entry**–to delete an entry from the VINES neighbor table
5. A COMMAND STATUS screen displays the VINES neighbor table information. An example of the output is in Figure 4-10 on page 4-13.

Fast-Path Command(s)

vines neighbors view -all
vines neighbors view *interface*
vines neighbors delete *net_number*

The VINES neighbor table contains these fields:

Network ID A 4-byte hexadecimal network ID.

Intf Indicates the network interface used for the route. Refer to Table 4-1 on page 4-7 for a description of the interface names used to identify the adapters.

Link address For an interface (Intf) value of:

tk# or te#	Indicates the MAC address of the network interface
to?	Indicates the DLCI address of the network interface

Metric Displays the value assigned by VINES to select the best route.

TTL Shows the time left, in seconds, before the route is aged out.

Flags Shows the state of the route:

U Up
P Permanent
C Change
R Redirect
S Suppress

RI Routing information (Token-Ring specific information)

```
Network ID    Intf    Link address    Metric   TTL    Flags

3080abab:0001 te0     08005a13209c    2        360    U
0027d089:0001 te0     10025a8229f7    2        360    U
0027d389:0001 tk0     10035a8229f7    2        360    U
RI=9000:2000:2000:1000:2300
00274089:0001 tk0     10045a8229f7    2        360    U
```

Figure 4-10. VINES Neighbor Table Output

DLSw Partners

Select this option to view the DLSw partners' addresses and the state of the connections. To get a list of the DLSw partners, and the connection state to the partners:

1. Select **Operations** from the System Manager main menu.
2. Select **Routing Information** from the next menu.
3. Select **DLSw Partners** from the next menu.
4. A COMMAND STATUS screen will display the DLSw partner connection state information. An example of the output is in Figure 4-11.

Fast-Path Command(s)

dlsw partners view

```
DLSw PARTNER          CONNECTION STATE
*.*                   LISTEN
125.5.5.1.2065        ESTABLISHED
125.5.5.1.2067        ESTABLISHED
```

Figure 4-11. DLSw Partners Output

DECnet Routing Information

This selection lets you view DECnet routing data base members. You may view a whole member, starting with the first entry, or choose a starting point entry.

To view DECnet routing information using the System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **Routing Information** from the next menu.

3. Select **DECnet Routing Information** from the next menu.
4. Select the data structure option you want from the selector screen.

   The data structures are defined as follows:

   hop matrix path length from the 6611 to the destination address.

   cost matrix path cost from the 6611 to the destination address.

   minimum hop vector path length of the least cost path from the 6611 to the destination address.

   minimum cost vector path cost of the least cost path from the 6611 to the destination address.

   area hop matrix path length from the 6611 to the destination area.

   area cost matrix path cost from the 6611 to the destination area.

   area minimum hop vector path length of the least cost path from the 6611 to the destination area.

   area minimum cost vector path cost of the least cost path from the 6611 to the destination area.

   reach vector whether the destination address is reachable.

   area reach vector whether the destination area is reachable.

   output adjacency vector identifies adjacency (next node) on which to forward packets to the destination address.

   area output adjacency vector identifies adjacency on which to forward packets to the destination area.

   adjacency vector supplies information on each adjacency.

   circuit vector supplies information on each circuit (interface).

   executor information supplies global DECnet information.

   Depending on your selection, you will get a dialog screen on which to supply information, such as the number of entries to display, and which entry with which to start. (The defaults depend on the information selected.)

Fast-Path Command(s)

decnet routes view -route_info
plus appropriate option and parameters

OSPF Routing Information

To view OSPF routing information using the System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **Routing Information** from the next menu.
3. Select **OSPF Routing Information** from the next menu.
4. Select the type of routing information from the next menu. Refer to Figure 4-12 for the OSPF Routing Information menu.

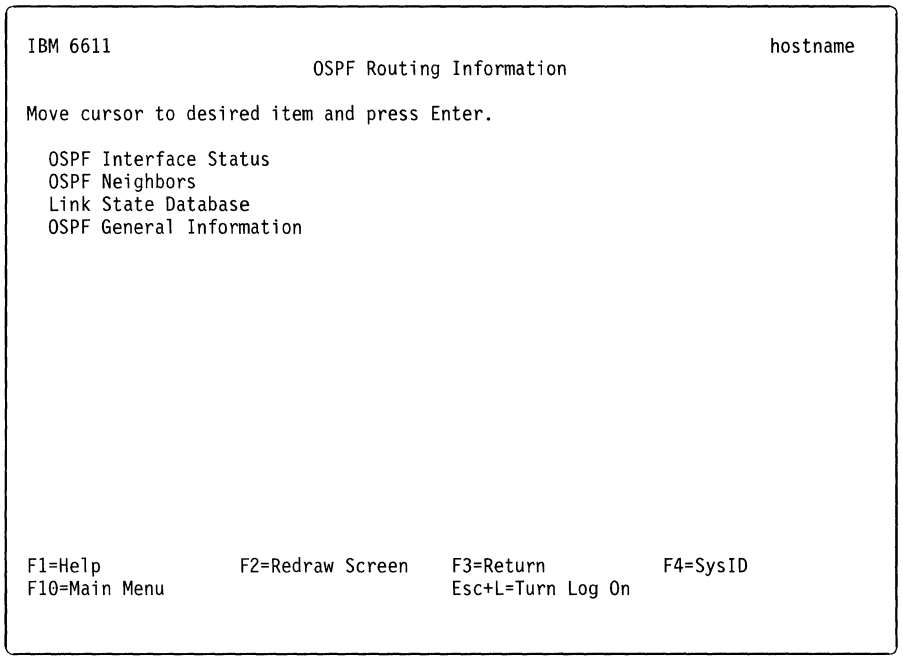


Figure 4-12. OSPF Routing Information Menu

5. A COMMAND STATUS screen will display the output.

Fast-Path Command(s)

ip ospf view [(-neighbors) | -interface | -lsdb | -general_info] *IP_address*

An example of the output for OSPF interface status is in Figure 4-13.

```
  Area      IP Address       Type  State    Pri    DR             BDR
-------------------------------------------------------------------------
0.0.0.0     211.7.192.202    Bcast DR       1    211.7.192.202    0.0.0.0
0.0.0.0     211.7.192.227    PtoP  P To P   0    0.0.0.0          0.0.0.0
0.0.0.0     211.7.192.230    PtoP  P To P   0    0.0.0.0          0.0.0.0
```

Figure 4-13. Sample OSPF Interface Status Output

The output contains these fields:

Area OSPF area ID for this 6611

IP Address Interface IP address

Type (interface)

- Bcast: Broadcast or point-to-point
- PtoP: Point-to-point
- NBMA: Non-Broadcast multi-access

State (interface)

- Down: The interface is down
- Loopbck: The interface used for loopback
- Waiting: The interface is waiting

- P to P: The interface is point-to-point
- DR: Designated router
- DR Othr: The interface is eligible to be the designated router
- Bckup DR: Backup designated router

Pri (priority) 0 means the neighbor router is not the designated router

1-255 means the designated router is the one with the highest number.

DR The IP address of the current designated router

BDR The IP address of backup designated router

An example of the output for OSPF neighbors is inFigure 4-14 .

```
  Router Id      Nbr IP Addr     State     Pri
---------------------------------------------
211.7.192.158   211.7.192.226   Full      0
211.7.192.81    211.7.192.231   Full      0
```

Figure 4-14. Sample OSPF Neighbors Output

The output contains these fields:

Router ID The neighbor's router ID. There is a unique ID for each router equal to one of its IP addresses.

Neighbor IP address

The IP address of the neighbor's interface that is directly attached.

Neighbor state

- Down: The neighbor is unreachable
- Attempt: Attempting to communicate with the neighbor
- Init: One-way communication is established with the neighbor
- 2 Way: Two-way communication is established with the neighbor
- Exch Start: Starting to exchange OSPF databases with the neighbor
- Exchange: Exchanging OSPF databases with the neighbor
- Loading: Exchanging OSPF databases with the neighbor
- Full: 6611 and neighbor databases are synchronized

Neighbor interface priority

0 means the neighbor router is not the designated router.

1 - 255 means the designated router is the one with the highest number.

An example of the output for link state database is in Figure 4-15 on page 4-17.

```
  Area        LSType Link ID         Adv Rtr         Age   Sequence
-----------------------------------------------------------------------
0.0.0.0       Router 211.7.192.50    211.7.192.50    743   80000280
0.0.0.0       Router 211.7.192.81    211.7.192.81    863   8000005B
0.0.0.0       Router 211.7.192.97    211.7.192.97    1161  80000A31
0.0.0.0       Router 211.7.192.101   211.7.192.101   819   8000151F
0.0.0.0       Router 211.7.192.138   211.7.192.138   259   800002BD
0.0.0.0       Router 211.7.192.158   211.7.192.158   325   80000240
0.0.0.0       Router 211.7.192.179   211.7.192.179   327   8000028A
0.0.0.0       Router 211.7.192.202   211.7.192.202   231   80000238
0.0.0.0       Net    211.7.192.101   211.7.192.101   1364  800003CD
```

Figure 4-15. Sample Link State Database Output

The output contains these fields:

Area OSPF area ID for this 6611

LSType The type of link state advertisement for the advertising node:

- Router: The advertisement is for another OSPF router
- Network: The advertisement is for a network
- SumNet: The summary advertisement of a network in another area
- SumASB: The summary advertisement of an autonomous system border (ASB) router
- ASE: The advertisement of an autonomous system external router

Link ID The interface IP address forwarding advertisement

Adv Rtr The router ID of the router that originated the link state advertisement

Age Elapsed time in seconds since the advertisement was originated

Sequence The version of the advertisement from the originator

An example of the output for OSPF general information is in Figure 4-16 .

```
RouterId:             211.7.192.202
AdminStatus:          enabled       Version:                2
Area Border Router:   false         External LSA Count:     2
AS Border Router:     false         External LSA Checksum:  0x190c0
TOS Support:          false
```

Figure 4-16. Sample OSPF General Information Output

The output contains these fields:

RouterId A unique ID for each router equal to one of its IP addresses.

AdminStatus Enabled: OSPF is enabled

Disabled: OSPF is disabled

Version The version of OSPF code

Area Border Router True: The 6611 is an area border router

False: The 6611 is not an area border router

AS Border Router True: The 6611 is an autonomous system b rder Router

False: The 6611 is not an autonomous system border Router

TOS Support True: 6611s support type of service

False: 6611s do not support type of service

External LSA Count The number of external link state advertisements

External LSA Checksum

Database checksum of the external link state advertisements

Remote Host Echo (Ping)/Route Trace

The echo facilities send ECHO_REQUESTS to obtain ECHO_RESPONSES from the destination nodes. They are useful to:

- Determine the status of the network and various remote stations
- Track and isolate hardware and software problems
- Test, measure, and manage networks

If the station is operational and the station is on the network, it responds to the echo.

The echo commands calculate round-trip times and packet loss statistics, and display a brief summary upon completion. They complete after sending a specified number of echo requests. Echo requests can be issued from the System Manager or from the fast-path environment.

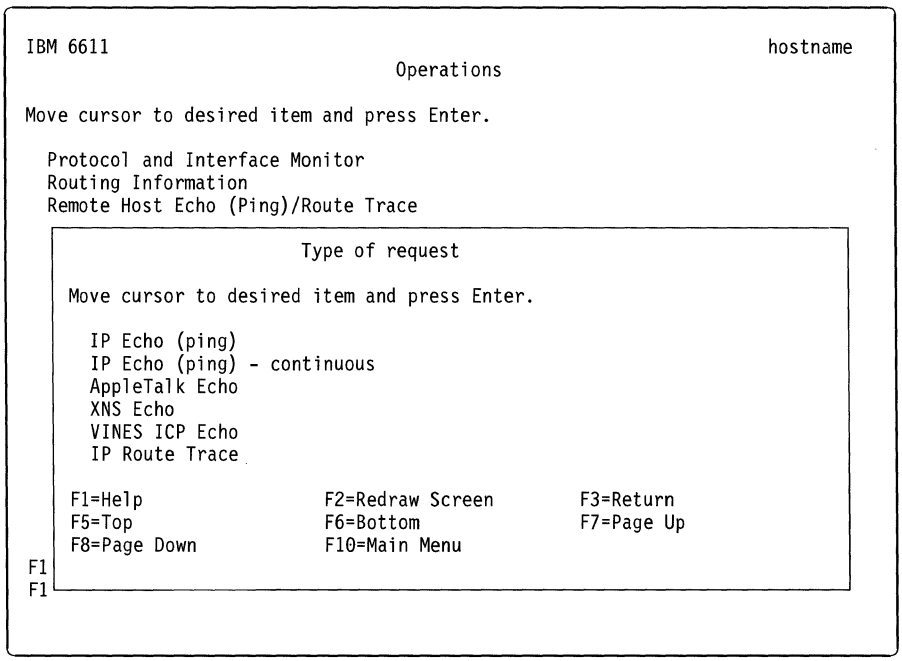


Figure 4-17. Remote Host Echo(Ping)/Route Trace Selector Screen

IP Echo (ping)

To issue a discrete number of IP echo requests to another node:

1. Select **Operations** from the System Manager main menu.
2. Select **Remote Host Echo (Ping)/Route Trace** from the next menu.
3. Select **IP Echo (ping)** on the selector screen as shown in Figure 4-17 on page 4-18.
4. Enter the following information on the dialog screen:
   - Host name or IP address

     The destination IP node for the echo request packets
   - Packet size

     The number of bytes sent with each echo request. The default is **64**.
   - Number of echoes

     The number of echo requests sent to the destination. The default is **3**.
5. Press **Enter** to activate your request.
6. A COMMAND STATUS screen will display the output.

Note: The IP echo command is commonly known as *ping*. Full ping support is only provided in the fast-path environment.

Fast-Path Command(s)

ip echo *dest_host_name packet_size num_echoes*

IP Echo (ping) - continuous

To issue IP echo requests to another node continuously:

1. Select **Operations** from the System Manager main menu.
2. Select **Remote Host Echo (Ping)/Route Trace** from the next menu.
3. Select **IP Echo (ping) - continuous** on the selector screen as shown in Figure 4-17 on page 4-18.
4. Enter the following information on the dialog screen:
   - Host name or IP address

     The destination IP node
   - Packet size

     The number of bytes sent with each echo request. The default is **64**.
   - Echo interval

     The number of seconds the 6611 waits between sending echo request packets. The default is **2**.
5. Press **Enter** to activate your request.
6. Press **Ctrl+C** to end your request.

Note: The IP echo command is commonly known as ping. Full ping support is only provided in the fast-path environment.

Fast-Path Command(s)

ip echo -continuous *dest_host_name packet_size num_echoes*

AppleTalk Echo

To issue AppleTalk echo requests to another node:

1. Select **Operations** from the System Manager main menu.
2. Select **Remote Host Echo (Ping)/Route Trace** from the next menu.
3. Select **AppleTalk Echo** on the selector screen as shown in Figure 4-17 on page 4-18.
4. Enter the following information on the dialog screen:
   - AppleTalk network id

     Unique for each AppleTalk network address
   - AppleTalk node id

     Unique for each AppleTalk network address
   - Number of echoes

     The number of echo requests sent to the destination. The default is **3**.
5. Press **Enter** to activate your request.
6. A COMMAND STATUS screen will display the output.

Fast-Path Command(s)

appletalk echo *dest_network_id dest_node_id number_echos*

XNS Echo

To issue XNS echo requests to another node:

1. Select **Operations** from the System Manager main menu.
2. Select **Remote Host Echo (Ping)/Route Trace** from the next menu.
3. Select **XNS Echo** on the selector screen as shown in Figure 4-17 on page 4-18.
4. Enter the following information on the dialog screen:
   - XNS network address

     This must be four hexadecimal bytes.
   - XNS host address

     This must be six hexadecimal bytes.
   - Packet size (Any value from 1 to 100)

     This is the number of bytes sent with each echo request. The default is **64**.
   - Number of echoes (Any value from 1 to 1000)

     The number of echo requests sent to the destination. The default is **3**.
5. Press **Enter** to activate your request.

6. A COMMAND STATUS screen will display the output.

Fast-Path Command(s)

xns echo *dest_net_num dest_host_addr packet_size num_echoes*

VINES ICP Echo

To issue VINES ICP echo requests to another node:

1. Select **Operations** from the System Manager main menu.
2. Select **Remote Host Echo (Ping)/Route Trace** from the next menu.
3. Select **VINES ICP Echo** on the selector screen as shown in Figure 4-17 on page 4-18.
4. Enter the following information on the dialog screen:
   - VINES network number

     The destination node for the echo request. This must be 4 hexadecimal bytes.
   - Packet size (Any value from 1 to 100)

     This is the number of bytes sent with each echo request. The default is **64**.
   - Number of echoes (Any value from 1 to 1000)

     The number of echo requests sent to the destination. The default is **3**.
5. Press **Enter** to activate your request.
6. A COMMAND STATUS screen will display the output.

Fast-Path Command(s)

vines echo *dest_net_num packet_size num_echoes*

IP Route Trace

To issue an IP route trace:

1. Select **Operations** from the System Manager main menu.
2. Select **Remote Host Echo (Ping)/Route Trace** from the next menu.
3. Select **IP Route Trace** on the selector screen as shown in Figure 4-17 on page 4-18.
4. Enter the following information on the dialog screen:
   - Destination host name or IP address
   - Source host name or IP address
   - Packet size (Any value from 1 to 2048)

     This is the number of bytes sent with each echo request. The default is **40**.
   - Number of queries (Any value from 1 to 1000)

     The default is **3**.
   - Maximum number of hops (Any value from 1 to 255)

The default is **30**.

5. Press **Enter** to activate your request.
6. A COMMAND STATUS screen will display the output.

Fast-Path Command(s)

ip routes trace *dest_host_name packet_size num_queries maximum_hops source_host_name*

Network Statistics

The system network connection statistics list the:

- Maximum transmission unit (MTU)
- Inbound packets and errors
- Outbound packets and errors

Figure 4-18 shows the Network Statistics menu, which is accessed by the Operations menu.

```
IBM 6611                                                          hostname
                          Network Statistics

Move cursor to desired item and press Enter.

  Connection
  Interface Status
  Interface Utilization Monitor
  Packet Traffic
  Protocol
  Bridge









F1=Help            F2=Redraw Screen    F3=Return          F4=SysID
F10=Main Menu                          Esc+L=Turn Log On
```

Figure 4-18. Network Statistics Menu

Connection

To view connection statistics using the System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **Network Statistics** on the next menu.
3. Select **Connection** on the next menu.

4. A COMMAND STATUS screen will display the output. An example of the output is in Figure 4-19 on page 4-23.

   If you receive an asterisk (*) beside any of the listed interface names, this is an indication that the adapter or port is not enabled.

Fast-Path Command(s)

system connections view

```
Name  Mtu   Network     Address      Ipkts Ierrs    Opkts  Oerrs Coll
lo0   1536  <Link>                   39457     0    39457      0     0
lo0   1536  127.0.0.1   127.0.0.1    39457     0    39457      0     0
to0   1500  <Link>                    2235     0     2233      0     0
to0   1500  none        none          2235     0     2233      0     0
to1   1500  <Link>                    2235     0     2233      0     0
to1   1500  none        none          2235     0     2233      0     0
tk0   1492  <Link>                   18005     0    19343      0     0
tk0   1492  1.1.1        1.1.1.1     18005     0    19343      0     0
tk0   1484  vn:30800001H 1H           18005     0    19343      0     0
```

Figure 4-19. Example of Connection Output

The output in Figure 4-19 contains these fields:

Name Interface name
Mtu Represents the maximum transmission unit.
Ipkts Represents input packets.
Ierrs Represents input errors.
Opkts Represents output packets.
Oerrs Represents output errors.
Coll Represents collisions.

Interface Status

Select **Interface Status** to view detailed information about a specified active interface in the 6611. Part of the output you will receive is protocol-specific.

1. Select **Operations** from the System Manager main menu.
2. Select **Network Statistics** on the next menu.
3. Select **Interface Status** on the next menu.
4. Select an interface name from the selector screen. Refer to Table 4-1 on page 4-7 for a description of the interface names used to identify the adapters.
5. You will see the output on a command status screen.

Fast-Path Command(s)

interface state view *interface*

An example of the generic output received is:

```
te0: flags=1c0063<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,DEEP>
```

where the hexadecimal flags are defined as:

```
PKTCHG          0x80000000 - Packet charges imposed
WAN             0x40000000 - WAN interface
NOECHO          0x02000000 - Receives echo packets
DEEP_ENABLE     0x00100000 - Deep adapter enabled
DEEP            0x00080000 - Adapter is deep (card-to-card)
MULTICAST       0x00040000 - For oncard IP Multicast code
DCD             0x00020000 - DCD is raised
DO_HW_LOOPBACK  0x00010000 - Force loopback through hardware
ALLCAST         0x00008000 - Global broadcast
SNAP            0x00002000 - Receive all ns packets
BRIDGE          0x00001000 - Receive all bridge packets
SIMPLEX         0x00000800 - Cannot hear own transmissions
OACTIVE         0x00000400 - Transmission is in progress
ALLMULTI        0x00000200 - Receive all multicast packets
PROMISC         0x00000100 - Receive all packets
NOARP           0x00000080 - No address resolution protocol
RUNNING         0x00000040 - Resources allocated
NOTRAILERS      0x00000020 - Do not use trailers
POINTOPOINT     0x00000010 - Point-to-point link
LOOPBACK        0x00000008 - Loopback network
DEBUG           0x00000004 - Turn on debugging
BROADCAST       0x00000002 - Broadcast address valid
UP              0x00000001 - Interface is up
```

A sample of IP-specific output is:

```
inet 145.1.1.3 netmask 0xffffff00 broadcast 145.1.1.255
```

The IP-specific output includes the IP address, network mask, and broadcast address.

A sample of VINES-specific output is:

```
vines 30800533H.1H --> 0.1H
```

The VINES-specific output includes the VINES network number.host number and the destination address, if configured.

A sample of DECnet-specific output is:

```
decnet 1.367 netmask 0xfc00 broadcast 63.1023
```

The DECnet-specific output includes DECnet network address, network mask, and broadcast address.

A sample of AppleTalk-specific output is:

```
at 666-666  666.6 zone: greenzone  hop weight: 1
at cnfg flags=5<ATUP,NBPFLT>
at oper flags=1<UP>
address filters:  1-299  7000-7999
additional zones:  bluezone

remote port:  4450-4499
zone:  brownzone
address filters:  6000-6999
```

On the first line, the AppleTalk-specific output includes the AppleTalk network number range, AppleTalk network ID, default zone name, and hop weight. The second line gives configuration flags defined as :

ATUP	AppleTalk is currently enabled for routing
ATDOWN	AppleTalk is currently disabled for routing
ADR	AppleTalk address needs to be sent to the adapter (FR ports)
CHKSUM	The port is configured to generate checksum in outgoing packets
CNSD	The port is configured as nonseed
DDACK	Waiting for AppleTalk daemon to acknowledge port restart
DLYNBP	NBP Broadcast optimization enabled
DSACK	Waiting for system daemon to acknowledge port restart
FRUP	Serial adapter has enabled frame relay port
NBPFLT	Security filter based on resource names enabled
TRT	Trusted port
ZNFLT	Security filter based on zone names enabled

The third line of the AppleTalk-specific output gives operation flags defined as:

DOWN	The port is currently in down state and is not routing
DAD	Duplicate address indication received
NAD	Probing for and acquiring AppleTalk address
NSD	Nonseed port
NZL	Nonseed port waiting for zone information from seed router
UP	The port is currently in up state and is routing

Additional AppleTalk information includes:

address filters	List of network range port filters
additional zones	List of any additional zone names
remote port	Network range for remote network configured as a selected network configured to control import of routing information.
zone	List of zones in selected network.
address filters	List of address filters in selected network.

Interface Utilization Monitor

Select **Interface Utilization Monitor** to determine the data rate of each of the active interfaces, and the percentage that each is being used.

To view interface utilization information:

1. Select **Operations** from the System Manager main menu.
2. Select **Network Statistics** from the next menu.
3. Select **Interface Utilization Monitor** from the next menu.
4. Select or type the line speed information on the dialog screen for X.25, if appropriate. (The dialog screen will only display if an X.25 adapter is present.)
5. A single-screen adapter interface monitor reports the current data rate of the interface in bits per second, and the percentage of the line capacity being used.

Figure 4-20 on page 4-26 shows an example of the output. Refer to Table 4-1 on page 4-7 for a description of the interface names.

```
Interface        Bits/Sec        Percent

   to0             2867            0.02
   to1              503            0.45
   tk0              998            1.66
   te0             4672            5.67
   xt0              255           34.45
```

Figure 4-20. Sample Interface Utilization Output

The screen is continually updated every 15 seconds until you choose to stop it. Press **Ctrl+C** to stop the screen updates and to end the command.

Packet Traffic

The main operating system keeps counters on various network parameters for the adapter interfaces. The statistics for packet counts are gathered here. They are displayed on the screen every few seconds, depending on the interval value.

To view packet traffic statistics using the System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **Network Statistics** on the next menu.
3. Select **Packet Traffic** on the next menu.
4. Select the location of the packet traffic you want to view.
   - Select **system** to view packet traffic from the system card perspective.
   - Select **interface** to view packet traffic from the peer-capable adapter perspective.
5. Select an interface name from the selector screen. Refer to Table 4-1 on page 4-7 for a description of the interface names.
6. Enter the number of seconds between displays on the dialog screen. The default is 2.
7. Press **Ctrl+C** to end this command.
8. Press **Enter** to return to System Manager.

Fast-Path Command(s)

system statistics view -traffic *interface number_seconds*
interface statistics view -traffic *interface number_seconds*

Figure 4-21 on page 4-27 shows an example of system packet traffic output.

```
   input    (te0)     output           input   (Total)    output
packets  errs  packets  errs  colls packets  errs  packets  errs  colls
    208     0      208     0     0     11428     0    11411     0     0
      0     0        0     0     0         0     0        0     0     0
      0     0        0     0     0         0     0        0     0     0
      0     0        0     0     0         0     0        0     0     0
```

Figure 4-21. Example of Packet Traffic Output

The output contains the fields:

Errs Represents errors.
Coll Represents collisions.

Protocol

The adapter protocol statistics list the protocol statistics kept on the specified adapter for the specified protocol.

To view protocol statistics using the System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **Network Statistics** on the next menu.
3. Select **Protocol** on the next menu.
4. Select the protocol for which you want to view protocol statistics from the next selector screen. The protocols supported are:
   - IP
   - IPX
   - XNS
   - DECnet
   - VINES
   - AppleTalk
5. For any of the protocols *except* DECnet or AppleTalk, select the location of the statistics you want to view.
   - Select **system** to view protocol statistics from the system card perspective.
   - Select **interface** to view protocol statistics from the peer-capable adapter perspective.

   If you selected **interface**, or if you selected DECnet or AppleTalk from Step 4, select the adapter interface name for the adapter containing the protocol statistics you want to view from the selector screen.
6. A COMMAND STATUS screen will display the output. An example of the protocol output for the Internet protocol is in Figure 4-22 on page 4-28. In the example, *icmp* is Internet Control Message Protocol. Refer to Table 4-1 on page 4-7 for a description of the interface names used to identify the adapters.

Fast-Path Command(s)

appletalk statistics view *interface*
decnet statistics view *interface*
ip statistics view -system
ip statistics view *interface*
ipx statistics view *interface*
ipx statistics view -system
vines statistics view *interface*
vines statistics view -system
xns statistics view *interface*
xns statistics view -system

```
ip:
        ocIpForwarding = 1
        ocIpDefaultTTL = 255
        ocIpInReceives = 0
        ocIpInHdrErrors = 0
        ocips_toosmall = 0
        ocips_badver = 0
        ocips_badhlen = 0
        ocips_badsum = 0
        ocips_badlen = 0
        ocips_tooshort = 0
        ocips_badttl = 0
        ocIpInAddrErrors = 0
        ocIpForwDatagrams = 0
        ocIpInUnknownProtos = 0
        ocIpInDiscards = 0
        ocIpInDelivers = 0
        ocIpOutRequests = 0
        ocIpOutDiscards = 0
        ocIpOutNoRoutes = 0
        ocIpReasmTimeout = 0
        ocIpReasmReqds = 0
        ocIpReasmOKs = 0
        ocIpReasmFails = 0
        ocIpFragOKs = 0
        ocIpFragFails = 0
        ocIpFragCreates = 0
        ocIpRoutingDiscards = 0
icmp:
        ocIcmpInMsgs = 0
        ocIcmpInErrors = 0
        ocicps_tooshort = 0
        ocicps_badlen = 0
        ocicps_checksum = 0
        ocIcmpOutMsgs = 0
        ocIcmpOutErrors = 0
        ocicps_squelched = 0
        Output histogram:
        Input histogram:
```

Figure 4-22. Example of Protocol Statistics Output

Bridge

Bridge statistics are gathered for:

- LAN bridge
- Source route bridge
- Transparent bridge
- Translational bridge

The bridge statistics display counters for various network parameters kept on the peer-capable adapters. These are useful for solving problems with the bridge protocol. They are displayed on the screen every few seconds, depending on the interval value.

To view bridge statistics using System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **Network Statistics** on the next menu.
3. Select **Bridge** on the next menu.
4. Select the type of bridging statistics you want to view. Your choices are:
   - LAN bridge system
   - LAN bridge interface
   - LAN bridge internal protocol frame
   - Source route bridge
   - Source route bridge spanning tree
   - Source route bridge spanning tree frame relay
   - Transparent bridge
   - Transparent bridge spanning tree
   - Transparent bridge spanning tree frame relay
   - Translational bridge spanning tree
   - Translational bridge spanning tree frame relay

   Figure 4-23 on page 4-30 shows the selector screen.

```
IBM 6611                                                        hostname
                                    Bridge

Move cursor to desired item and press Enter.

  LAN Bridge System Statistics
  LAN Bridge Interface Statistics
  LAN Bridge Internal Protocol Frame Statistics

  Source Route Bridge Statistics
  Source Route Bridge Spanning Tree Statistics
  Source Route Bridge Spanning Tree Frame Relay Statistics

  Transparent Bridge Statistics
  Transparent Bridge Spanning Tree Statistics
  Transparent Bridge Spanning Tree Frame Relay Statistics

  Translational Bridge Spanning Tree Statistics
  Translational Bridge Spanning Tree Frame Relay Statistics


F1=Help           F2=Redraw Screen     F3=Return          F4=SysID
F10=Main Menu                          Esc+L=Turn Log On
```

Figure 4-23. Bridge Statistics Menu

5. Select the interface name from the next selector screen. Refer to Table 4-1 on page 4-7 for a description of the interface name used to identify the adapters.
6. Enter the number of seconds between displays on the dialog screen. The default is 2.

   Press **F1 (Esc+1)** for help on the dialog screen title to view a description of the output for the particular type of bridge statistics.
7. Press **Ctrl+C** to end this command.

   If you choose an adapter interface that is not enabled for bridging, there is no output displayed with this command. However, you still need to press **Ctrl+C** to end the command.
8. Press **Enter** to return to System Manager.

Fast-Path Command(s)

For LAN bridge:
bridge lb view -statistics *interface number_seconds*
bridge lb view -internal_frames *interface number_seconds*

For source route bridge:
bridge srb view -statistics *interface number_seconds*
bridge srb view -statistics -spt *interface number_seconds*
bridge srb view -statistics -sptfr *port_index number_seconds*

For transparent bridge:
bridge tb view -statistics *interface number_seconds*
bridge tb view -statistics -spt *interface number_seconds*
bridge tb view -statistics -sptfr *port_index number_seconds*

For translational bridge:
bridge tlb view -statistics -spt *interface number_seconds*
bridge tlb view -statistics -sptfr *port_index number_seconds*

Figure 4-24 shows an example of bridge output for source route bridge statistics, as shown in these fields:

iSPEC	Specifically routed frames received
oSPEC	Specifically routed frames sent
iARB	All route broadcasts received
oARB	All route broadcasts sent
iSRB	Single route broadcasts and non-broadcasts received
oSRB	Single route broadcasts and non-broadcasts sent
MTU	Discarded frames due to oversize
Dups	Duplicated ring numbers in route indicator frame
Mismatch	Ring number mismatches

```
iSPEC  oSPEC   iARB   oARB   iSRB   oSRB    MTU   Dups Mismatch
    9     18      9      9      0      0      0      0        0
    1      2      2      2      0      0      0      0        0
    0      0      0      0      0      0      0      0        0
```

Figure 4-24. Example of Source Route Bridge Statistics Output

ARP Table Management

The Address Resolution Protocol (ARP) translates unique IP addresses into unique hardware addresses. Tables on the peer-capable adapters store the mapping of the hardware address to its host name or IP address. You can view the tables, and add or delete entries from the tables. Tables may be IP or AppleTalk ARP tables.

Figure 4-25 on page 4-32 displays the ARP Table Management menu.

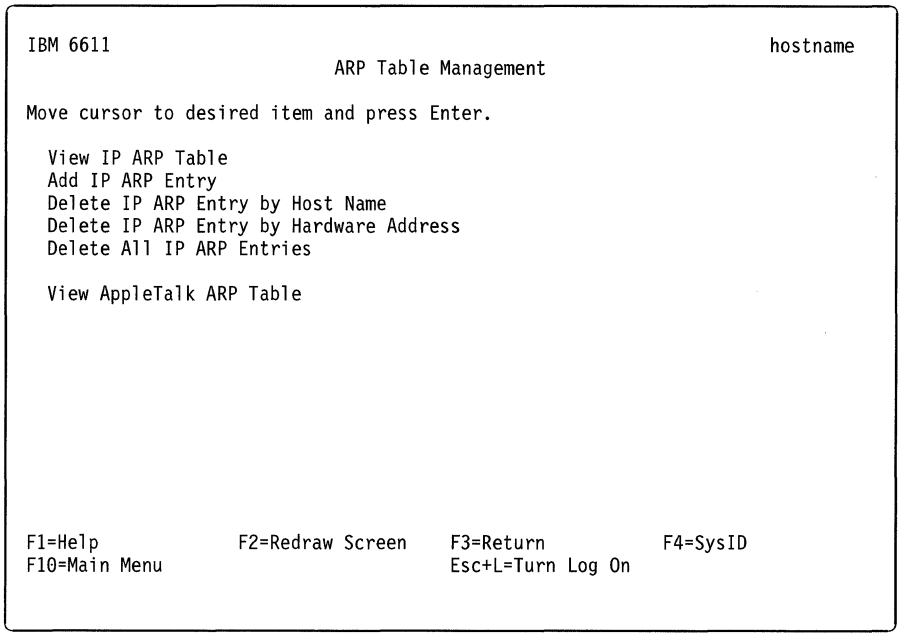


Figure 4-25. Address Resolution Protocol (ARP) Menu

View IP ARP Table

To view IP ARP entries using the System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **ARP Table Management** from the next menu.
3. Select **View IP ARP Table** from the next menu.
4. Select the adapter interface from the selector screen. Refer to Table 4-1 on page 4-7 for a description of the interface names used
5. A COMMAND STATUS screen will display a copy of all of the current entries in the IP ARP table.

The format for the table entries is as follows:

```
hostname (IP address) at HWaddress [HWtype]
```

An example of an ARP table is shown below:

```
666.8 at 10:0:5a:a8:a5:5 [802.3] permanent timer: 0
444.4 at 11:0:6a:a7:11:3 [802.3] permanent timer: 0
```

Fast-Path Command(s)

ip arp view *interface*

Add IP ARP Entry

To add an IP ARP entry using the System Manager:

1. Log in using a controlling user ID.
2. Select **Operations** from the System Manager main menu.
3. Select **ARP Table Management** from the next menu.
4. Select **Add IP ARP Entry** from the next menu.
5. Enter this information or select the appropriate values in the dialog screen and press **Enter**:

   Host name or IP Address
   Specify the remote host being added. If the host name is not known, you can use its IP address. The format for an IP address is *nnn.nnn.nnn.nnn* where *nnn* can be any decimal number from 1 to 255.

   Hardware address
   Specify the address of the adapter in use for the ARP entry action being performed. The format for a hardware address is *nn:nn:nn:nn:nn:nn* where *nn* can be any hexadecimal number from X'0' to X'FF'.

   Is this entry temporary or permanent?
   Select whether the system ARP table entry is permanent or temporary. Temporary entries are removed when the table fills up. Permanent entries are only removed if the system is restarted. The default is permanent.

   Do you want to publish this entry?
   Select whether this 6611 system should act as an ARP server and respond to requests for the host name being added, even though the host address does not exist on this particular 6611. This 6611 responds to translation requests for the host name, if the entry is published. The default is no.

6. A COMMAND STATUS screen will display a message specifying the added entry. For example:

   ```
   Entry lorax (17.17.17.3) was added to the system ARP table.
   ```

Fast-Path Command(s)

ip arp add -permanent -nopublish *host_name hw_address interface*
ip arp add -permanent -publish *host_name hw_address interface*
ip arp add -temporary -nopublish *host_name hw_address interface*
ip arp add -temporary -publish *host_name hw_address interface*

Delete IP ARP Entry by Host Name

To delete an IP ARP entry with a host name using the System Manager:

1. Log in using a controlling user ID.
2. Select **Operations** from the System Manager main menu.
3. Select **ARP Table Management** from the next menu.
4. Select **Delete IP ARP Entry by Host Name** from the next menu.

5. Select the adapter interface name from the selector screen. to identify the adapters.
6. Specify the remote host name of the entry to be deleted on the dialog screen and press **Enter**. You can use the IP address of the remote host, if the host name is not known. The format for an IP address is *nnn.nnn.nnn.nnn* where *nnn* can be any decimal number from 1 to 255.
7. You receive a COMMAND STATUS screen displaying a message regarding the delete entry. For example:

   ```
   jack (36.24.36.2) deleted
   ```

   The entry in the adapter interface ARP table is deleted for the specified host name or IP address.

Fast-Path Command(s)

ip arp delete -host_name *host_name interface*

Delete IP ARP Entry by Hardware Address

To delete an IP ARP entry with a hardware address using the System Manager:

1. Log in using a controlling user ID.
2. Select **Operations** from the System Manager main menu.
3. Select **ARP Table Management** from the next menu.
4. Select **Delete IP ARP Entry by Hardware Address** from the next menu.
5. Select the adapter interface name from the selector screen. Refer to Table 4-1 on page 4-7 for a description of the interface names used to identify the adapters.
6. Enter the hardware address of the entry to be deleted on the dialog screen and press **Enter**. The format for a hardware address is *nn:nn:nn:nn:nn:nn* where *nn* can be any hexadecimal number from X'0' to X'FF'.
7. A COMMAND STATUS screen will display a message regarding the delete entry. For example:

   ```
   10:0:5a:c8:0:5a (36.24.36.2) deleted
   ```

   The entry in the adapter interface ARP table is deleted for the specified hardware address.

Fast-Path Command(s)

ip arp delete -hwaddress *hw_address interface*

Delete All IP ARP Entries

This function clears out the IP ARP table for a specific network interface.

To clear an adapter ARP table using the System Manager:

1. Log in using a controlling user ID.
2. Select **Operations** from the System Manager main menu.

3. Select **ARP Table Management** from the next menu.
4. Select **Delete All IP ARP Entries** from the next menu.
5. Select the adapter interface name from the selector screen. Refer to Table 4-1 on page 4-7 for a description of the interface names used to identify the adapters.
6. A COMMAND STATUS screen will display a message stating that the ARP table for the specified adapter is cleared.

Fast-Path Command(s)

ip arp delete -all *interface*

View AppleTalk ARP Table

The AppleTalk ARP (AARP) translates AppleTalk addresses into hardware addresses. The AARP table only exists on the peer-capable adapter. To view this table and its entries using the System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **ARP Table Management** from the next menu.
3. Select **View AppleTalk ARP Table** from the next menu.
4. Select one or more interfaces names from the selector screen. Refer to Table 4-1 on page 4-7 for a description of the interface names used to identify the adapters.
5. Press **Enter** after making all selections.
6. A COMMAND STATUS screen will display a copy of all of the current entries in each of the interface's AARP table.

The format for the table entries is as follows:

```
network_number.nodeID at HWaddress [HWtype] Status EntryAge
```

- The HWtype includes [802.3] Ethernet, [802.5] token-ring, and [T1] serial interfaces.
- The AARP status indicators are in_use, permanent, need_AARP, did_AARP, and new_entry.
- The EntryAge is represented in seconds, where the low values represents recently used entries and high timer values represent old entries.

An example of an AARP table is shown below:

```
666.8 at 10:0:5a:a8:a5:5 [802.3] permanent timer: 0
444.4 at 11:0:6a:a7:11:3 [802.3] permanent timer: 0
```

Fast-Path Command(s)

appletalk arp view -interface *interface*

Port Filters

The filter information lists the configured filters for the specified protocol.

To view filter information using the System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **Port Filters** on the next menu.
3. Select the protocol for which you want to view filter information from the selector screen. The supported protocols are:
   - IP
   - IPX
   - XNS
   - VINES
   - DECnet
   - AppleTalk
   - Source route bridge
   - Transparent bridge
4. Select the interface name for which you want to view adapter interface statistical data from the selector screen. If you select **VINES**, you have the additional choice of selecting either VINES RouTing Update Protocol (RTP) filters or the VINES interface filters. Refer to Table 4-1 on page 4-7 for a description of the interface names used to identify the adapters.
5. A COMMAND STATUS screen will display the output. An example of the output for AppleTalk is in Figure 4-26.

   If you choose an adapter interface that is not enabled for the chosen protocol, no output is displayed with this command.

Fast-Path Command(s)

ip filters view *interface*
decnet filters view *interface*
ipx filters view *interface*
xns filters view *interface*
vines filters view *interface*
vines filters view -RTP
appletalk filters view *interface*
bridge srb view -filter *interface*
bridge tb view -filter *interface*

```
AppleTalk Network Number Filter Data:

                  Fltr                      Filtered_Packets
Flt  FilterRange  Type   Intf  Slot  Port InBound OutBound

  1     1 - 10    PERMIT to0      4     1       0        0
```

Figure 4-26. Example of Filter Output for AppleTalk

The field descriptions for the AppleTalk filter output are:

Flt Filter number

FilterRange Filter Range

Fltr Type Filter Type:

- Permit—Allow data to flow through the filter
- Deny—Do not allow data to flow through the filter

Intf Interface Name on which filter resides

Slot Slot number of interface

Port Port number of interface

Filtered_Packets InBound
Number of filtered packets, inbound

Filtered_Packets OutBound
Number of filtered packets, outbound

Network Management Information

The Simple Network Management Protocol (SNMP) network management data that is gathered for all the adapters and the base operating system can be viewed. The output you receive is based on the Management Information Base (MIB) variable that you select and the type of request.

To view network management information using the System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **Network Management Information (MIBs)** from the next menu.
3. Select a MIB module to be viewed from the list in the selector screen.

   A management information base (MIB) module is a collection of MIB variables relating to a common management area. The module defines each of the MIB variables, providing their syntax, numeric names, and textual names. The MIB module you select will be used to interpret the MIB variable name you provide. You provide the MIB variable name in the MIB variable being requested entry field on the next dialog screen.

   MIB modules are provided for standard MIBs as well as many vendor specific MIBs.

   Note: If you are querying an IBM 6611, select **IBM_6611 Complete MIB**. This is the default.

4. Enter or select values for the dialog items that follow:

Type of request.
The following requests are supported:

dump
Requests the value of the specified MIB variable and all of its objects. This request allows you to query MIB variables without knowledge of each instance present. By specifying the first object in the MIB (in the MIB variable being requested entry field), the dump request lets you query the entire MIB.

Dump is the default for type of request.

next
Requests the value of the MIB variable following the specified variable. Like the dump request, the next request makes it possible to query MIB variables without knowledge of the instance qualifiers.

get
Requests the value of the specified MIB variable. You must specify the exact instance (in the MIB variable being requested entry field) of the variable you are querying. For example, if you want to query the sysDescr variable in MIB-II, you must specify sysDescr.0. It is often easier to use a dump request for the entire table and then sort through the resulting data until you find the data for which you are looking.

Press **Tab** to select either **dump**, **next**, or **get**.

Community name to be used with query
This entry field specifies the community name to be used with the query. Each node supporting SNMP is configured with specific communities from which it will accept SNMP commands. A community is a pairing of a community name and an IP address. You must provide a community name that the node you are querying will accept from the address that is issuing the SNMP command. If this value is not specified, a community name of public is used.

Name of host to be queried
This entry field specifies the host name or the IP address of the host to be queried for MIB information. If this field is left blank, the MIB information is obtained from this IBM 6611. If you specify a host name, the host name must be mapped to an IP address in this IBM 6611 or be translated to one by a name server. You cannot specify an IP address that is associated with the local end of an Serial Adapter or a V.35/V.36 Serial Adapter. In order to obtain MIB information from a remote host, there must an IP route to that host. The IP address format is *nnn.nnn.nnn.nnn*, where *nnn* can be any decimal number from 1 to 255.

MIB variable being requested
There are two methods for specifying the MIB variable to be queried:

a. If you know the name of the desired MIB variable, type it in the entry field. If you have selected **get** as the type of request, you will use this method.

   The variable is specified in Variable.Instance format.

Variable:
Specifies the name in text format or numeric format of a specific MIB variable as defined in the specified MIB module. If the type of request is next or dump, the Variable parameter can be a MIB group.

Instance:
Specifies the instance qualifier for the MIB Variable parameter. The Instance parameter is required if the request is get. The Instance parameter is optional, if the request is next or dump.

b. Press **F4 (Esc+4)** to get a list of all the MIB variables available for the selected MIB module. A very long list is displayed. The list contains only variable groups without instance qualifiers. Press **Enter** to select the desired MIB variable.

Internet is the default for MIB variable being requested.

Figure 4-27 shows an example of network management information output.

```
ifNumber.0 = 6
ifIndex.1 = 1
ifIndex.2 = 2
ifIndex.3 = 3
ifIndex.4 = 4
ifIndex.5 = 5
ifIndex.6 = 6
ifDescr.1 = "lo0; Software Loopback"
ifDescr.2 = "te0; enty0; IBM 6611 Ethernet Network Interface"
ifDescr.3 = "te1; enty1; IBM 6611 Ethernet Network Interface"
ifDescr.4 = "tk0; trty0; IBM 6611 Token-Ring Network Interface"
ifDescr.5 = "te2; enty2; IBM 6611 Ethernet Network Interface"
ifDescr.6 = "to0; t1ty0; IBM 6611 Serial Network Interface"
ifType.1 = softwareLoopback(24)
ifType.2 = ethernet-csmacd(6)
ifType.3 = ethernet-csmacd(6)
ifType.4 = iso88025-tokenRing(9)
ifType.5 = ethernet-csmacd(6)
ifType.6 = t1-carrier(18)
ifMtu.1 = 1536
ifMtu.2 = 1500
ifMtu.3 = 1500
ifMtu.4 = 1500
ifMtu.5 = 1500
ifMtu.6 = 1500
```

Figure 4-27 (Part 1 of 2). Example of Network Management Information Output

```
ifSpeed.1 = 0
ifSpeed.2 = 10000000
ifSpeed.3 = 10000000
ifSpeed.4 = 4000000
ifSpeed.5 = 10000000
ifSpeed.6 = 0
ifPhysAddress.1 =
ifPhysAddress.2 = 08:00:5a:13:22:4d
ifPhysAddress.3 = 08:00:5a:13:20:29
ifPhysAddress.4 = 08:00:5a:13:00:6a
ifPhysAddress.5 = 08:00:5a:13:22:18
ifPhysAddress.6 =
```

Figure 4-27 (Part 2 of 2). Example of Network Management Information Output

For additional network management information, refer to the *IBM 6611 Network Processor Network Management Reference*.

File Systems

The File Systems function allows you to view the used and available space on the 6611 file systems. If the usage for the /tmp directory exceeds 75%, you should delete files from the transfer directory. Refer to "File Names for Output in Transfer Directory" on page 4-62 for more information about deleting files from the transfer directory.

To view the storage usage on the file systems:

1. Select **Operations** from the System Manager main menu.
2. Select **File Systems** from the next menu.
3. A COMMAND STATUS screen displays the output.

Fast-Path Command(s)

files system view

Figure 4-28 shows an example of the output.

```
Filesystem    Total KB     free %used    iused %iused Mounted on
/dev/hd4          8192     2272   72%      731    35% /
/dev/hd9var       4096     1716   58%      114    11% /var
/dev/hd2        405504   130384   67%    17521    17% /usr
/dev/hd3          8192     5840   28%       56     2% /tmp
/dev/hd1        106496    23776   77%      946     3% /home
```

Figure 4-28. Example of File Systems Output

The field descriptions for file systems output are:

Filesystem Name of the file system

Total KB Total number of kilobytes allocated to the file system

free Number of kilobytes currently available

%used Percentage of kilobytes currently used

iused Number of inodes used

%iused Percentage of inodes used

Mounted on Directory name where file system is mounted

File and Diskette Operations

The File and Diskette Operations menu (Figure 4-29) allows you to perform several tasks involving the manipulation of files.

```
IBM 6611                                                          hostname
                        File and Diskette Operations

Move cursor to desired item and press Enter.

  View Transfer Directory File
  Rename Transfer Directory File
  Delete Transfer Directory Files
  Send Transfer Directory File
  Receive Transfer Directory File
  Checksum Transfer Directory Files
  Compress/Uncompress Transfer Directory Files
  Scan Transfer Directory Files
  Clear Log Files

  View Static Directory File
  Send Static Directory File

  List Diskette Files
  Format Diskette


F1=Help             F2=Redraw Screen    F3=Return           F4=SysID
F10=Main Menu                           Esc+L=Turn Log On
```

Figure 4-29. File and Diskette Operations Menu

Transfer Directory Files

A file transferred into the 6611 is placed in the transfer directory. A file that needs to be transferred out of the 6611 must be in either the transfer directory or the static directory.

You can view, rename, delete, and transfer the files in the transfer directory. Only a controlling user can rename or delete files in the transfer directory. The static directory holds special files placed there by system components that allow the files to be viewed or transferred out of the 6611, but do not allow them to be deleted or renamed.

A few files in the transfer directory are trace logs that can grow. Most of these are not started by System Manager commands. Do not erase these files, unless you are instructed to do so by IBM service personnel.

There is a detailed discussion about the transfer directory files in "File Names for Output in Transfer Directory" on page 4-62. If you notice some files in the transfer

directory which are not listed in the tables in that section, contact IBM service personnel.

View Transfer Directory File

You may use System Manager to view files in the transfer directory. For example, you may want to view transfer directory files before performing a system back up so as to decide if you can delete them or not.

To view the files in the transfer directory using the System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **File and Diskette Operations** from the next menu screen.
3. Select **View Transfer Directory File** from the next menu to view the contents of a selected file in the transfer directory.
4. Select the file to view on the selector screen. At the top of the screen, the amount of space available in the transfer directory is displayed.
5. A COMMAND STATUS screen displays the contents of the file you selected to view. Refer to Figure 4-30 for an example of viewing a summary configuration report in the transfer directory.

```
    Command: OK           stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

[TOP]
Summary Configuration Report
IBM 6611 '6611host' on Mon Jul 13 14:09:57 1992

    IBM 6611 Host Name: 6611host
    IBM 6611 Domain name:
    System contact:
    System name:
    System location:

Slot 1 contains a 6611 X.25 Adapter

Slot 2 contains a 6611 Ethernet Adapter

[MORE...46]
```

Figure 4-30. Viewing a Report in the Transfer Directory

Fast-Path Command(s)

files transfer view *file_name*

Rename Transfer Directory File

To rename a file in the transfer directory using System Manager:

1. Log in using a controlling user ID.
2. Select **Operations** from the System Manager main menu.
3. Select **File and Diskette Operations** from the next menu.
4. Select **Rename Transfer Directory File** from the next menu.
5. Select the file to rename on the selector screen.
6. Enter the new name of the file on the next dialog screen.
7. A COMMAND STATUS screen displays the following message:

   ```
   File, old_file_name, in the transfer directory has been renamed to new_file_name.
   ```

Fast-Path Command(s)

files transfer rename *file_name new_file_name*

Delete Transfer Directory Files

You may use System Manager to delete files in the transfer directory. You may want to delete long, unnecessary files (such as dumps) before performing a system backup so as to save time.

To delete a file in the transfer directory using the System Manager:

1. Log in using a controlling user ID.
2. Select **Operations** from the System Manager main menu.
3. Select **File and Diskette Operations** from the next menu.
4. Select **Delete Transfer Directory Files** from the next menu.
5. Select the files to delete on the selector screen. Press **F9 (Esc+9)** to select the files to delete. Press **Enter** to register the selections.

   A COMMAND STATUS screen will display the following message:

   ```
   Files file_name deleted from the transfer directory
   ```

Fast-Path Command(s)

files transfer delete *file_name*
files transfer delete -all

If you need to transfer files to or from the transfer directory, refer to "Transferring Files" on page 4-62.

Send Transfer Directory File

To transfer a file out of the transfer directory using System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **File and Diskette Operations** from the next menu.
3. Select **Send Transfer Directory File** from the next menu.

4. Select the file destination on the selector screen as shown in Figure 4-31 on page 4-44.

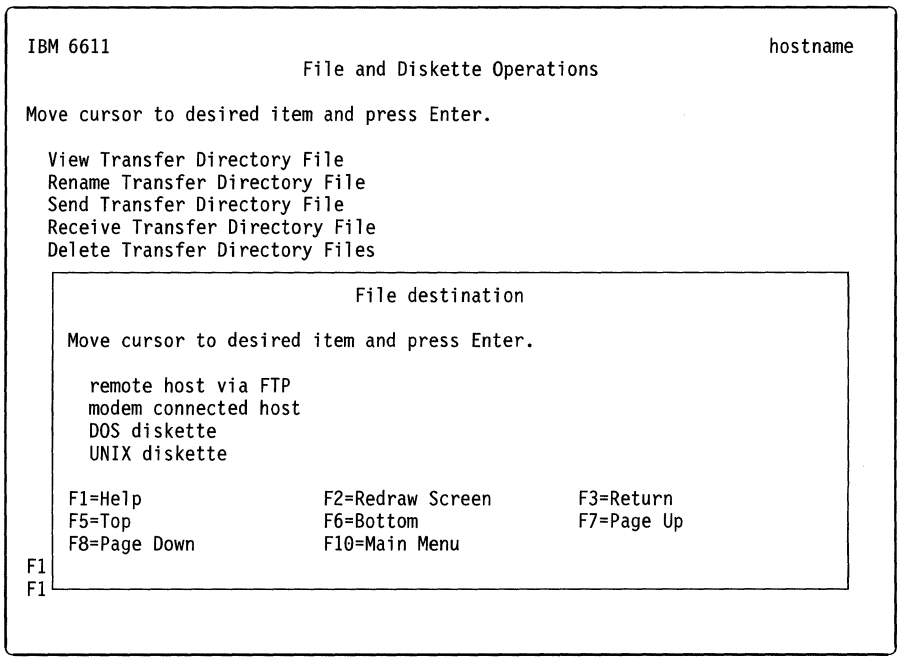


Figure 4-31. Send Transfer Directory File Selector Screen

If you select **remote host via FTP**, you must specify the host name or IP address of where to send the file on the dialog screen. You will then be entered into an interactive FTP dialog. Refer to "Using the File Transfer Protocol" on page 4-67 for information on using FTP and for an example of an interactive dialog. You will be prompted for a user ID and password configured at the remote node and for the name of the file to send.

Note: To do a send, you would specify **put "file_name"** in the interactive dialog.

Fast-Path Command(s)

files transfer send -ftp *host_name*

If you select **modem connected host**, you must specify the file to transfer. You may do this either on a dialog screen or on a pop-up list screen after pressing **F4 (Esc+4)** to bring up a list of files.

Fast-Path Command(s)

files transfer send -modem *file_name*

If you select **DOS diskette**, you must specify both the file to transfer (in the transfer directory) and the name of the file as it will be on the DOS diskette. You may choose the file to transfer on a pop-up list screen after pressing **F4 (Esc+4)** to bring up a list of files, or enter the file name on the dialog screen.

Fast-Path Command(s)

files transfer send -dos *file_name DOS_file_name*

If you select **UNIX diskette**, you must specify both the file to transfer (in the transfer directory) and whether the archive type will be create or append. You may choose the file to transfer on a pop-up list screen after pressing **F4 (Esc+4)** to bring up a list of files, or enter the file name on the dialog screen. Create places a file on a UNIX** diskette so that it overwrites existing files already on the diskette. Append adds a file to the existing files on the UNIX diskette.

Fast-Path Command(s)

files transfer send -unix -create *file_name*
files transfer send -unix -append *file_name*

5. A COMMAND STATUS screen will display the following message:

   `Files file_name sent from the transfer directory`

Receive Transfer Directory File

To receive a file into the transfer directory using System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **File and Diskette Operations** from the next menu.
3. Select **Receive Transfer Directory File** from the next menu.
4. Select the file source on the next selector screen.

   When you select **remote host via FTP**, you must specify the host name or IP address of where to receive the file on the dialog screen. You will then be entered into an interactive FTP dialog. Refer to "Using the File Transfer Protocol" on page 4-67 for information on using FTP and for an example of an interactive dialog. You will be prompted for a user ID and password configured at the remote node and for the name of the file to receive.

   Note: To do a receive, you would specify **get "file_name"** in the interactive dialog.

   Fast-Path Command(s)

   files transfer receive -ftp *host_name*

   When you select **modem connected host**, you must specify the file to be received. Type the file name on the entry field of the dialog screen.

   Fast-Path Command(s)

   files transfer receive -modem *file_name*

   When you select **DOS diskette**, you must specify both the file to receive (in the transfer directory) and the name of the file on the DOS diskette. Type the file names on the appropriate entry fields of the dialog screen.

   Fast-Path Command(s)

   files transfer receive -dos *file_name DOS_file_name*

   When you select **UNIX diskette**, you must specify the file or files to be received. Press **F9 (Esc+9)** to select the files. The default is all.

Fast-Path Command(s)

files transfer receive -unix *file_name*
files transfer receive -unix -all

5. A COMMAND STATUS screen displays the following message:

   ```
   Files file_name received from the transfer directory
   ```

Checksums

To perform checksums on transfer directory files:

1. Select **Operations** from the System Manager main menu.
2. Select **File and Diskette Operations** from the next menu.
3. Select √ from the next menu.
4. Select the files to checksum on the selector screen using **F9 (Esc+9)**. Press **Enter** to register the selections.

Fast-Path Command(s)

files transfer checksum {-log} *file_name*

Compress/Uncompress Transfer Directory Files

To compress or uncompress transfer directory files:

1. Log in using a controlling user ID.
2. Select **Operations** from the System Manager main menu.
3. Select **File and Diskette Operations** from the next menu.
4. Select **Compress/Uncompress Transfer Directory Files** from the next menu.
5. Select the files to compress or uncompress on the selector screen using **F9 (Esc+9)**. Press **Enter** to register the selections.

   Any file name with the suffix `.Z` is compressed. System Manager uncompresses the files you select and removes the suffixes.

   Otherwise, System Manager compresses the files you select and adds the `.Z` suffix to the file names.

Fast-Path Command(s)

files transfer compress *file_name*
files transfer uncompress *file_name*

Scan Transfer Directory Files

To scan transfer directory files for a specific pattern:

1. Select **Operations** from the System Manager main menu.
2. Select **File and Diskette Operations** from the next menu.
3. Select **Scan Transfer Directory Files** from the next menu.
4. Enter the **Pattern** on the dialog screen.

5. Select which files to scan on the dialog screen.
   a. Press **F4 (Esc+4)** to list the files.
   b. Press **F9 (Esc+9)** to select one or more files in the list.
   c. Press **Enter** to register your selections.
6. Press **Enter** to begin the scan.
7. A COMMAND STATUS screen will display the output.

Fast-Path Command(s)

files transfer scan *pattern file_names*
files transfer scan -all *pattern*

Clear Log File

This function lets you erase the contents of the System Manager and fast-path log files. These files are also pruned at login time if they are larger than 512 K bytes. Refer to "Using the System Manager Log" on page 2-14 for a detailed discussion about the System Manager log. Refer to "The Fast-Path Log" on page 9-4 for a detailed discussion of the fast-path log.

To clear a System Manager log file using System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **File and Diskette Operations** from the next menu.
3. Select **Clear Log File** from the next menu.
4. Select a file name on the selector screen.
5. Press **Enter** to make your selection.
6. A COMMAND STATUS screen will display a message when the log file is cleared.

Static Directory Files

A file that needs to be transferred out of the 6611 must be in either the transfer directory or the static directory. You can view, rename, delete and transfer the files in the transfer directory. The static directory holds special files placed there by system components that allow the files to be viewed or transferred out of the 6611, but do not allow them to be deleted or renamed.

View Static Directory File

To view files in the static directory:

1. Select **Operations** from the System Manager main menu.
2. Select **File and Diskette Operations** from the next menu.
3. Select **View Static Directory File** from the next menu. A selector screen appears listing all of the files in the static directory.
4. Select the file name that you want to view.
5. A COMMAND STATUS screen displays the contents of the file you selected to view. Refer to Figure 4-32 on page 4-48 for an example of viewing a file from the static directory.

```
Before command completion, additional instructions may appear below.

[TOP]

IBM 6611 NETWORK MANAGEMENT
_____________________


This file contains information regarding network management of the IBM
6611 Network Processor running the IBM Multiprotocol Network Program
Version 1.1.


DOCUMENTATION
_____________
[MORE...106]
```

Figure 4-32. Viewing a Static Directory File

Fast-Path Command(s)

files static view *file_name*

Send Static Directory File

To transfer a file out of the static directory using the System Manager:

1. Select **Operations** from the System Manager main menu.
2. Select **File and Diskette Operations** from the next menu.
3. Select **Send Static Directory File** from the next menu.
4. Select the file destination from the selector screen.

   When you select **remote host via FTP**, you must supply the host name or IP address. You will then enter into an interactive FTP dialog. Refer to "Using the File Transfer Protocol" on page 4-67 for information on using FTP and for an example of an interactive dialog. You will be prompted for a user ID and password configured at the remote node and for the name of the file to send.

   Note: To do a send, you would specify **put** *file_name* in the interactive dialog.

   Fast-Path Command(s)

   files static send -ftp *host_name*

   When you select **modem connected host**, you must state the file to transfer. You may do this either on the dialog screen or on the pop-up list screen after pressing **F4 (Esc+4)** for a list.

   Fast-Path Command(s)

   files static send -modem *file_name*

When you select **DOS diskette**, you must specify both the file to transfer (in the static directory) and the name of the file as it exists on the DOS diskette. You may choose the file to transfer on a pop-up list screen after pressing **F4 (Esc+4)** for a list of files, or on the dialog screen.

Fast-Path Command(s)

files static send -dos *file_name DOS_file_name*

When you select **UNIX diskette**, you must specify both the file to transfer (in the static directory) and whether the archive type is create or append. You may choose the file to transfer on a pop-up list screen after pressing **F4 (Esc+4)** for a list of files, or on the dialog screen. Create places a file on a UNIX diskette so that it overlays existing files already on the diskette. Append adds a file to the existing files on the UNIX diskette.

Fast-Path Command(s)

files static send -unix -create *file_name*
files static send -unix -append *file_name*

5. A COMMAND STATUS screen displays the file you selected to send.

If you need to transfer a file out of the static directory, refer to "Transferring Files" on page 4-62.

List DOS Diskette Files

To list the files on a diskette:

1. Place the diskette in the 6611 diskette drive.
2. Select **Operations** from the System Manager main menu.
3. Select **File and Diskette Operations** from the next menu.
4. Select **List DOS Diskette Files** from the next menu.
5. Select **DOS** or **UNIX** from the selector screen.
6. A COMMAND STATUS screen displays the files on the diskette. Figure 4-33 shows output for a DOS diskette.

```
SCM_CONF.RPT
CONFIG
PS.STA
VPD.LST
PD_ERROR.LOG
CONF.SH
TRBUG1.ERR
TRBUG7.ERR
SCM.RPT
IOSTAT.TXT
Free space: 680960 bytes
```

Figure 4-33. List of Files on DOS Diskette Example

Figure 4-34 on page 4-50 shows output for a UNIX diskette.

```
-rw-rw-rw-   0 0      734 Apr 23 18:06:20 1992 ps_io.stat
-rw-rw-rw-   0 0     1124 Apr 23 18:06:22 1992 ps_vm.stat
```

Figure 4-34. List of Files on UNIX Diskette Example

If the diskette is not in the 6611 diskette drive, you will see an error message on the COMMAND STATUS screen.

Fast-Path Command(s)

files diskette list -dos
files diskette list -unix

Format Diskette

To format a diskette:

1. Place the diskette in the 6611 diskette drive.
2. Select **Operations** from the System Manager main menu.
3. Select **File and Diskette Operations** from the next menu.
4. Select **Format Diskette** from the next menu.
5. Select the type of diskette on the selector screen from these choices:

   DOS high
   DOS low
   UNIX high
   UNIX low

   High is 1.4M bytes; low is 720K bytes.
6. An information message screen displays requesting you to confirm your decision to format the diskette.
7. A COMMAND STATUS screen displays the following message when formatting a DOS diskette:

   ```
   Formatting ... Format Complete
      1457664 bytes total disk space
      1457664 bytes available on disk
   Format another (Y/N)?
   ```

   Answer either **Y** or **N**.

   A COMMAND STATUS screen displays the following message when formatting a UNIX diskette:

   ```
   Formatting UNIX Diskette
   Press Ctrl+C to stop
   Formatting: 2 side(s), 80 trl/side, 18 sect/trk
   Format completed
   Completed formatting UNIX diskette
   ```

Fast-Path Command(s)

diskette dos format -high
diskette dos format -low
diskette unix format -high
diskette unix format -low

Login Information

Through System Manager, you may obtain login information such as who is logged into the system, when they logged in, and how long they have been logged on. Figure 4-35 shows the Login Information selector screen.

```
IBM 6611                                                          hostname
                                   Operations

Move cursor to desired item and press Enter.

  Protocol and Interface Monitor
  Routing Information
  Remote Host Echo(Ping)/Route Trace
  Network Statistics
  Address Resolution Protocol (ARP)
  Port Filters
  Network Management Information (MIBs)
    ┌──────────────────────────────────────────────────────────────┐
    │                          Login information                   │
    │                                                              │
    │ Move cursor to desired item and press Enter.                 │
    │                                                              │
    │   current logged in users                                    │
    │   login history                                              │
    │                                                              │
    │ F1=Help              F2=Redraw Screen      F3=Return         │
    │ F5=Top               F6=Bottom             F7=Page Up        │
    │ F8=Page Down         F10=Main Menu                           │
F1  │                                                              │
F1  └──────────────────────────────────────────────────────────────┘
```

Figure 4-35. Login Information Selector Screen

Currently Logged In Users

To obtain a list of all users currently logged into System Manager:

1. Log in using a controlling user ID.
2. Select **Operations** from the System Manager main menu.
3. Select **Login Information** from the next menu.
4. Select **current logged in users** from the selector screen (refer to Figure 4-35).
5. A COMMAND STATUS screen will display the output. Figure 4-36 on page 4-52 shows an example of the output.

Fast-Path Command(s)

user id view -logged_in

```
User            Terminal   Login Time                  Host          Type
-------------------------------------------------------------------------
ibm6611c        pts/1      Mar 31 11:09          9.67.250.2   controlling
ibm6611v        pts/2      Mar 31 11:30          9.67.84.23   viewing
```

Figure 4-36. Example of Current Logged In Users Output

The output contains these fields:

User User ID
Terminal Line on which user is logged on
Login Time When the user logged on
Host Name of the host from which the user is telnetting
Type Whether the user is a controlling or viewing user

Login History

To obtain the login history of one or more users:

1. Log in using a controlling user ID.
2. Select **Operations** from the System Manager main menu.
3. Select **Login Information** from the next menu.
4. Select **login history** from the selector screen (refer to Figure 4-35 on page 4-51).
5. Enter the following information on the dialog screen:
   - Number of lines to display
   - User ID to display
   - Terminal to display

   If you leave the entry fields blank, System Manager assumes a default of **all**.
6. A COMMAND STATUS screen will display the output. Figure 4-37 shows an example of the output.

Fast-Path Command(s)

user id view -history

```
User      Terminal        Host         Login Time       Duration
-------------------------------------------------------------------------
ibm6611c  ftp          relayer           Thu Mar 31 11:06   still logged in
ibm6611c  pts/1        1.1.1.2           Thu Mar 31 07:09 - 07:13  (00:03)
ibm6611c  pts/1        1.1.1.2           Thu Mar 31 06:13 - 07:04  (00:51)
ibm6611c  ftp          relayer           Wed Mar 30 11:25 - 14:43  (03:18)
ibm6611c  ftp          relayer           Tue Mar 29 15:38 - 10:30  (18:52)
ibm6611c  ftp          relayer           Tue Mar 29 15:10 - 15:38  (00:27)
ibm6611c  pts/2        1.1.1.2           Tue Mar 29 14:31 - 06:20  (15:49)
ibm6611c  ftp          relayer           Tue Mar 29 14:19 - 15:10  (00:51)
ibm6611c  pts/1        1.1.1.2           Tue Mar 29 14:07 - 14:16  (00:09)
```

Figure 4-37. Example of Login User History Output

The output contains these fields:

User	User ID of who is logging in
Terminal	Line on which user is logged on
Host	Name of the host from which the user is telnetting
Login time	When the user logged on
Duration	Logout time and duration of user session. The reason why the user was forced off the system is also shown.

System Activity Report

The system activity report gets the contents of selected cumulative activity counters in the operating system. The accounting system, based on the values in the Number and Interval parameters, writes information the specified number of times at the specified intervals in seconds. There are many system activity functions about which to report.

To view the system activity report using the System Manager:

1. Log in using a controlling user ID.
2. Select **Operations** from the System Manager main menu.
3. Select **System Activity Report** from the next menu.
4. On the dialog screen, specify the entry fields as follows:

   Interval length of each system activity sampling
   Type an interval length in seconds.

   The recommended value is between 1 and 5. The default is 2.

   Number of sampling intervals
   Type the number of intervals.

   The recommended value is between 1 and 5. The default is 4.

   Press **Tab** to select either **yes** or **no** on the dialog screen to turn on or off each of the following report options:

   - Report all activities listed below?
   - Use of file access system routines?
   - Buffer activity for transfers, accesses, and cache hit ratios?
   - System calls?
   - System activity?
   - Message and semaphore activities?
   - Average queue length while occupied, and percentage of time occupied?
   - Paging statistics?
   - CPU activity?
   - Status of text, process, i-node, and file tables?
   - System switching activity?
   - TTY device activity?

Fast-Path Command(s)

system statistics view -activity

Figure 4-38 on page 4-54 shows an example of System Activity Report output. For additional information on the output column headings, see online help for each option on the dialog screen. Press **F1 (Esc+1)** for help.

%usr Percent of CPU cycles consumed by the user

%sys Percent of CPU cycles consumed by system processes

%wio Percent of time spent waiting for I/O devices

%idle Percent of time not used

```
IBM 6611 mprII 2 3 000009133000    04/23/92

17:49:24
CPU Activity
            %usr    %sys    %wio   %idle
               6       9       1      83
17:49:27
CPU Activity
            %usr    %sys    %wio   %idle
               2      15       0      83

CPU Activity
            %usr    %sys    %wio   %idle
Average        4      12       1      83
```

Figure 4-38. Example of System Activity Report Output

EIA 232 Serial Ports

The EIA 232 serial ports connect the 6611 to a terminal either directly or over a modem. This menu option configures either the S1 or S2 port for use with a terminal.

Users who configure the S2 serial port to support network management of the Cylink** 4201 cannot use the S2 serial port for local or remote access to the 6611 as described in Chapter 3 on page 3-1. See the *IBM Multiprotocol Network Program Configuration Guide* qor information on configuring Cylink. For more information on accessing the 6611, refer to Chapter 3.

The 6611 supports modem configuration using the Attention (AT) command set, which allows the 6611 to control a modem operating in asynchronous mode. Refer to the manufacturer's documentation for the modem you are using for more information.

Figure 4-39 on page 4-55 shows the EIA 232 Serial Port function selector screen.

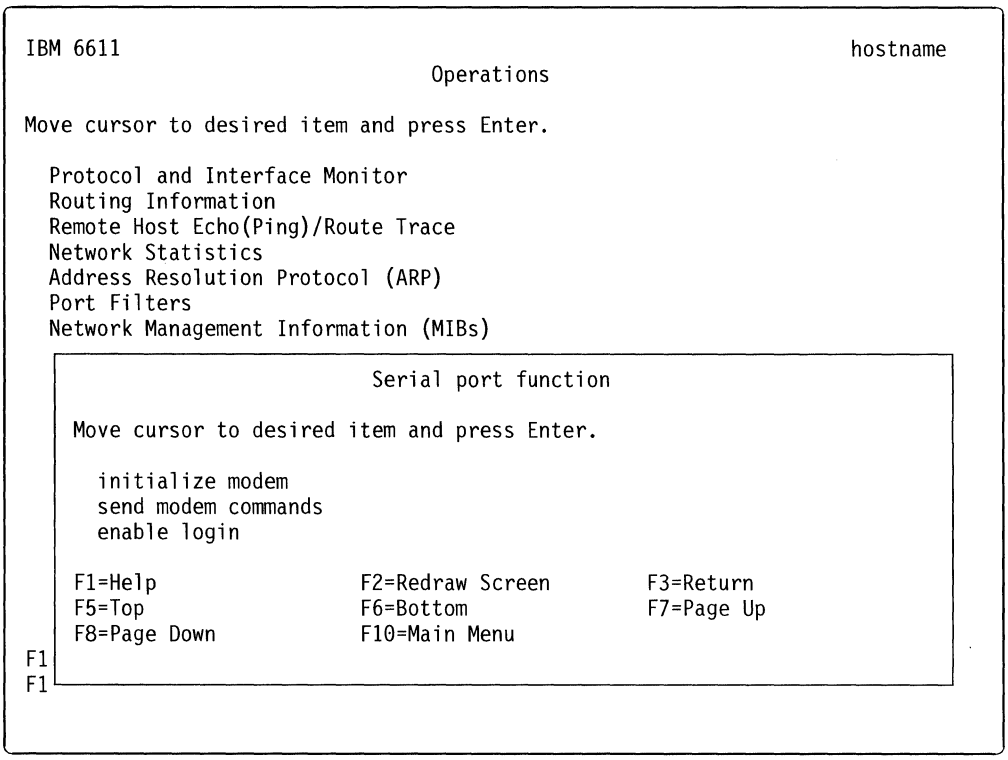


Figure 4-39. EIA 232 Serial Port Function Selector Screen

Initalize Modem

To send an AT command to initialize the modem configuration:

1. Log in using a controlling user ID.
2. Select **Operations** from the System Manager main menu.
3. Select **EIA 232 Serial Ports** from the next menu.
4. Select **initalize modem** on the selector screen.
5. Select the EIA 232 serial port on the selector screen. Refer to Figure 4-40 on page 4-56 for the serial port selector screen. Your choices are:
   - **S1**–For terminal or modem attachment.

     If you select S1, you must set the baud rate:

     2400 bps (normally set for modem-attached terminals)
     9600 bps (normally set for direct-attached terminals)
   - **S2**–For terminal or modem attachment *only* if S2 is not configured for network management Cylink.

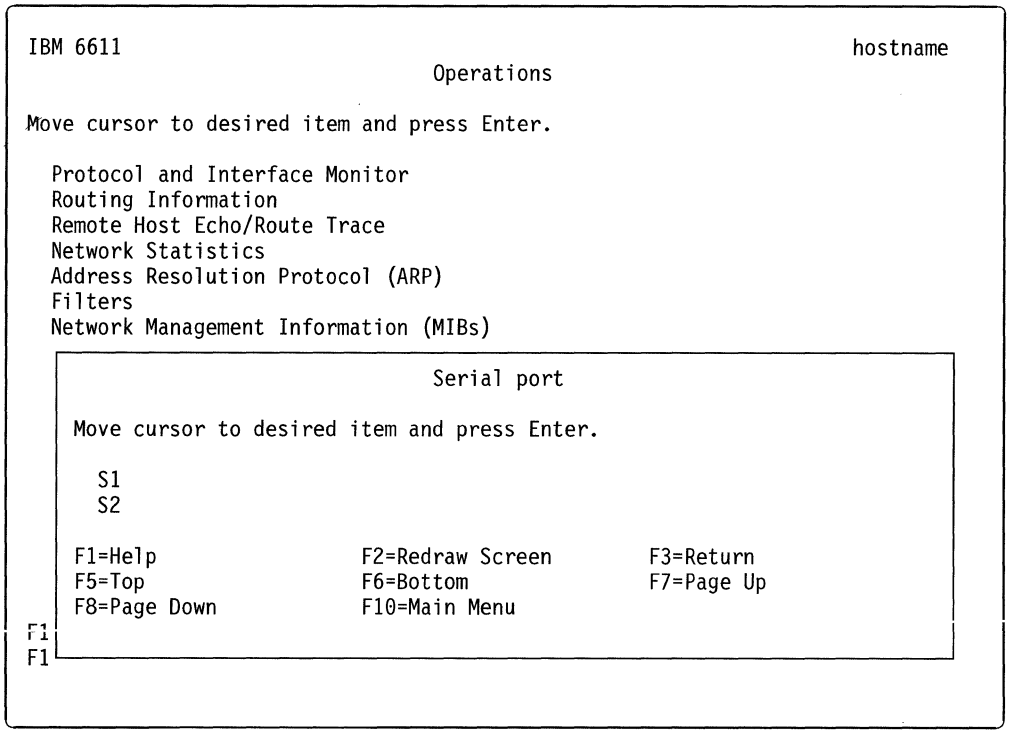


Figure 4-40. EIA 232 Serial Ports Selector Screen

6. Enter the AT initialization command on the dialog screen. The default AT command is **ATqv0&c1&d2sO=1**.
7. Press **Enter** to send the command.

   You will receive a message that the port is being initialized. This takes several seconds.

You will be asked if you want to send additional AT commands. To send additional AT commands:

1. Press **Y** (yes) and then press **Enter**.
2. Type in the next AT command to send.
3. Press **Enter** to send the command.
4. Repeat this procedure until you have sent all additional AT commands.

When you have finished sending AT commands, press **N** (no) and then press **Enter**.

Fast-Path Command(s)

serialport modem set -s1 *AT_command(s)*
serialport modem set -s2 *AT_command(s)*

To set the baud rate:

serialport baud set -s1 *baud_rate*
serialport baud set -s2 *baud_rate*

Send Modem Commands

To send an AT command to a modem:

1. Log in using a controlling user ID.
2. Select **Operations** from the System Manager main menu.
3. Select **EIA 232 Serial Ports** from the next menu.
4. Select **send modem commands** on the selector screen.
5. Select the EIA 232 serial port on the selector screen. Refer to Figure 4-40 on page 4-56 for the serial port selector screen. Your choices are:
   - **S1**–For terminal or modem attachment.

     If you select S1, you must set the baud rate:

     2400 bps (normally set for modem-attached terminals)
     9600 bps (normally set for direct-attached terminals)
   - **S2**–For terminal or modem attachment *only* if S2 is not configured for network management Cylink

   You will receive a message that the port is being initialized. This takes several seconds.
6. Press **Y** (yes) when asked if you want to send additional AT commands.
7. Press **Enter**.
8. Type in an AT command.
9. Press **Enter** to send the command.

   System Manager will continue to ask if you want to send additional AT commands until you press **N** (no).

Fast-Path Command(s)

serialport modem set -s1 *AT_command(s)*
serialport modem set -s2 *AT_command(s)*

To set the baud rate:

serialport baud set -s1 *baud_rate*
serialport baud set -s2 *baud_rate*

Enable Login

To enable the selected serial port for login:

1. Log in using a controlling user ID.
2. Select **Operations** from the System Manager main menu.
3. Select **EIA 232 Serial Ports** from the next menu.
4. Select **enable login** on the selector screen.
5. Select the EIA 232 serial port on the selector screen. Refer to Figure 4-40 on page 4-56 for the serial port selector screen. Your choices are:
   - **S1**–For terminal or modem attachment.

     If you select S1, you must set the baud rate:

2400 bps (normally set for modem-attached terminals)
9600 bps (normally set for direct-attached terminals)

- **S2**–For terminal or modem attachment *only* if S2 is not configured for network management Cylink.

6. A COMMAND STATUS screen will display any output.

Fast-Path Command(s)

serialport modem set -s1 *AT_command(s)*
serialport modem set -s2 *AT_command(s)*

To set the baud rate:

serialport baud set -s1 *baud_rate*
serialport baud set -s2 *baud_rate*

System Shutdown

There are times when it is necessary to stop the operation of the 6611. Do not stop operations by turning the power switch to **Off (O)**. There is a special process to shut down the 6611 that performs all necessary cleanup operations. The shutdown process stops all operations in the base operating system, including all routes needing to access the main system and all user sessions. This process does not stop the operation of the peer-capable adapters, just their communication with the main operating system. After the system has been stopped, you can power off the IBM 6611. Turning off the power is the only method of stopping the peer-capable adapters.

Note: Do not attempt to restart the system or turn off the 6611 before the shutdown completion message is displayed. Otherwise, file system damage can result.

Only a controlling user can shut down the 6611.

Before beginning the shutdown, you will receive a message including the number of minutes before the system is shut down. There is a series of messages displayed during the shutdown process. These messages vary slightly depending on whether you are connected over an EIA 232 serial port or a remote network connection, such as Telnet, and whether or not you asked to restart the system immediately after shutdown. You receive the following messages over a direct connection without the restart option specified.

```
SHUTDOWN PROGRAM
Sun Nov 14 18:07:50 1993


Broadcast message from ibm6611c on tty ...

PLEASE LOG OFF NOW !!!

System maintenance in progress.
All processes will be terminated in 3 minutes.

Broadcast message from ibm6611c on tty ...

THE SYSTEM IS BEING BROUGHT DOWN NOW

Wait for '...Halt complete ...' before stopping.
Process accounting has stopped.
Error reporting has stopped.
Stopping NFS/NIS Daemons
The Subsystem or Group, nfsd, is currently inoperative.
The Subsystem or Group, biod, is currently inoperative.
The Subsystem or Group, rpc.lockd, currently inoperative.
The Subsystem or Group, rpc.statd, currently inoperative.
The Subsystem or Group, rpc.mountd, currently inoperative.
The Subsystem or Group, yppasswdd, currently inoperative.
The Subsystem or Group, ypupdated, currently inoperative.
All processes currently running will now be terminated.
Halt complete ...
```

Figure 4-41. Example of System Shutdown Messages

The last two lines are not displayed if the system shutdown command is issued from a remote user over a Telnet session.

To stop the 6611 from the System Manager:

1. Log in using a controlling user ID.
2. Select **Operations** from the System Manager main menu.
3. Select **System Shutdown** from the next menu.
4. From the dialog screen, select **yes** or **no** to indicate whether or not you want to restart the system after the shutdown. Enter the elapsed time, in minutes, when the system should begin to shut down. The default is one minute.

Fast-Path Command(s)

system stop [(-restart)|-norestart] -minutes *number_minutes*
system stop [(-restart)|-norestart] -time *time*

5. You receive the following two messages warning you of the results of shutting down your 6611:

```
                    ARE YOU SURE?

Executing this command will shut down your IBM 6611,
stopping all the protocols and processess
including the current System Manager session.
Performing this function requires controlling
user privileges.  If you are a viewing user, you
will be logged out from this IBM 6611.

    Press Enter to shutdown the IBM 6611.
    Press F3 (Esc+3) to cancel and return to
        the System Manager.



F1=Help          F2=Redraw Screen    F3=Return
F10=Main Menu
```

```
                  INFORMATION MESSAGE


NOTE: This command needs to be run
      outside of the System Manager.
      Therefore the System Manager will exit
      immediately before running this command.

   Press Enter to proceed with the command.

   Press F3 (Esc+3) to cancel and return to
   the System Manager.

F1=Help          F2=Redraw Screen  F3=Return
F10=Main Menu
```

   To continue with the system shutdown, press **Enter**.

You can start the 6611 two ways:

- Using the power switch
- Using the Reset push button.

To start the 6611:

1. Set the key mode switch to **Normal**.
2. Start the 6611, by setting the power switch to **On (I)**.

   When you set the power switch to **On (I)**, the power-on light comes on and the 6611 starts a power-on self-test (POST). During the POST, numbers are displayed on the 3-digit display.
3. If the power-on light does not come on, check the power cord that is located at the back of the 6611 to ensure that it is plugged into a grounded electrical wall outlet. If this does not solve the problem, contact IBM service personnel.

To restart a 6611, when the 6611 is powered on:

1. Set the key mode switch to **Normal**.
2. Press the **Reset** push button causing the 6611 to reset and restart the system.

   Note: If the 6611 has a flashing **888** on the 3-digit display, pressing the Reset button displays additional codes or diagnostic messages. When this happens, turn the power switch to **Off (O)** for one minute, then turn it to **On (I)** again to start the 6611.

Note: Perform a controlled shutdown of System Manager before pressing the **Reset** push button or turning off the 6611. Doing either of these without first performing the shutdown could result in damage to the system files.

Date and Time

You can change or view the date and time from this menu item. When changing the date and time, the changes do not become effective for any user until they log out and log back into the 6611.

IBM recommends that you use this function to synchronize the time on any 6611s participating in:

- The automatic installation of software updates from a central point. Refer to "Automating Software Installation and Maintenance Facility Functions" on page 7-37 for details.
- The distribution of configurations across the network. Refer to the *Configuration Guide* for details.

To change the date and time:

1. Log in using a controlling user ID.
2. Select **Operations** from the System Manager main menu.
3. Select **Date and Time** from the next menu.
4. Select **yes** or **no** to answer the question "Do you want to change the time zone?" on the resulting screen.

   If you select **no**, go to step 7.
5. Answer the daylight savings time question from the selector screen. Select **yes** if the time zone goes on daylight savings time, or **no** if it does not.
6. Select the correct time zone from the next selector screen.
7. On the dialog screen, enter the new time and date. The accepted values are:

Year	00–99
Month	01–12
Day	01–31
Hour	00–23
Minutes	00–59
Seconds	00–59

8. A COMMAND STATUS screen appears with the new date and time and a message. For example:

```
Fri Apr 24 09:30:20 1992

Now exit System Manager and then re-enter so that any
changes to date, time, and time zone will be reflected in
your current session.
```

Fast-Path Command(s)

timeofday set *date-time*
where *date-time* is in the form "YYMMDDhhmm.ss"

After changing the time from the System Manager or the fast-path environment, log out and log back in again if you want the changed time to reflect your current session, and so you can view the changed time.

Transferring Files

You can transfer files to and from the 6611 using:

- FTP
- Xmodem Protocol
- Diskettes (DOS or UNIX)

A file transferred into the 6611 is placed in the transfer directory. A file that needs to be transferred out of the 6611 must be in either the transfer directory or the static directory.

You can view, rename, delete, and transfer the files in the transfer directory. Most of the files are in ASCII format. A few of the files are in binary format. None of the files are in EBCDIC. You can determine which files are binary because the files appear as a memory dump when they are browsed. The static directory holds files placed there by system components that allow the files to be viewed or transferred out of the 6611, but do not allow them to be deleted or renamed.

File Names for Output in Transfer Directory

There are various areas in the System Manager and in the fast-path environment where data is generated. The data is sent to the screen in most instances. Large outputs, such as dumps or traces, are sent to files in the transfer directory. In each of the cases where the output is directed to the transfer directory, the file name is set by the 6611. You can find these file names in the tables starting with Table 4-3 on page 4-63 through Table 4-6 on page 4-66. You can find other files not created or used by System Manager processes in Table 4-2.

There is also a System Manager log and a fast-path log for gathering data together in one file. Refer to "Using the System Manager Log" on page 2-14 for a detailed discussion about the System Manager log. Refer to "The Fast-Path Log" on page 9-4 for a detailed discussion about the fast-path log.

Table 4-2. Output File Names not Generated from System Manager

File name in transfer directory
pd_lcpd.log
console
mail

You should delete unneeded files that you create from the transfer directory in a timely manner to prevent the transfer directory from becoming full.

Trace Log Files

A few files in the transfer directory are trace logs. The size of these files can increase. Most of these are not started by System Manager commands. Do not erase these files, unless you are instructed to do so by IBM service personnel.

These trace log files all have a limit. When these files reach their size limit, a pruning process copies them into a file with the same name and an extension of mondisk.2 appended to the end. The pruning process zeros the original file and the trace continues to write into the file. The trace file with the mondisk.2 extension contains the earliest trace data. You can find the file names for these pruned files in Table 4-3.

Table 4-3. Trace Log Files That Are Automatically Pruned

File name in transfer directory	Upper limit (kilobytes)
console	10
mail	10
pd_appletalk.trc	100
pd_dnarouted.log	160
pd_lcpd.log	100
pd_pppsysmond.log	100
pd_sr-sptree	100
pd_sr-sptree.conf	500
pd_srtb-sptree	100
pd_srtb-sptree.conf	500
pd_swap.monproc.out	200
pd_sysmon.trc	500
pd_tb-sptree	100
pd_tb-sptree.conf	500
pd_vines.trc	100
pd_x25d.out	10

For example, the limit of the system monitor trace log is 500 Kb. The output of the trace is written into pd_sysmon.trc. When pd_sysmon.trc reaches 500 Kb, the pruning process copies the trace files into pd_sysmon.trc.mondisk.2 overlaying the existing data in that file. The pd_sysmon.trc file is zeroed and tracing continues.

Automatic Pruning Of The Transfer Directory

The pruning process monitors the file system of the transfer directory. When it becomes 97% full, it removes certain files from the transfer directory that have been targeted for removal. These targeted files include the System Manager log, all generated reports, statistics, vital product data, and dumps and most problem determination output. A wildcard character, the asterisk (*), is used to locate the files to remove. You can find the file names for these removed files in Table 4-4 on page 4-64.

Table 4-4. Output File Names for Removed Files

File name groupings
pd_r66d.log*
pd_rs960d.log*
pd_snmpd.log*
pd_t960logd.log*
pd_t1d.log*
pd_trapd.log*
pd_dlsd.*
pd_pppd.log*
pd_cfgd.log*
sysman.trace
config.report.*
vpd_*
pd_config*
pd_bsap*
pd_err*
pd_tra*
config.src*
.route
pd_dump*
core*
*.bak
*.regs
*.dram
*.sram
*.prom
*.read
*.report
*.errmsgs
*dump
*.linetrace
*.mondisk.2

If this removal does not reduce the file system of the transfer directory to below 97%, the pruning process removes all the files in the transfer directory that are over 2 days old, except for the special trace files. The pruning process continues to prune these trace files. If this additional removal does not reduce the file system of the transfer directory to below 97%, the pruning process removes all the files in the transfer directory regardless of how long they have existed, except for the special trace files that the pruning process continues to prune.

The pruning process does not remove any software installation packages that are in the transfer directory. These should be removed by the Software Installation and Maintenance Facility after the software is installed.

Most of the data generated in System Manager or in the fast-path environment is for problem solving and the contents of the files are analyzed only by IBM service personnel. This book does not explain the content of most of these files, except for the error report. Refer to "Contents of an Error Record" on page 5-24 for details about reading an error report.

Table 4-5 (Page 1 of 3). Output File Names Generated from Problem Determination Menu Items

Problem Determination Menu Item	Items on Next Menu	File Names in Transfer Directory
Error Logs and Reports	**Copy Error Log to Transfer Directory**	pd_error.log

Table 4-5 (Page 2 of 3). Output File Names Generated from Problem Determination Menu Items

Problem Determination Menu Item	Items on Next Menu	File Names in Transfer Directory
System Dump	**Start**	pd_system.dump
	Copy to Diskette or Transfer Directory	pd_system.dump
	Format	pd_system.fdump
Process and Protocol Dumps	**Start Nondisruptive**	pd_ip.dump.# ps_ipxd.tables pd_dls.dump pd_route_vines.dump pd_dump.APPN.d#
	Start Disruptive	pd_dump.*
System Trace	**Start**	trcfile
	Format	pd_trace.report
Process and Protocol Traces	**Start**	pd_appletalk.trc pd_appn.trc pd_bnbmast* pd_bnbrifh* pd_bnpmanp* pd_bnpxipf* pd_dnarouted.trc pd_dls.trc pd_ip.trc* pd_ipxd.RIP pd_ipxd.SAP pd_pppsysmond.log pd_sr-sptree pd_sr-sptree.conf pd_sysmon.trc* pd_tb-sptree pd_tb-sptree.conf pd_vines.trc pd_XNSrouted.RIP pd_x25d.out* trcfile (APPN, DLSw)

Table 4-5 (Page 3 of 3). Output File Names Generated from Problem Determination Menu Items

Problem Determination Menu Item	Items on Next Menu	File Names in Transfer Directory
Protocol Debug	**AppleTalk Debug Information**	pd_*hostname*.appletalk.debug
	APPN Debug Information	pd_*hostname*.appn.debug
	DECnet Debug Information	pd_*hostname*.decnet.debug
	DLSw Debug Information	pd_*hostname*.dls.debug
	IP Debug Information	pd_*hostname*.ip.debug
	IPX Debug Information	pd_*hostname*.ipx.debug
	LAN Bridge Debug Information	pd_*hostname*.lb.debug
	PPP Debug Information	pd_*hostname*.ppp.debug
	SNMP Debug Information	pd_*hostname*.snmp.debug
	Source Route Bridge Debug Information	pd_*hostname*.srb.debug
	Translational Bridge Debug Information	pd_*hostname*.tlb.debug
	Transparent Bridge Debug Information	pd_*hostname*.tb.debug
	VINES Debug Information	pd_*hostname*.vines.debug
	XNS Debug Information	pd_*hostname*.xns.debug
	X.25 Debug Information	pd_*hostname*.x25.debug

Note:

1. *nnnn* is the sequence number
2. This file name is assigned if you do not specify a different file name.

Table 4-6. Output File Names Generated from Configuration Menu Items

Configuration menu item	Items on next menu	File names in transfer directory
Configuration Reports		config.report.brief config.report.detail

Table 4-7. Output File Names Generated from Software Installation and Maintenance Facility Menu Items

Software Installation menu item	Items on next menu	File names in transfer directory
Apply Software Components		pd_prereq.chk.# pd_space.chk.#
Apply Software Updates		pd_prereq.chk.# pd_space.chk.#

Using the File Transfer Protocol

FTP allows file transfer between a 6611 and another IP node (for example, to another 6611). The 6611 can issue and receive FTP requests. To transfer files using FTP, specify some or all of the following information in response to prompts:

- Host name or IP address of the IP node that is sending or receiving the file
- User ID and password of a user at the remote IP node
- File name to be transferred
- Type of transfer (get or put)
- Type of file (binary or ASCII)

You can use only a limited number of FTP subcommands when you issue **ftp** *from* a remote IP host *to* the 6611. The commands are as follows:

get	Sends a file from the 6611 to the remote IP host.
mget	Sends multiple files from the 6611 to the remote IP host.
put	Copies a file from the remote IP host to the 6611.
mput	Copies multiple files from the remote IP host to the 6611.
cd /static	Changes the current directory to the static directory. To transfer files from the static directory, the current directory must be the static directory.
cd /transfer	Changes the current directory to the transfer directory. To transfer files to or from the transfer directory, the current directory must be the transfer directory.
ls	Lists the files in the current directory, either the transfer directory or the static directory.

If a file is to be transferred into a remote IP node that is *not* a 6611, the file is added (put) in the home directory for the specified user ID. If a file is to be retrieved from the remote IP node, it is retrieved (get) from the home directory of the remote IP node. If a file is to be transferred to a 6611, it is placed in the transfer directory. If a file is to be transferred from a 6611, it is taken from either the transfer directory or the static directory.

There are two versions of FTP used by the 6611:

Single line version All options specified first. This is used *only* in 6611 shell scripts. Only the get and put FTP subcommands are correct with the single line version.

Interactive version FTP initiated with only the host name; all other information is prompted.

With the interactive version, used with System Manager and in the fast-path environment, a typical scenario is:

- Select **Operations** from the System Manager main menu.
- Select **File and Diskette Operations** from the next menu.
- Select either **Send Transfer Directory File**, **Receive Transfer Directory File**, or **Send Static Directory File** from the next menu.
- Select **remote host via FTP** from the selector screen.
- Enter the **Host name** on the dialog screen.

You are then entered into an interactive dialog with FTP.

Output displayed:

```
Trying to connect to hostname
Once successfully connected, you may send a file
from the transfer directory by typing
       put <file_name>
at the ftp prompt

To quit an FTP session and return to System Manager
Type 'quit' at the ftp prompt

 Press Any Key to Continue ..
```

Type in: Press any key

Output displayed:

```
Connected to hostname.
 220 hostname ftp server (Version 4.1 Date) ready.
 Name (hostname: local_userid):
```

Type in:

Name (hostname: local_userid): remote_userid

Output displayed:

```
 331 Password required for remote_userid.
 Password:
```

Type in: (Enter the password. It will not be displayed.)

Output displayed:

```
230 User remote_userid logged in.
 ftp>
```

Type in:

```
ftp> put file_name
```

Output displayed:

```
200 PORT command successful.
150 Opening ASCII mode data connection for file_name.
226 Transfer complete.
13029 bytes sent in 0.07388 seconds (172.2 Kbytes/s)
ftp>
```

Type in:

```
ftp> quit
```

Output displayed:

```
221 Goodbye.
```

The numbers associated with the FTP messages are standard message numbers for this protocol. They have no significance other than to identify the message.

Fast-Path Command(s)

files transfer send -ftp *host_name*
files static send -ftp *host_name*
files transfer receive -ftp *host_name*

Using the Xmodem Protocol

The Xmodem Protocol is an 8-bit transfer protocol that can detect data transmission errors and then retransmit the data. The station that sends the data waits until the remote station sends a signal that it is ready to receive data. When the remote station gets the data, it returns an acknowledgment to the sender. Sending and receiving files with the Xmodem command are complementary operations. One system must be set to send while the other is set to receive. To interrupt the Xmodem file transfer, press **Ctrl+X**.

To transfer files between a 6611 and a local workstation via Xmodem:

1. Establish the connection between the local workstation and the 6611 with the attached modem. Refer to the documentation about the Xmodem Protocol in the manual supplied with the communications package for the exact syntax.
2. A login prompt appears. You are requested to type in a user ID and password.
3. If the file transfer is between a 6611 that is not equipped with the modem and the workstation from which the telephone connection was made, then an RLOGIN network connection is needed from the 6611 or other IP node equipped with the modem and the 6611 from which or to which the file is to be transferred. Refer to "Using Remote Login" on page 3-6 for details about establishing a remote login connection.

4. When the login has completed to the 6611 needing a file transfer, you are in the System Manager. There are several menu items pertaining to transferring files via modem access. Use the System Manager menus to find the menu item relating to the file transfer needed.
5. Select the file name you want to transfer. The 6611 issues the message:

```
Sending (Receiving) file file_name via Xmodem
You can return to local machine and begin file transmission.
```

6. Return to the local machine (the one that initiated the telephone call) using the key sequence defined by the communication program that supports the Xmodem Protocol.
7. Receive or send the file, and wait until the file transfer completes.
8. When the file has been transferred, return to the 6611 by reconnecting using the communication program.

Transferring Files between a RISC System/6000 and a 6611: To establish a remote login session between a RISC System/6000* workstation and the 6611 using a modem, use the Asynchronous Terminal Emulation (ATE) program located on the RISC System/6000 workstation. The ATE program allows you to establish a connection between the RISC System/6000 workstation and the 6611. The workstation acts as a terminal connected to the 6611. Using ATE, you can run commands on the 6611 and send and receive files using Xmodem.

The ATE program is menu driven and uses subcommands. The RISC System/6000 ATE program has a dialing directory feature that is a list of up to 20 frequently dialed phone numbers. The dialing directory contains the telephone number and other connection information such as baud rate, parity, and the name of the host at the other end of the connection. The **directory** subcommand allows you to display the telephone numbers and select the one you need to connect to the system you are calling, instead of entering the phone number with the connect subcommand. The **send** subcommand is used to send files from the RISC System/6000 workstation to the 6611. The **receive** subcommand is used to receive files from the 6611 to the RISC System/6000 workstation. The subcommands are entered from the appropriate menu by typing in the first letter of the subcommand followed by the command parameters.

Use the following scenarios to connect to the 6611, and send or receive files from the RISC System/6000 workstation. To send a file from 6611 to RISC System/6000 workstation:

1. To start the ATE program, type **ate** on the command line of the RISC System/6000 workstation.
2. The ATE Unconnected Main Menu is displayed. Using the ATE menus, set the following values:

Terminal type	VT100**
Line speed	2400 bps
Transfer Protocol	Xmodem

3. From this menu, specify either the **connect** or **directory** subcommand to connect to the 6611.
   - For the connect subcommand, type **c** *telephone_number.*
   - For the directory subcommand, type **d**.

A list of remote station names and phone numbers appears. Select the one corresponding to the 6611 which needs a file transfer.

4. The remote connection is made. Enter this login information when prompted:
   - User ID
   - Password
   - Terminal type
5. You are automatically placed in the System Manager. Find the menu item you want to use to transfer the file to the RISC System/6000 workstation or go to the fast-path environment and enter the following command primitive to send a file from either the transfer or static directory.

   Fast-Path Command(s)

   files transfer send -modem *file_name*
   files static send -modem *file_name*

6. Press **Ctrl+V** (main menu key) at the RISC System/6000 workstation to return to ATE. The ATE Connected Main Menu is displayed.
7. Type the receive subcommand as follows: **r** *file_name*. The **receive** subcommand instructs the workstation to receive the file from the remote 6611.
8. After transferring the file, the ATE program displays the Connected Main Menu.

To receive a file at the 6611 from the RISC System/6000 workstation:

1. To start the ATE program, type **ate** on the command line of the RISC System/6000 workstation.
2. From this menu, specify either the **connect** or **directory** subcommand to connect to the 6611.
   - For the connect subcommand, type **c** *telephone_number*.
   - For the directory subcommand, type **d**.

   A list of remote station names and phone numbers appears. Select the one corresponding to the 6611 needing a file transfer.
3. The remote connection is made. Enter this login information when prompted:
   - User ID
   - Password
   - Terminal type
4. You are automatically placed in the System Manager. Find the menu item you want to use to transfer the file from the RISC System/6000 workstation or go to the fast-path environment and enter the following command primitive to receive a file from the current directory of the RISC System/6000 into the transfer directory of the 6611.

   Fast-Path Command(s)

   files transfer receive -modem *file_name*

5. Press **Ctrl+V** (main menu key) at the RISC System/6000 workstation to return to ATE on the workstation. The ATE Connected Main Menu is displayed.
6. To issue the **send** subcommand, type: **s** *file_name*. The send subcommand instructs the workstation to send the file to the remote 6611.

7. After transferring the file, the ATE program displays the Connected Main Menu.

Transferring Files to Diskette

In many cases, it is not possible to transfer files remotely. Specifically, large files, such as a system dump or a trace report, cannot be transferred remotely. The needed information can be provided to IBM service personnel on a diskette.

The System Manager supports transferring the data on a diskette in either DOS or UNIX format. However, a file transferred to a DOS diskette must be small enough to fit on a single diskette. There is a System Manager menu sequence for transferring the system dump to diskettes. Refer to "Copy to Diskette or Transfer Directory" on page 5-34 for details.

Chapter 5. Problem Determination

About This Chapter

This chapter provides information about how to use the Problem Determination facilities provided by the System Manager and information about how to run system diagnostics.

The performance data generated is designed to be used for problem determination by IBM service personnel. If IBM service personnel are not given remote access to this 6611 for problem determination, you may be asked to retrieve some of this performance data. This book does not explain or interpret the details of the operations data.

Figure 5-1 shows the Problem Determination menu screen, which you reach by selecting **Problem Determination** on the System Manager main menu.

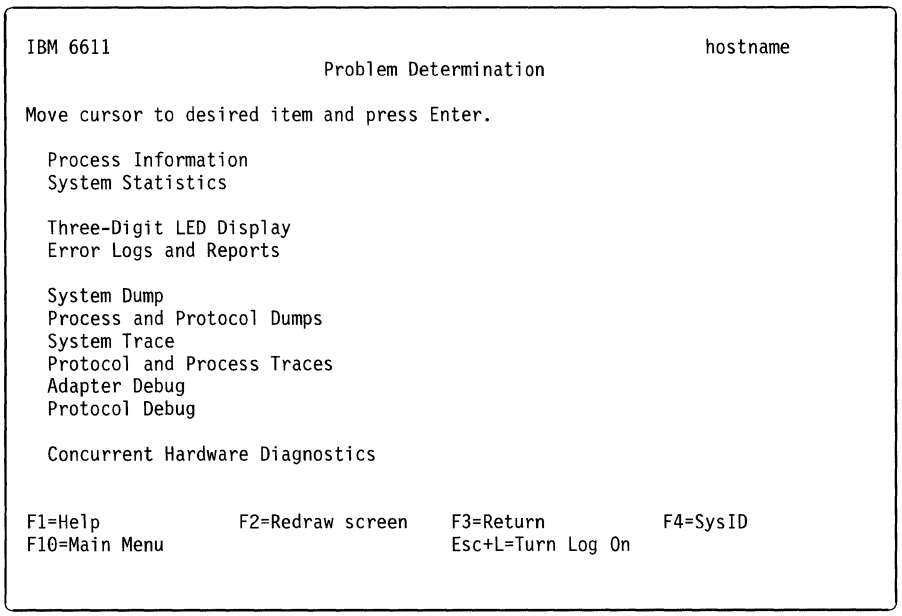


Figure 5-1. Problem Determination Menu

Refer to the following for information about the individual menu items:

Process Information

The user processes that are running in the 6611 have various pieces of statistical information that you can view. This information can be useful for debugging problems with the user processes or with the performance of the operating system. The Process Information menu provides five different options for how you can view the process information to get the full range of statistics.

Figure 5-2 shows the Process Information menu screen.

```
IBM 6611                                                          hostname
                              Process Information

Move cursor to desired item and press Enter.

  Processes
  Process Commands
  Process Information
  Process Status and Resource Utilitzation
  Processes by Protocol

  Process Table Information









F1=Help             F2=Redraw screen    F3=Return           F4=SysID
F10=Main Menu                           Esc+L=Turn Log On
```

Figure 5-2. Process Information Menu

Processes

To use the System Manager to list the running processes:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Process Information** from the next menu.
3. Select **Processes** on the next menu.
4. A COMMAND STATUS screen displays the output, as shown in Figure 5-3 on page 5-5. The output is sorted alphabetically by process name.

The field descriptions for the processes output (see Figure 5-3 on page 5-5) are:

PID The process ID of the process.

USER The user name of the process owner.

COMMAND The command name used to represent the process.

Fast-Path Command(s)

process list

```
  PID     USER COMMAND
 7692     root DNArouted
 7182     root XNSrouted
11379     root analyst
 5905     root atd
 5720     root cfgerr
 4429     root cron
 6676     root dlsinit
 3104     root errdemon
 9750     root gated
 6928     root gatedcfgd
 4939     root inetd
    1     root init
 8973     root ipxd
12667     root lanread
12152     root lanwrite
 5205     root mondisk
 1289     root monintr
 9224     root monproc
10873     root nb_timer
 7947     root protocfgd
14881     root ps
 5467     root rt66cfgd
 6236     root scram
 4153     root scsid
 8202     root smux.cfgd
11041     root smux.r66d
10272     root snmpd
 8467     root sptree
 1594     root srcmstr
    0     root swapper
 1822     root syncd
 3909     root syslogd
13807     root sysman
 6493     root t960logd
12509     root telnetd
 2638     root uprintfd
 7439     root vinesd
11636     root wandaemon
 9493     root x25d
```

Figure 5-3. Example of Processes Output

Process Commands

To use the System Manager to list the full process command names and parameters for all running user processes:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Process Information** on the next menu.
3. Select **Process Commands** on the next menu.
4. A COMMAND STATUS screen displays the output, as shown in Figure 5-4. The output is sorted in ascending order by process ID (PID).

The field descriptions for the process commands output (see Figure 5-4) are:

PID The process ID of the process.

COMMAND The full command name and parameters used to start the process.

Fast-Path Command(s)

process list -commands

```
  PID COMMAND
    0 swapper
    1 /etc/init
  514 kproc
 1289 /etc/monintr
 1594 /etc/srcmstr
 1822 /etc/syncd 60
 2638 /etc/uprintfd
 2875 /etc/sysmon
 3104 /usr/lib/errdemon
 3665 /etc/getty /dev/tty1
 3909 /etc/syslogd
 4153 /etc/scsid
 4429 /etc/cron
 4688 /etc/getty /dev/tty0
 4939 /etc/inetd
 5205 /etc/mondisk
 5467 /etc/rt66cfgd
 5720 /etc/cfgerr
 5905 /etc/atd
 6236 /etc/scram -s
 6493 /etc/t960logd
 6676 /usr/lpp/dls/dlsinit -c
 6928 /etc/gatedcfgd
```

Figure 5-4. Example of Process Commands Output

Process Information

To use the System Manager to view process information, including priority, size, and address of processes:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Process Information** on the next menu.
3. Select **Process Information** on the next menu.
4. A COMMAND STATUS screen displays the output, as shown in Figure 5-5 on page 5-8. The output is sorted alphabetically by process command name (CMD).

Fast-Path Command(s)

process list -detail

The field descriptions for the process information output (see Figure 5-5 on page 5-8 for an example) are:

F Flags, which are octal and additive and have the following meanings:

- **01** In core
- **02** System process
- **04** Locked in core
- **10** Waiting for a page default, or forking
- **20** Being traced by another process
- **40** Another tracing flag
- **100** Process has shared text

S State of the process:

- **0** Nonexistent
- **S** Sleeping
- **W** Waiting
- **R** Running
- **I** Intermediate
- **Z** Canceled
- **T** Stopped
- **K** Available system process
- **X** Growing

UID User ID of the process owner

PID Process ID of the process

PPID Process ID of the parent process

C Processor utilization for scheduling

PRI Priority of the process; higher numbers mean lower priority

NI Nice value; the priority of the process

ADDR Segment number of the process stack, if it is a normal process. The address of the preprocess data area, if it is a system process.

SZ Size (in 1024 byte units) of the core image of the process

WCHAN Event for which the process is waiting or sleeping; if blank, the process is running.

TTY Controlling workstation for the process:

- **-** Process is not associated with a workstation
- **?** Controlling workstation is unknown
- **Number** Serial port number minus 1; 0 for S1 and 1 for S2.

TIME Total execution time for the process

CMD Command name of the process

```
     F S UID   PID  PPID   C PRI NI ADDR    SZ    WCHAN    TTY  TIME CMD
260801 S   0  7692  2875   0  60 20  783   760             -  2:07 DNAroute
260801 S   0  7182  2875   0  60 20  f87   140             -  0:18 XNSroute
240801 S   0 11379  6676   0  58 18 37db    80  12cfd48    -  0:00 analyst
260801 S   0  5905  2875   0  60 20 1b8d   168             -  1:42 atd
260801 S   0  5720  2875   0  60 20 1128    52             -  0:00 cfgerr
240801 S   0  4429     1   0  60 20  f07   140  58220a4    -  0:08 cron
240801 S   0  6676  2875   0  60 20 2b95   100             -  0:00 dlsinit
 42801 S   0  3104     1   0  60 20  ec7   256     bc58    -  0:00 errdemon
262801 S   0  9750  2875   0  60 20 3198   600             -  0:34 gated
260801 S   0  6928  2875   0  60 20 178b    72             -  0:00 gatedcfg
260801 S   0  4939  1594   0  60 20 3eff   168             -  0:00 inetd
202803 S   0     1     0   4  62 20  804   144             -  0:39 init
260801 S   0  8973  2875   0  60 20  b85   164             -  0:26 ipxd
260801 S   0 12667 12152   0  60 20 21f0    76             -  0:05 lanread
240801 S   0 12152     1   0  60 20  de6    84  12cfe2c    -  0:00 lanwrite
240c01 S   0  5205  2875   1  60 20  723   152             -  0:35 mondisk
240c01 S   0  1289  2875   1  60 20 357a   104             -  0:07 monintr
240c01 S   0  9224  2875   0  60 20 2974   140             -  5:08 monproc
240801 S   0 10873 11379   0  58 18  7e3    72  58e6cd8    -  0:53 nb_timer
260801 S   0  7947  2875   0  60 20  180   692             -  0:01 protocfg
200001 R   0 14970 15202   9  64 20 3258    96         pts/1  0:00 ps
260801 S   0  5467  2875   0  60 20 152a   424             -  0:02 rt66cfgd
260801 S   0  6236  2875   2  61 20 2f37   300             -  3:45 scram
240801 S   0  4153     1   0  60 20 34da    48  54e2dd8    -  0:00 scsid
260801 S   0  8202  2875   0  60 20 3b7d   248             -  0:00 smux.cfg
260801 S   0 11041  2875   0  60 20 35ba   988             -  0:01 smux.r66
260801 S   0 10272  2875   0  60 20 3f7f   400             -  0:01 snmpd
260801 S   0  8467  2875   1  60 20 2592   304             -  4:10 sptree
260801 S   0  8722  2875   0  60 20 1f8f   288             -  2:32 sptree
260801 S   0  1594     1   0  60 20   e0   176             -  0:00 srcmstr
   b03 S   0     0     0 120  16 -- 1008     8             -  0:29 swapper
240801 S   0  1822     1   0  60 20 3abd    48  58e1698    -  0:06 syncd
260801 S   0  3909  1594   0  60 20 2cf6   124             -  0:00 syslogd
260801 S   0  2875     1   0  60 20  4e2  1364             -  0:18 sysmon
240801 S   0  6493  2875   0  60 20 393c    56   1f92e4    -  0:00 t960logd
260801 S   0  7439  2875   0  60 20 1389   132             -  0:05 vinesd
260801 S   0 11636  6676   0  60 20 3dde   100             -  0:00 wandaemo
240801 S   0  9493  2875   0  60 20 2d96    76   1f9354    -  0:00 x25d
```

Figure 5-5. Example of Process Information Output

Process Status and Resource Utilization

To use the System Manager to view process table information:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Process Information** on the next menu.
3. Select **Process Status and Resource Utilization** on the next menu.
4. A COMMAND STATUS screen displays the output, as shown in Figure 5-6 on page 5-10. The output is sorted in ascending order by process ID (PID).

Fast-Path Command(s)

process list -status

The field descriptions for the process status output (refer to Figure 5-6 on page 5-10 for an example) are:

PID Process ID of the process

TTY Controlling workstation for the process:

- **-** Process is not associated with a workstation
- **?** Controlling workstation is unknown
- **Number** Serial port number minus 1; 0 for S1 and 1 for S2

STAT State of the process:

- **0** Nonexistent
- **S** Sleeping
- **W** Waiting
- **R** Running
- **I** Intermediate
- **Z** Canceled
- **T** Stopped
- **K** Available system process
- **X** Growing

TIME Total execution time for the process

PGIN Number of disk I/Os resulting from references by the process to pages not loaded in core

SIZE Virtual size of the data section of the process (in 1kilobyte units)

RSS Real memory (resident set) size of the process (in 1kilobyte units)

LIM Soft limit on memory (in KB) the process can use before failing. If no limit has been specified, it is shown as xx. If the limit is set to the system limit, a value of UNLIM is displayed.

TSIZ Size of text (shared program) image

TRS Size of resident (real memory) set of text

%CPU Elapsed CPU utilization of the process since it was started. This is a cumulative value. Because the time base over which this is computed varies, it is possible for the sum of all %CPU fields to exceed 100%.

%MEM Percentage of real memory used by this process

COMMAND Full command name and its parameters. This field is truncated to 10 characters.

```
   PID    TTY STAT  TIME PGIN  SIZE   RSS    LIM  TSIZ   TRS %CPU %MEM COMMAND
     0      - S     0:29    6     8     8     xx     0     0  0.1  0.0 swapper
     1      - S     0:39   50   144   140     xx    21    24  0.1  1.0 /etc/init
   514      - R   862:00    0    12     8     xx     0     0  0.0  0.0 kp roc
   771      - S     1:40    0    16    16     xx     0     0  0.0  0.0 kproc
  1028      - S     0:00    3    16    16     xx     0     0  0.0  0.0 kproc
  1289      - S     0:07   32   104   120     xx    33    32  0.0  1.0 /etc/monintr
  1594      - S     0:00   12   176    12     xx    21     0  0.0  0.0 /etc/srcmstr
  1822      - S     0:06   15    48    28     xx     1     4  0.0  0.0 /etc/syncd 60
  2147      - S     0:00    0    16     8     xx     0     0  0.0  0.0 kproc
  2638      - S     0:00    2    36    12     xx     4     0  0.0  0.0 /etc/uprintfd
  2875      - S     0:18  255  1364   424     xx   130    84  0.0  2.0 /etc/sysmon
  3104      - S     0:00   64   256    76     xx    39    28  0.0  0.0 /usr/lib/errdemon
  3480      - S     0:00    0    16     8     xx     0     0  0.0  0.0 kproc
  3665      ? S     0:00   12   204    68     xx    38    56  0.0  0.0 /etc/getty /dev/tty1
  3909      - S     0:00   32   124    68  32768    16    24  0.0  0.0 /etc/syslogd
  4153      - S     0:00    4    48    28     xx     1     4  0.0  0.0 /etc/scsid
  4429      - S     0:08   52   140    88     xx    24    28  0.0  0.0 /etc/cron
  4688      ? S     0:00   13   208    68     xx    38    56  0.0  0.0 /etc/getty /dev/tty0
  4939      - S     0:00   52   168   172  32768    26    32  0.0  1.0 /etc/inetd
  5205      - S     0:35   30   152   140     xx    12    12  0.1  1.0 /etc/mondisk
  5467      - S     0:02  126   424   216     xx   206    80  0.0  1.0 /etc/rt66cfgd
  5720      - S     0:00    3    52    12     xx     6     0  0.0  0.0 /etc/cfgerr
  5905      - S     1:42   35   168   152     xx    86    52  0.2  1.0 /etc/atd
  6236      - S     3:45   55   300   140     xx   113    52  0.4  1.0 /etc/scram -s
  6493      - S     0:00    3    56    12     xx     7     0  0.0  0.0 /etc/t960logd
  6676      - S     0:00   30   100    12     xx    41     0  0.0  0.0 /usr/lpp/dls/dlsinit -c
  6928      - S     0:00   11    72    12     xx    33     0  0.0  0.0 /etc/gatedcfgd
  7182      - S     0:18   16   140    92     xx    33    32  0.0  0.0 /etc/XNSrouted -S
  7439      - S     0:05   51   132   104     xx    82    56  0.0  0.0 /etc/vinesd -S
  7692      - S     2:07  191   760   692     xx   251   112  0.2  3.0 /etc/DNArouted
  7947      - S     0:01   23   692    12     xx    83     0  0.0  0.0 /etc/protocfgd
  8202      - S     0:00   84   248    48     xx    79    16  0.0  0.0 /usr/sbin/smux.cfgd
  8467      - S     4:10   21   304   144     xx    84    44  0.5  1.0 /etc/sr-sptree
  8722      - S     2:32   19   288   128     xx    84    44  0.3  1.0 /etc/tb-sptree
  8973      - S     0:26   28   164   128     xx    62    52  0.0  1.0 /etc/ipxd -S
  9224      - S     5:08   38   140   116     xx    39    24  0.6  0.0 /etc/monproc
                                                                       -s/testbin/swap.monproc -r30
  9493      - S     0:00    5    76    12     xx     6     0  0.0  0.0 /etc/x25d -d
  9750      - S     0:34  226   600   556     xx   712   152  0.1  2.0 /etc/gated -N
```

Figure 5-6. Example of Process Status and Resource Utilization Output

Processes by Protocol

To use the System Manager to list the running protocols and their associated processes:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Process Information** on the next menu.
3. Select **Processes by Protocol** on the next menu.
4. A COMMAND STATUS screen displays the output, as shown in Figure 5-7.

Fast-Path Command(s)

process list -protocol

```
Protocol    Process_name   ID Parent %CPU    ELAPSED       TIME   VSZ
-------------------------------------------------------------------------
TCP/IP      inetd        1672   3191  0.0  1-05:10:00  00:00:00   188
            telnetd     13640   1672  0.0       09:24  00:00:00   196
            gated        7823   3960  0.1  1-03:44:32  00:00:59   608
AppleTalk   atd          9945   3960  0.2       59:18  00:00:06   184
DECnet      DNArouted    7277   1960  0.5  1-03:44:40  00:07:47   772
IPX         ipxd         9582   3960  0.0  1-03:44:40  00:00:46   176
VINES       vinesd       8560   3960  0.0  1-03:44:40  00:00:10   148
XNS         XNSrouted    8815   3960  0.0  1-03:44:40  00:00:34   156
System      init            1      0  0.1  1-05:11:24  00:01:22   252
            sysmon       3960      1  0.0  1-05:10:09  00:00:20  1412
            syncd        1797      1  0.0  1-05:10:23  00:00:17    64
            srcmstr      3191      1  0.0  1-05:10:09  00:00:00   192
            cron         5258      1  0.0  1-05:10:00  00:00:22   152
SNMP        snmpd       11388   3960  0.0  1-03:44:27  00:00:06   424
```

Figure 5-7. Example of Processes by Protocol Output

The field descriptions for the output are:

Protocol The protocol or software component to which this process belongs

Process_name The name of the process

ID The process identifier (PID)

Parent The process identifier of the parent process (PPID)

%CPU CPU utilization of the process

Because the time base over which this is computed varies it is possible for the sum of all %CPU fields to exceed 100%.

ELAPSED Elapsed time since the process started

TIME The cumulative CPU time for the process

VSZ Indicates the size, in kilobytes, of the process in virtual memory as a decimal integer.

Process Table Information

The process table maintains statistics on system variables, paging information, and file table information. Only a controlling user can invoke the function to view this information.

To use the System Manager to view process table information:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **Process Information** on the next menu.
4. Select **Process Table Information** on the next menu.

5. On the dialog screen, press **Tab** to select either **yes** or **no** to turn on or off each of the following process table options:
   - Display process table?
   - Display entries in the process table?
   - Display file table?
   - Display system variables?
   - Display i-node information?
   - Display paging information?

   The defaults are *yes* for all of the above.
6. A COMMAND STATUS screen displays the output. Figure 5-8 on page 5-14 shows an example of process table information output.

Fast-Path Command(s)

process table view

The field descriptions for the process table output are:

SLT Slot number in process table

ST Process state:
- s - sleeping
- r - running
- t - stopped
- i - idle
- z - zombie

PID Process ID

PPID Parent process ID

PGRP Parent group ID

UID User ID

EUID Effective user ID

PRI Process priority; the lower the number, the higher the priority

CPU CPU utilization; the amount of time in ticks used by the process

EVENT The location in storage of an event being waited for by a sleeping process

NAME The name of the process

```
SYSTEM VARS:

buffers    20
files      456
e_files    456
procs      131071
e_procs    48
clists     16384
maxproc    40
iostats    1
locks      200
e_locks    8522048

SLT ST    PID   PPID   PGRP   UID  EUID  PRI   CPU  EVENT  NAME
  0 s       0      0      0     0     0   16   120         swapper
 FLAGS: swapped_in no_swap fixed_pri kproc wake/sig
  1 s       1      0      0     0     0   60     1         init
 FLAGS: swapped_in no_swap wake/sig locks
  2 r     202      0      0     0     0  127   120         wait
 FLAGS: swapped_in no_swap fixed_pri kproc
  6 s     61c      1    61c     0     0   60     0         sysmon
 FLAGS: swapped_in wake/sig
 18 s    1229    61c    61c     0     0   60     0         mondisk
```

Figure 5-8. Example of Process Table Information Output

System Statistics

System network statistics are those network parameters that are gathered by the base operating system, as opposed to the peer-capable adapters. Some packets are forwarded by the adapters bypassing the base operating system. Select this option to view various system-related statistics.

Figure 5-9 on page 5-15 shows the System Statistics menu screen.

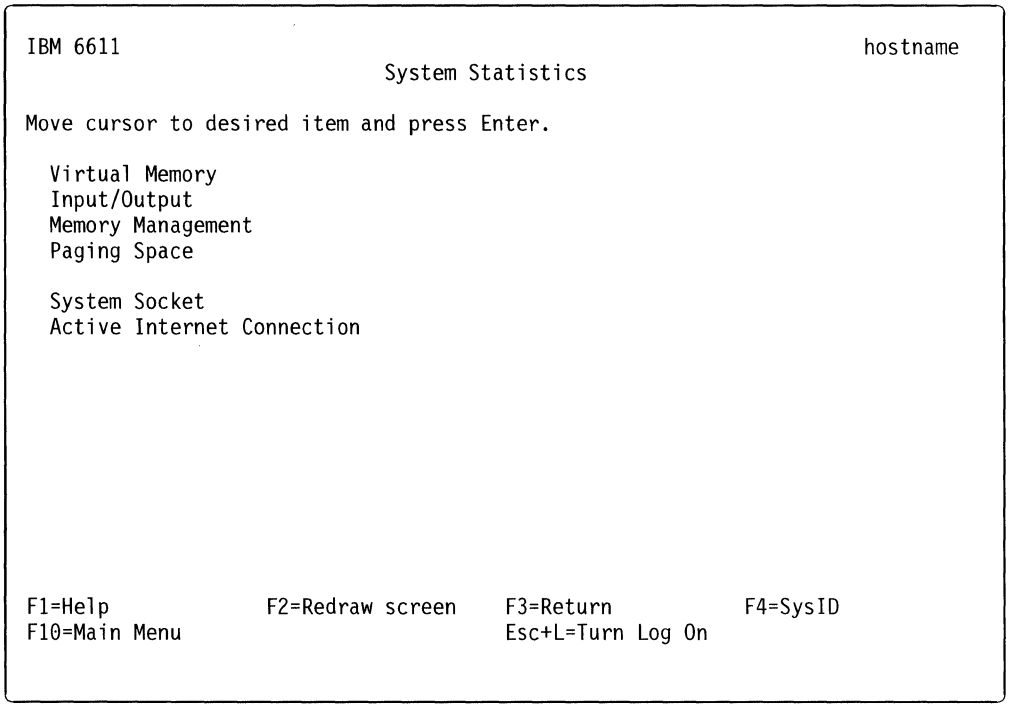


Figure 5-9. System Statistics Menu

Virtual Memory

This option provides statistics about processes, virtual memory, disks, and CPU activity.

To use the System Manager to view virtual memory statistics:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **System Statistics** on the next menu.
4. Select **Virtual Memory** on the next menu.
5. Enter values for **Seconds between samples** and **Number of samples** on the dialog screen.

   Seconds between samples Specifies the amount of time between reports. The first report contains statistics from the time the system started. Subsequent reports contain statistics collected from the end of the last interval that was reported.

   Number of samples Specifies the number of reports. If the Number of samples parameter is 1, the task generates a single report that contains a summary of the virtual memory activity since the system was started, then exits.
6. A COMMAND STATUS screen displays the statistical output, as shown in Figure 5-10 on page 5-16.

Fast-Path Command(s)

system statistics view -virtual_memory *number_seconds number_samples*

The field descriptions for the virtual memory output (see Figure 5-10 for an example) are:

procs Number of processes in various states:

- **r** In the run queue
- **b** In pager wait (awaiting resource, awaiting input/output)

memory Virtual and real memory usage:

- **avm** Active virtual pages
- **fre** Size of free list

page Page activity and page fault information:

- **re** Pager input/output list
- **pi** Pages paged in from paging space
- **po** Pages paged out to paging space
- **fr** Pages freed (page replacement)
- **sr** Pages scanned by page replacement algorithm
- **cy** Clock cycles by page replacement algorithm

faults Trap and interrupt rate averages per second over sampling interval:

- **in** Device interrupts
- **sy** Subroutines
- **cs** CPU context switch

cpu Breakdown of percentage usage of CPU time:

- **us** User time
- **sy** System time
- **id** CPU idle time
- **wa** CPU cycles to determine that the current process is in wait and there is pending input/output

```
procs    memory            page                  faults        cpu
----- ----------- ---------------------- ------------ -----------
 r  b   avm   fre  re  pi  po  fr   sr  cy  in   sy  cs us sy id wa
 0  0  5441    91   0   0   0   0    0   0 111   69  22  1  1 97  1
 0  0  5441    91   0   0   0   0    0   0 212  277 166  4  5 91  0
```

Figure 5-10. Example of Virtual Memory Output

Input/Output (I/O)

This task is performed to monitor system input and output device loading. It generates statistical reports for the terminal and disk devices.

The first report generated by this menu item provides statistics concerning the time since the system was started. Each subsequent report contains statistics collected since the previous report. All statistics are reported each time this task is invoked.

To use the System Manager to view I/O statistics:

1. Log in with a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **System Statistics** on the next menu.
4. Select **Input/Output** on the next menu.
5. Enter values for the **Seconds between samples** and **Number of samples** on the dialog screen.

   Seconds between samples Specifies the amount of time between reports. The first report contains statistics from the time the system started. Subsequent reports contain statistics collected from the end of the last interval that was reported.

   Number of samples Specifies the number of reports. If the Number of samples parameter is 1, the task generates a single report that contains a summary of the virtual memory activity since the system was started, then exits.
6. A COMMAND STATUS screen displays the I/O output, as shown in Figure 5-11 on page 5-18.

Fast-Path Command(s)

system statistics view -input_output *number_seconds number_samples*

The field descriptions for input/output output (see Figure 5-11 on page 5-18 for an example) are:

tin	Number of characters per second received from all terminals on the system
tout	Number of characters per second output to all terminals on the system
% user	Percentage of time system has spent in user mode
% sys	Percentage of time system has spent in system mode
% idle	Percentage of time system has spent in idle state
% iowait	Percentage of time system has spent in wait state
% tm_act	Percentage of time disk was active
Kbps	Kilobytes transferred per second
tps	Number of transfers per second
msps	Average seek time
Kb_read	Number of kilobytes read during interval reported
Kb_wrtn	Number of kilobytes written during interval reported

```
tty:      tin         tout      cpu:   % user    % sys     % idle    % iowait
          0.0          3.1                0.5      1.1       97.1       1.2

Disks:        % tm_act     Kbps      tps    msps   Kb_read   Kb_wrtn
hdisk0           1.3       2.2       0.5             26912    215638
hdisk1           0.1       0.2       0.0              3447     18368

tty:      tin         tout      cpu:   % user    % sys     % idle    % iowait
          0.0        142.8                3.5      4.0       92.5       0.0

Disks:        % tm_act     Kbps      tps    msps   Kb_read   Kb_wrtn
hdisk0           0.0       0.0       0.0                0         0
hdisk1           0.0       0.0       0.0                0         0
```

Figure 5-11. Example of Input/Output Output

Memory Management

Use the Memory Management menu item to view memory management statistics that are reported by the base operating system. These statistics show memory management information related to the network interfaces.

To use the System Manager to view memory management information:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **System Statistics** on the next menu.
3. Select **Memory Management** on the next menu.
4. A COMMAND STATUS screen displays the output. See Figure 5-12 on page 5-19 for an example of memory management output. *Mbufs* represents memory buffers.

Fast-Path Command(s)

system statistics view -memory_management

```
540 mbufs in use:
       35 mbufs allocated to data
       12 mbufs allocated to packet headers
       204 mbufs allocated to socket structures
       233 mbufs allocated to protocol control blocks
       20 mbufs allocated to routing table entries
       33 mbufs allocated to socket names and addresses
       3 mbufs allocated to interface addresses
       1 mbufs allocated to <mbuf type 17>
32/74 mapped pages in use
431 Kbytes allocated to network (61% in use)
0 requests for memory denied
0 requests for memory delayed
0 calls to protocol drain routines
```

Figure 5-12. Example of Memory Management Output

Paging Space

Use the Paging Space menu item to view the characteristics of paging spaces. Characteristics displayed in the output are:

- Paging space name
- Physical volume name
- Volume-group name
- Size
- Percentage of paging space used
- Indication of whether paging space is active or inactive
- Indication of whether paging space is set to automatic or not
- Paging space type; *lv* is logical volume

To use the System Manager to view paging space information:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **System Statistics** on the next menu.
3. Select **Paging Space** on the next menu.
4. A COMMAND STATUS screen displays the output.

   See Figure 5-13 for an example of paging space output.

Fast-Path Command(s)

system statistics view -paging_space

```
Function name: Paging Space

Page Space   Physical Volume  Volume Group  Size  %Used  Active  Auto  Type
hd61         hdisk1           rootvg        16MB  81     yes     yes   lv
hd6          hdisk0           rootvg        32MB  63     yes     yes   lv
```

Figure 5-13. Example of Paging Space Output

System Socket

To use the System Manager to view system socket information that is reported by the base operating system:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **System Statistics** on the next menu.
3. Select **System Socket** on the next menu.
4. A COMMAND STATUS screen displays the output.

Fast-Path Command(s)

system statistics view -socket_info

The field descriptions for the system socket output (see Figure 5-14 for an example) are:

SADR/PCB	System address of the protocol control block
Type	Socket type
Recv-Q	Receive queue size
Send-Q	Send queue size
Inode	Disk inode associated with the socket
Conn	Control block of a connected socket
Refs	Referencing socket linked list
Nextref	Pointer to socket referencing linked list

```
Active UNIX domain sockets
SADR/PCB  Type  Recv-Q Send-Q    Inode     Conn     Refs     Nextref
 54f0a14 stream      0      0  5840928        0        0        0 /tmp/sysmon.action
 54f0b14
 54f0c14 stream      0      0        0  54ef114        0        0
 54ef514
 54e3014 dgram       0      0  5840108        0        0        0 /dev/SRC
 54f0014
 54f0d14 stream      0      0        0  54ef514        0        0
 54ef114
 54ee114 stream      0      0        0  54ee414        0        0
 54ee214
 54ef414 stream      0      0        0  54ef714        0        0
 54ef014
 54ee314 stream      0      0        0  54ee214        0        0
 54ee414
 54ef314 dgram       0      0  5840a60        0        0        0 /dev/.SRC-unix/SRCEigCnm
 54f0e14
 54eea14 stream      0      0        0  54eed14        0        0
```

Figure 5-14. Example of System Socket Output

Active Internet Connection

These statistics show active Internet connection information that is reported by the base operating system.

To use the System Manager to view active Internet connection information:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **System Statistics** on the next menu.
3. Select **Active Internet Connection** on the next menu.
4. A COMMAND STATUS screen displays the output. See Figure 5-15 for an example.

Fast-Path Command(s)

system connections view

The field descriptions for the active internet connection output (see Figure 5-15) are:

PCB/ADDR Protocol control block address

Proto Protocol name

Recv-Q Receive queue size

Send-Q Send queue size

Local Address Local address

Foreign Address Remote address

(state) Connection state status

```
Active Internet connections
PCB/ADDR Proto Recv-Q Send-Q Local Address  Foreign Address (state)
 5548714 tcp        0      0 1.1.1.1.23     1.1.1.2.1639    ESTABLISHED
 5548b14 tcp        0      0 1.1.1.1.23     1.1.1.2.1638    ESTABLISHED
 5548d14 tcp        0      0 127.0.0.1.199  127.0.0.1.1025  ESTABLISHED
 5551514 tcp        0      0 127.0.0.1.1025 127.0.0.1.199   ESTABLISHED
 5553d14 tcp        0      0 127.0.0.1.199  127.0.0.1.1024  ESTABLISHED
 5552614 tcp        0      0 127.0.0.1.1024 127.0.0.1.199   ESTABLISHED
```

Figure 5-15. Example of Active Internet Connection Output

Three-Digit LED Display

There is a 3-digit light-emitting diode (LED) display on the operator panel of the 6611 that displays error and status codes at various times during 6611 operation. The value displayed can be read remotely from the 6611 using the System Manager.

For more information about error and status codes, refer to the *IBM Multiprotocol Network Program Operations Pocket Guide*.

To use the System Manager to retrieve error or status codes which appear on the 3-digit LED display:

1. Log in using a controlling user ID.
2. Select **Problem Determination** on the System Manager main menu.
3. Select **Three-Digit LED Display** from the next menu.
4. A COMMAND STATUS screen displays the error or status code along with its meaning and user response.

   If an error or status code is currently not displayed on the 3-digit display, you will see the message:

   ```
   The 3-digit display is blank.
   ```

Fast-Path Command(s)

led view

Figure 5-16 shows an example of the display output when you read the 3-digit display using the System Manager.

```
Code: 10c
Message: The system monitor process cannot access the adapter
installed in slot 1 because of a problem with:

    System code that communicates with the adapter
    Adapter microcode
    Adapter hardware

User Response:  For a suspected software problem, check
the error log to determine a software problem.

For a suspected hardware problem:

    Execute adapter diagnostic tests
    Check the adapter for correct installation
    Check the adapter for defects
```

Figure 5-16. Sample Output from Reading the 3-Digit Display

Error Logs and Reports

The Multiprotocol Network Program uses an error log to record activities that occur on the base operating system and the peer-capable adapters. Some of the recorded errors are sent as traps to the 6611 SNMP Trap Facility to communicate error information to you and to IBM service personnel.

Most of the activities recorded in the error log are error conditions. A subset of the errors recorded are classified as *alerts*. Alerts are events that require a user response, for example:

Error:	Adapter disabled
Probable Cause:	Hardware failure

User Response: Call service personnel

Alerts are converted to SNMP traps and transmitted to the network management station, if one exists. The trap data presented at the SNMP network management station tells you the action to perform. In some cases, you receive error notification on the 3-digit display of the 6611.

If IBM NetView* for AIX is used as the SNMP network manager, all traps can be converted to alerts and forwarded to NetView. Refer to the *IBM 6611 Network Processor Network Management Reference* for more information about using an SNMP network manager and traps.

Warning: The error log has a capacity of 1 MB and wraps when it is filled. Generally, the entries in the error log should never be deleted. However, entries for specific hardware failures should be deleted after the hardware has been replaced. Otherwise, errors in the log from the failed hardware will continue to appear in error reports.

To use the System Manager to work with error logs and reports:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Error Logs and Reports** on the next menu.

Figure 5-17 shows the Error Logs and Reports menu.

```
IBM 6611
                          Error Logs and Reports

Move cursor to desired item and press Enter.

  View an Error Report
  View Error Log Continuously
  View an Error Report for a Single Sequence Number

  Copy Error Log to Transfer Directory
  Clear the Error Log









F1=Help           F2=Redraw screen    F3=Return          F4=SysID
F10=Main Menu                         Esc+L=Turn Log On
```

Figure 5-17. Error Logs and Reports Menu

Contents of an Error Record

An error record contains the following information:

- Error label and error ID
- Date and time
- Sequence number
- Machine ID and node ID
- Error class (hardware [H], software [S], or operator [O])
- Resource name
- Resource class (hardware only)
- Vital product data (hardware only)
- Error type:

Permanent (PERM)	For conditions when the recovery is unsuccessful.
Performance (PERF)	For conditions that degrade performance of a component (hardware and software) below an acceptable level.
Impending (PEND)	For conditions that signify the loss of a component is threatened.
Temporary (TEMP)	For conditions when the recovery is successful. This error type is also used for non-error events.
Unknown (UNKN)	For conditions when the severity cannot be determined.

- Error descriptions contain messages indicating what caused the event and what action can be taken, if any. The four types of cause or action messages are:
  - Probable cause messages
  - Failure-related error cause or action messages
  - Installation-related cause or action messages
  - User-related cause or action messages

  For each cause or action message, up to four message texts can be displayed. Of the four types of causes, the probable cause message and at least one of the remaining three types of cause messages is provided.

View an Error Report

To use the System Manager to view an error report:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Error Logs and Reports** on the next menu.
3. Select **View an Error Report** on the next menu.
4. On the dialog screen:
   a. Press **Tab** to select a style of error report, either **summary** or **detailed**.

      The detailed report contains all the data in the error record in readable form. The summary report contains:

      - Event ID value (ERROR_ID)
      - Time stamp (TIMESTAMP)
      - Severity (T)
      - Event class (CL)
      - Resource name (RESOURCE_NAME)
      - Event description message (ERROR_DESCRIPTION)

b. Select values from the dialog screen to limit the scope of the error report. Use the default values in the dialog items to get a full report. If a null report is created, you have chosen a combination of options that are not found in the error log.

Error classes

Press **F4 (Esc+4)** to list, **F9 (Esc+9)** to select, and **Enter** to record selections. If you type in your selections, you cannot use lowercase letters. Only the following uppercase letters are supported:

- H (hardware)
- S (software)
- O (operator)

The default is all.

Error types

Press **F4 (Esc+4)** to list, **F9 (Esc+9)** to select, and **Enter** to record selections.

- PERM (permanent)
- TEMP (temporary)
- PERF (performance)
- PEND (impending)
- UNKN (unknown)

The default is all.

Resource classes

Press **F4 (Esc+4)** to list, **F9 (Esc+9)** to select, and **Enter** to record selections from a hardware device class list. This field is only selected for hardware errors.

The default is all.

Resource names

Press **F4 (Esc+4)** to list, **F9 (Esc+9)** to select, and **Enter** to record selections. For hardware errors, the resource name is a device name. For software errors, the resource name is the name of the failing executable resource.

Error ID filter action

Press **Tab** to select **include** or **exclude**. The default is **include**.

Error IDs on which to filter

Press **F4 (Esc+4)** to list, **F9 (Esc+9)** to select, and **Enter** to record selections. The default is all.

Starting date and time

Type in **MMDDhhmmYY** format.

Ending date and time

Type in **MMDDhhmmYY** format.

Fast-Path Command(s)

error report -detail *start_date end_date*
error report -summary *start_date end_date*
error report -error_ID [-detailI-summary] *error_ID start_date end_date*
error report -hardware [-detailI-summary] *start_date end_date*
error report -hw_resource [-detailI-summary] *hw_resource start_date end_date*
error report -software [-detailI-summary] *start_date end_date*
error report -sw_resource [-detailI-summary] *sw_resource start_date end_date*
error report -operator [-detailI-summary] *start_date end_date*

Figure 5-18 displays an example of summary style error report output.

```
ERROR_ID TIMESTAMP  T CL RESOURCE_NAME  ERROR_DESCRIPTION
9DBCFDEE 1203125991 T O  errdemon       Error logging turned on
192AC071 1202161691 T O  errdemon       Error logging turned off
FCA960CE 1120114691 T S  tok0           EXCESSIVE TOKEN-RING ERRORS
C14C511C 1120113291 T H  scsi0          ADAPTER ERROR
C14C511C 1120113291 T H  scsi0          ADAPTER ERROR
74533D1A 1120113191 U H  SYSIOS         LOSS OF ELECTRICAL POWER
9DBCFDEE 1120113391 T O  errdemon       Error logging turned on
74533D1A 1107094791 U H  SYSIOS         LOSS OF ELECTRICAL POWER
C14C511C 1031070991 T H  scsi0          ADAPTER ERROR
74533D1A 1031065091 U H  SYSIOS         LOSS OF ELECTRICAL POWER
83F06558 0915220491 P S  SYSPROC        SOFTWARE PROGRAM ABNORMALLY TERMINATED
AA8AB241 0914230491 T O  OPERATOR       OPERATOR NOTIFICATION
9DBCFDEE 0913556891 T O  errdemon       Error logging turned on
192AC071 0912456791 T O  errdemon       Error logging turned off
```

Figure 5-18. Example of View an Error Report Output - Summary Style

View Error Log Continuously

To view the error log in real time:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Error Logs and Reports** on the next menu.
3. Select **View Error Log Continuously** on the next menu.

   The output scrolls continuously on the screen as entries are made to the error log.
4. Press **Ctrl+C** to stop your request.

Fast-Path Command(s)

error report -continuous

View an Error Report for a Single Sequence Number

Each error record contains a unique sequence number. This sequence number is sent to the network management station in the trap.

To use the System Manager to view a detailed error report for a single sequence number:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Error Logs and Reports** on the next menu.
3. Select **View an Error Report for a Single Sequence Number** on the next menu.
4. On the selector screen, select the sequence number from a list of all sequence numbers that are currently in the error log. The list can be long. Press **Enter** to execute.
5. A COMMAND STATUS screen displays the error report if it is less than 512 kilobytes. If the error report is greater than 512 kilobytes, it is sent to the transfer directory as `pd_error.report`. You can view it from the fast-path environment by issuing the command:

   ```
   files transfer view pd_error.report
   ```

Fast-Path Command(s)

error report -sequence_number *sequence_number*

Figure 5-19 on page 5-29 shows an example of a software error report.

```
ERROR LABEL:   SNMP_05
ERROR ID:  0FF3E351

Date/Time:       Mon Nov 11 10:32:09
Sequence Number: 74529
Machine Id:      000000183000
Node Id:         whip1
Error Class:     S
Error Type:      PERM
Resource Name:   snmp

Error Description
SOFTWARE PROGRAM ERROR

Probable Causes
SOFTWARE PROGRAM

Failure Causes
SOFTWARE PROGRAM

   Recommended Actions
   CONTACT SERVICE REPRESENTATIVE
   REPORT THE FOLLOWING
Detail Data
SYMPTOM CODE
5549       smux.t1d      interface-snmp  192
FILE NAME
snmp.config
REFERENCE CODE
423
```

Figure 5-19. Example of View an Error Report for a Single Sequence Number (Software Error)

Figure 5-20 on page 5-30 shows an example of a hardware error report.

```
ERROR LABEL:       TOK_RCVRY_ENTER
ERROR ID:          0502F666

Date/Time:         Jun 19 22:29:51
Sequence Number:   6824
Machine ID:        123456789012
Node ID:           u2
Class:             H
Type:              TEMP
Resource Name:     tok0
Resource Class:    adapter
Resource Type:     tokenring
Location:          00-03
VPD:
     Network Address.............10005A4F35D2
     Display Message.............TOKEN RING
     EC Level....................A78976
     FRU Number..................022F9380
     Manufacturer................VEN0809375
     Part Number.................074F4134
     Serial Number...............009683
     ROS Level and ID............0000
     Loadable Microcode Level....00
Error Description
ADAPTER ERROR

Probable Causes
REMOTE CSMA/CD ADAPTER
LOCAL TOKEN-RING ADAPTER
ADAPTER HARDWARE
ADAPTER MICROCODE

Failure Causes
LOCAL TOKEN-RING ADAPTER INTERFACE
TOKEN-RING ADAPTER

   Recommended Actions
   CHECK CABLES AND THEIR CONNECTIONS
   WAIT THEN RETRY
   PERFORM PROBLEM DETERMINATION PROCEDURES

Detail Data
SENSE DATA
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
```

Figure 5-20. Example of View an Error Report for a Single Sequence Number (Hardware Error)

Copy Error Log to Transfer Directory

To use the System Manager to copy the error log to the transfer directory, so that you can retrieve the error log and generate reports:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Error Logs and Reports** on the next menu.

3. Select **Copy Error Log to Transfer Directory** on the next menu.

   The error log is placed in the transfer directory as `pd_error.log`.

Fast-Path Command(s)

error transfer -error_log

Figure 5-21 shows an example of the status message that you receive after the copy completes. There is no other output.

```
The error log was copied to pd_error.log in the transfer directory.
```

Figure 5-21. Example of Copy Error Log to Transfer Directory Output

Clear the Error Log

The error log has a capacity of 1 MB and wraps when it is filled. Generally, the entries in the error log should never be deleted. However, entries for specific hardware failures should be deleted after the hardware is replaced. Otherwise, errors in the log from the failed hardware will continue to appear in error reports.

To use the System Manager to delete specific error log entries:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **Error Logs and Reports** on the next menu.
4. Select **Clear the Error Log** on the next menu.
5. Select appropriate days, resource classes, resource names, and error IDs from the dialog screen to limit deleting the entries for the failed hardware:

   Remove entries older than this number of days
   Supply the number of days.

   Remove entries for these resource classes
   Press **F4 (Esc+4)** to list, **F9 (Esc+9)** to select, and **Enter** to record the selections. Valid options are any resource class in the hardware device class list.

   Remove entries for these resource names
   Press **F4 (Esc+4)** to list, **F9 (Esc+9)** to select, and **Enter** to record the selections.

   Remove entries for these error IDs
   Press **F4 (Esc+4)** to list, **F9 (Esc+9)** to select, and **Enter** to record the selections.
6. A COMMAND STATUS screen appears, but no output is displayed from the Clear the Error Log menu item.

Fast-Path Command(s)

error clear *number_of_days*
error clear -error_ID *error_ID number_of_days*
error clear -hardware *number_of_days*
error clear -hw_resource *hw_resource number_of_days*
error clear -operator *number_of_days*
error clear -software *number_of_days*
error clear -sw_resource *sw_resource number_of_days*

System Dump

Use System Dump to dump the base operating code of a 6611. Only a controlling user can issue dump requests. Figure 5-22 shows the System Dump menu.

```
IBM 6611                                                        hostname
                                System Dump

Move cursor to desired item and press Enter.

  Start
  View Dump Information
  Copy to Diskette or Transfer Directory
  Format

  Extract Error Log Records
  Extract Trace Log Records









F1=Help             F2=Redraw screen    F3=Return           F4=SysID
F10=Main Menu                           Esc+L=Turn Log On
```

Figure 5-22. System Dump Menu

Start

To use the System Manager to start a system dump to the dump device, */dev/hd7*:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **System Dump** on the next menu.
4. Select **Start** on the next menu.

You receive the following ARE YOU SURE? message warning you of the results of the 6611 dump:

```
                    ARE YOU SURE?

Executing this command will shut down your IBM 6611,
stopping all the protocols and processes including
the current System Manager session.
Performing this function requires controlling user
privileges. If you are a viewing user, you will be
logged out from this IBM 6611.  Press the Reset
button to restart the 6611 when the dump completes.

    Press Enter to start the system dump.
    Press F3 (Esc+3) to cancel and return to
        the System Manager.



F1=Help          F2=Redraw Screen  F3=Return
F10=Main Menu
```

5. Press **Enter** to continue the 6611 dump:

   You receive the following INFORMATION MESSAGE stating that your System Manager session is stopped:

```
                  INFORMATION MESSAGE


NOTE: This command needs to be run outside of the
      System Manager.  The System Manager will
      exit immediately before running this
      command.

   Press Enter to proceed with the command.

   Press F3 (Esc+3) to cancel and return to
   the System Manager.

F1=Help          F2=Redraw Screen  F3=Return
F10=Main Menu
```

6. Press **Enter** to start the dump process.

   `0c2` is displayed in the 3-digit display on the 6611 during the dump process. `0c0` is displayed when the dump is complete.

7. Press **Reset** push button to restart the 6611.

Fast-Path Command(s)

system dump

View Dump Information

The 6611 dump device, */dev/hd7*, stores the last system dump taken. Certain statistical information about the last dump is also kept, such as the date and time of the last dump, the number of blocks written, and the completion status.

To use the System Manager to view previous system dump information:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **System Dump** on the next menu.
4. Select **View Dump Information** on the next menu.
5. If no dump is available, the following message is displayed:

   ```
   There is no previous system dump to view.
   ```

Fast-Path Command(s)

system dump view -previous_dump info

Figure 5-23 shows an example of view dump information output.

```
Device name:          /dev/hd7
Major device number: 10
Minor device number: 4
Size:                 3461632 bytes
Date/Time:            Sat Jul 10 10:15:57 CDT 1993
Dump status:          successful
```

Figure 5-23. Example of View Dump Information Output

Copy to Diskette or Transfer Directory

You can copy the system dump to a diskette or place the dump in the transfer directory. You can then view the dump while it resides in the dump device or transfer it out of the 6611 to be viewed using a remote 6611.

To use the System Manager to copy a system dump to a diskette or to the transfer directory:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **System Dump** on the next menu.
4. Select **Copy to Diskette or Transfer Directory** on the next menu.

5. Select a system dump destination (**dump diskette** or **transfer directory**) from the selector screen. If sent to the transfer directory, the system dump can be exported using:
   - FTP
   - A modem
   - A DOS diskette
   - A UNIX diskette

Fast-Path Command(s)

system dump transfer

An example of the status message you receive is:

```
The system dump is copied to the transfer directory as pd_system.dump
```

Figure 5-24. Example of System Dump Status Message

Format

The formatted dump facility interprets and formats the control structures in the base operating system and certain miscellaneous functions that are useful when examining a system dump.

To use the System Manager to view a formatted system dump:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **System Dump** on the next menu.
4. Select **Format** on the next menu.
5. Select the current dump location (**dump device** or **transfer directory**) from the System dump location selector screen.
6. Wait several minutes until the format processing stops.

   If no dump is available, the following message is displayed:

```
There is not a dump in the dump device or the dump device
cannot be accessed.
```

Figure 5-25. Example of No Dump Available Message

Fast-Path Command(s)

system dump format -dump_device
system dump format -transfer

Figure 5-26 shows an example of the beginning of the format output. The formatted dump is placed in the transfer directory in the file named pd_system.fdump. Select **File and Diskette Operations** from the Operations menu of the System Manager to view the dump in the transfer directory file.

```
SYSTEM STAT:

        sysname: IBM 6611
        nodename: u2
        release: 1
        version: 0
        machine: 000268543100
        time of crash: Sat Jul 10 10:15:57 1993
        age of system: 4 day, 15 hr., 50 min.
SYSTEM VARIABLES

[MORE...10995]
```

Figure 5-26. Example of a Partial Format Output

Extract Error Log Records

When the writing of a record to the error log on the hard disk is interrupted by a system dump, the error log record is still available in the system dump.

To use the System Manager to extract error log records from a system dump and copy them into the error log:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **System Dump** on the next menu.
4. Select **Extract Error Log Records** on the next menu.
5. If there are no lost error records, the following message is displayed:

```
There are no error records to extract from the previous system dump.
```

Figure 5-27. Example of No Lost Error Records Message

If error records do exist, the error log records are copied into the error log.

Fast-Path Command(s)

system dump extract -error_log

Extract Trace Log Records

When the writing of a record to the trace log on the hard disk is interrupted by a system dump, the trace log record is still available in the system dump.

To use the System Manager to extract trace log records from a system dump and copy them into the trace log:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **System Dump** on the next menu.
4. Select **Extract Trace Log Records** on the next menu.
5. If there are no lost trace records, the following message is displayed:

```
There are no trace records to extract from the previous system dump.

A trace session must be in progress when the system dump is invoked.
```

Figure 5-28. Example of No Lost Trace Records Message

If trace log records do exist, the trace log records are copied into the trace log.

Fast-Path Command(s)

system dump extract -trace_log

Process and Protocol Dumps

Use this function to nondisruptively start or view dumps of selected protocols, or to disruptively start or view dumps of any user process. Only controlling users can issue dump requests. Figure 5-29 on page 5-38 shows the Process and Protocol Dumps menu.

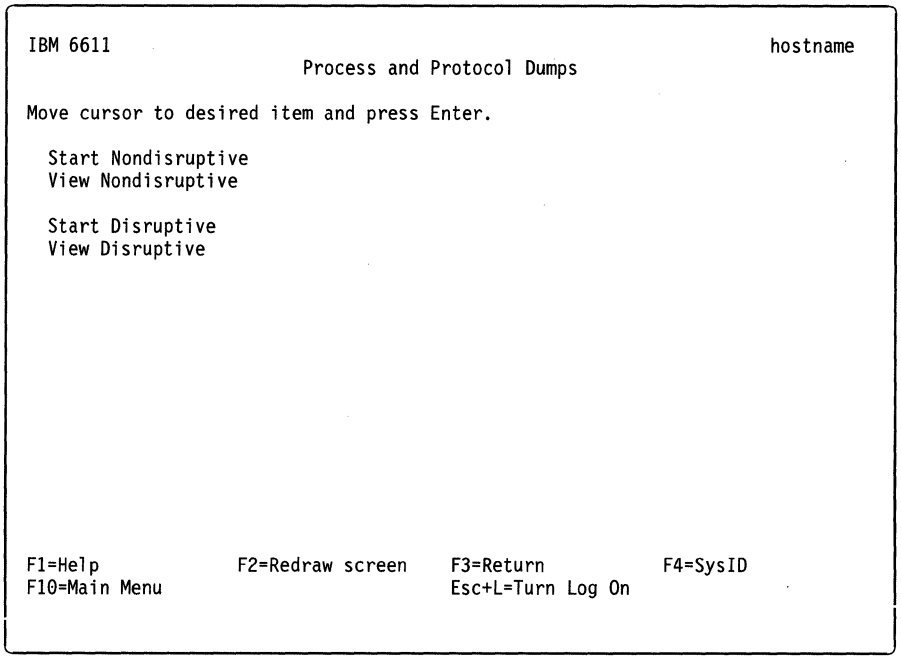


Figure 5-29. Process and Protocol Dumps Menu

Start Nondisruptive

To use the System Manager to start a nondisruptive dump of a selected protocol:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **Process and Protocol Dumps** on the next menu.
4. Select **Start Nondisruptive** on the next menu.
5. Select the protocol to dump from the list in the selector screen:
   - IP
   - VINES
   - DLSw
   - APPN
   - IPX
6. The dump is placed in the transfer directory. The name of the dump is displayed in a message, such as:

```
VINES routing protocol dump has started...
The VINES protocol dump is in the transfer directory as
pd_route_vines.dump.
```

Figure 5-30. Example of Start Nondisruptive Dump Message

The dumped output depends on the protocol you select.

Fast-Path Command(s)

ip dump
vines dump
dls dump
appn dump
ipx dump

View Nondisruptive

To use the System Manager to view a nondisruptive dump of a selected process:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Process and Protocol Dumps** on the next menu.
3. Select **View Nondisruptive** on the next menu.
4. Select the protocol whose dump you want to view from the list in the selector screen:
   - IP
   - VINES
   - DLSw
   - APPN
   - IPX
5. If a dump exists, a COMMAND STATUS screen displays the dump. If the dump does not exist, you will get a message stating that the dump could not be found in the transfer directory. You may need to start a dump of that protocol first.

Fast-Path Command(s)

files transfer view *file_name*

where *file_name* is the name of the dump you want to view

Start Disruptive

Any active user process in the 6611 can be sent a signal telling it to dump its memory. This is a disruptive dump; the user process must be restarted by restarting the 6611.

A user process disruptive dump is created automatically if the process crashes.

The dump is automatically sent to the transfer directory, where you can view it or transfer it to a remote node.

To use the System Manager to start a disruptive dump of a user process:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **Process and Protocol Dumps** on the next menu.
4. Select **Start Disruptive** on the next menu.

5. Select a process name from the list in the selector screen.
6. You receive the following warning message:

```
                    ARE YOU SURE?

Executing a dump on a user process terminates
the process.  Dumping certain processes may hang
your terminal or even bring down your IBM 6611,
stopping all the protocols and processes
including the current System Manager session.

    Press Enter to continue with the dump.
    Press F3 (Esc+3) to cancel and return to
        the System Manager.



F1=Help           F2=Redraw Screen    F3=Return
F10=Main Menu
```

7. Press **Enter** to start the dump process.
8. This status message is displayed:

```
The dump has started.
When completed, the dump will be located in
the transfer directory referenced by the process name.
```

Figure 5-31. Example of Start Disruptive Dump Message

Fast-Path Command(s)

process dump *processID*

View Disruptive

To use the System Manager to view a memory dump of a user process:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Process and Protocol Dumps** on the next menu.
3. Select **View Disruptive** on the next menu.
4. Select a process dump name from the list in the selector screen.
5. A COMMAND STATUS screen displays the dump, an example of which is shown in Figure 5-32 on page 5-41.

Fast-Path Command(s)

files transfer view *file_name*

Where *file_name* is the name of the dump you want to view.

Figure 5-32 on page 5-41 shows an example of view disruptive output.

```
00000000:    06700003   000048A4   00004E0F   00002FE8    .p....H...N.../.
00000010:    2FF7DC80   00000000   00000000   0B000000    /...............
00000020:    0000283A   00000000   D00F22A8   0000D0B0    ..(:......".....
00000030:    00224000   D00F22A8   DEADBEEF   DEADBEEF    ."@..."."".....
00000040:    DEADBEEF   00000000   00000000   01000000    ................
00000050:    30000000   40000000   200006A4   30000000    0...@... ...0...
00000060:    00000106   00000000   00000000   00000000    ................
00000070:    00000000   00000000   00000000   00000000    ................
00000080:    00000000   00000000   00000000   00000000    ................
00000090:    00000000   00000000   00000000   E01E0000    ................
000000A0:    40000707   40001A9A   40000666   007FFFFF    @...@...@..f....
000000B0:    007FFFFF   007FFFFF   007FFFFF   007FFFFF    ................
000000C0:    007FFFFF   007FFFFF   007FFFFF   007FFFFF    ................
000000D0:    007FFFFF   40000A0A   007FFFFF   007FFFFF    ....@...........
000000E0:    DEADBEEF   2FF7E018   2001C128   00000158    ..../... ..(...X
000000F0:    DEADBEEF   DEADBEEF   DEADBEEF   DEADBEEF    ................
00000100:    DEADBEEF   DEADBEEF   DEADBEEF   DEADBEEF    ................
00000110:    DEADBEEF   200528F0   200528D8   20052D20    .... .(. .(. .-
00000120:    00000000   20051A10   200533B8   200533C8    .... ... .3. .3.
00000130:    20052D28   200534A8   20051A10   00000000     .-( .4. .......
00000140:    20052D36   20052078   000A0007   20052D39     .-6 . x.... .-9
00000150:    00000000   00001000   2007C7C8   2007C7C8    ........ ... ...
00000160:    00000000   00000000   00000000   00000000    ................
00000170:    00000000   00000000   00000000   00000000    ................
00000180:    00000000   00000000   00000000   00000000    ................
```

Figure 5-32. Example of View Disruptive Output

System Trace

The system trace facility is a system observation tool that captures a sequential flow of time-stamped system events. This facility is used by service personnel for problem determination. The trace goes to a 1 MB trace log that wraps when it is full. You can issue start and stop trace requests and generate and view trace reports.

Figure 5-33 on page 5-42 shows the System Trace menu.

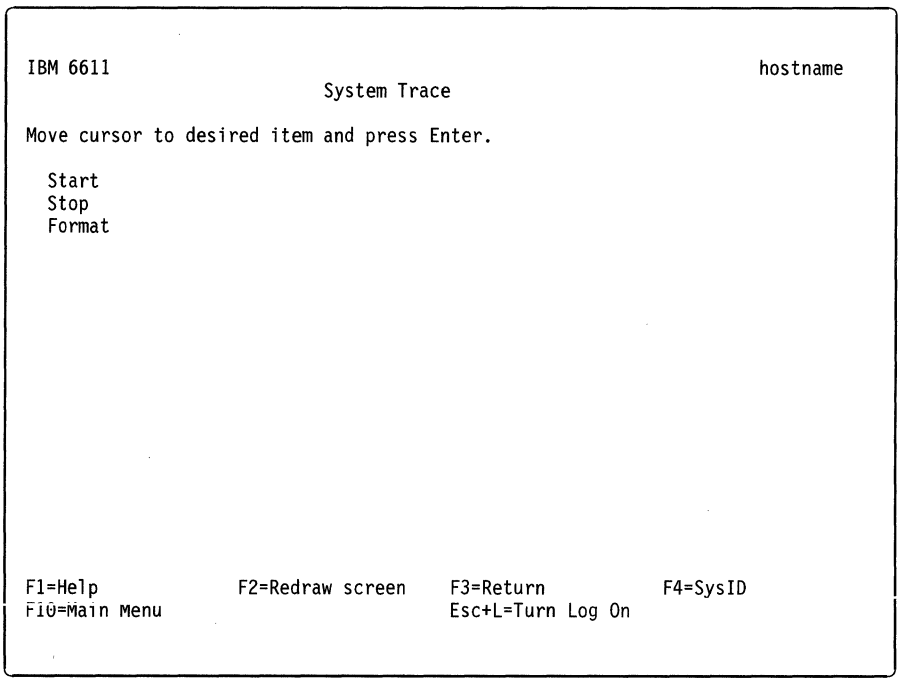


Figure 5-33. System Trace Menu

Start

Three buffer modes are available for tracing:

Circular buffer mode Two collection buffers are maintained. When one buffer becomes full, collection switches to the second buffer. The previous contents in the buffers are overwritten. The two buffers are written to the trace log when the trace is stopped. Only the last two buffers' worth of data is collected.

Alternate buffer mode Two collection buffers are maintained. When one buffer becomes full, collection switches to the second buffer, while the contents of the first buffer are written to the trace log. All data is collected, except when the trace log fills up.

Single sweep buffer mode A single collection buffer is maintained. The trace is stopped when the buffer is filled, or when a trace stop request is received, whichever happens first. The trace data is then written to the trace log.

To use the System Manager to start a system trace:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **System Trace** on the next menu.
4. Select **Start** on the next menu.
5. Select a trace mode, trace buffer size, trace log size, and event IDs from the dialog screen.

Additional event IDs to include in trace
Press **F4 (Esc+4)** to list, **F9 (Esc+9)** to select, and **Enter** to record selections. The default is **None**.

Trace mode
Press **Tab** to select either **alternate**, **single**, or **circular**.

Trace buffer size in bytes
Define between 8192 and 524288 (between 8K and 512K). This value must be in decimal. The default is 131072 or 128K.

Trace log size in bytes
Define between 1048576 and 10485760. The default is 1048576 or 1 M.

Fast-Path Command(s)

system trace -on (-trace_ID) *trace_IDs*
system trace -on -trace_group *trace_groups*

No output is generated from the Start menu.

Stop

To use the System Manager to stop a system trace:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **System Trace** on the next menu.
4. Select **Stop** on the next menu.

   No output is generated from the Stop menu.

Fast-Path Command(s)

system trace -off

Format

The system trace facility creates a formatted trace report. The report can include:

- The whole trace log
- Selected specific event IDs
- Only trace records recorded between a specific start and end date and time

You may also specify specific event IDs to exclude.

To use the System Manager to view a system trace report:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **System Trace** on the next menu.
4. Select **Format** on the next menu.

5. Select values from the dialog screen to limit the scope of the trace report. To get a full report, use the default.

   Event ID filter action
   Press **Tab** to select **include** or **exclude**. The default is include.

   Event IDs on which to filter
   Press **F4 (Esc+4)** to list, **F9 (Esc+9)** to select, and **Enter** to record selections. The default is all.

   Starting date and time
   Type in **MMDDhhmmssYY** format.

   Ending date and time
   Type in **MMDDhhmmssYY** format.

6. A COMMAND STATUS screen displays the trace report, if it is less than 512 kilobytes. If the trace report is greater than 512 kilobytes, it is sent to the transfer directory as `pd_trace.report`. It must be viewed from the fast-path environment by issuing:

   files transfer view pd_trace.report

   Figure 5-34 on page 5-45 shows an example of format output. If the status changes from `running` to `OK` and no trace output is displayed, no trace records meet the specified date and event ID criteria.

Fast-Path Command(s)

system trace report -all *start_time end_time*
system trace report -trace_ID *trace_IDs*

```
Tue May 26 13:15:46 1992
System: IBM 6611 000013163000 Node: 3
Machine: 000013163000
Internet Address: 00000000 0.0.0.0


ID  PROCESS NAME   PID      I SYSTEM CALL     ELAPSED   APPL    SYSCALL KERNEL  INTERRUPT

001 trace          10526                     0.000000                  TRACE ON channel 0
20F trace          10526                     0.000055                  unlockl         lock addr=11478
20E trace          10526                     0.000065                  lockl           lock addr=30C38
20F trace          10526                     0.000080                  unlockl         lock addr=30C38
104 trace          10526                     0.000086          return from system call
101 trace          10526      getppid        0.000112          getppid
147 trace          10526      getppid        0.000116                  GETPPID
104 trace          10526      getppid        0.000120          return from getppid [8 usec]
101 trace          10526      kill           0.000137          kill
14E trace          10526      kill           0.000146                  kill: signal SIGUSR1 to process 10269 trace
20E trace          10526      kill           0.000153                  lockl           lock addr=30C30
119 trace          10526      kill           0.000183                  KERN_SENDSIGNAL hookdata 0000
11F trace          10526      kill           0.000208                  set on ready queue trace 10269
11F trace          10526      kill           0.000238                  set on ready queue trace 10526
106 trace          10269                     0.000249                  dispatch trace 10269
200 trace          10269                     0.000261                  resume   trace
20F sysmon         7006                      0.145551                  unlockl         lock addr=56E8248
20E sysmon         7006                      0.145576                  lockl           lock addr=56E8248
20F sysmon         7006                      0.145590                  unlockl         lock addr=56E8248
20E sysmon         7006                      0.145710                  lockl           lock addr=30C38
20F sysmon         7006                      0.145769                  unlockl         lock addr=30C38
100 sysmon         7006                      0.145841                          DATA ACCESS PAGE FAULT
1B4 sysmon         7006                      0.145869                  VMM lockmiss:         V.S=02DD.345A ppage=03C1
                   persistent_storage journaled system_segment modified
200 sysmon         7006                      0.145895                  resume   sysmon
403 kproc          514        1              3.587969                  (0010,0000,0000) rs offlevel ret 0 @ 2315
103 kproc          514        1              3.587981                          return from slih [121 usec]
200 kproc          514        1              3.587988                  resume    IDLE
100 kproc          514                       3.589197                          I/O INTERRUPT
102 kproc          514        1              3.589214                          slih clock [1354 usec]
234 kproc          514        1              3.589236                  KERN_PROF 7630  [10007 usec]
103 kproc          514        1              3.589315                          return from slih [100 usec]
10C kproc          514        1              3.589347                  DISPATCH IDLE PROCESS
200 kproc          514        1              3.589350                  resume    IDLE
100 kproc          514                       3.599195                          I/O INTERRUPT
102 kproc          514        1              3.599212                          slih clock [9997 usec]
234 kproc          514        1              3.599232                  KERN_PROF 7630  [9995 usec]
103 kproc          514        1              3.599296                          return from slih [84 usec]
10C kproc          514        1              3.599321                  DISPATCH IDLE PROCESS
```

Figure 5-34. Example of Format Output

Protocol and Process Traces

System Manager provides access to those traces that are designed to help debug problems in their respective protocols or processes. Some traces run continually, and some must be started and stopped manually.

Figure 5-35 on page 5-46 shows the Protocol and Process Traces menu.

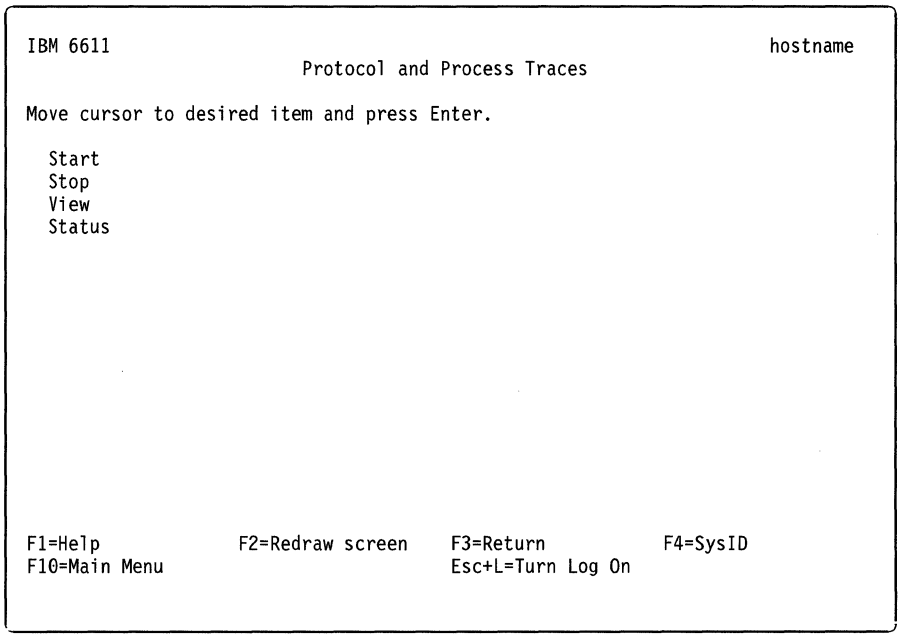


Figure 5-35. Protocol and Process Traces Menu

Start

To use System Manager to start a protocol or process trace:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **Protocol and Process Traces** on the next menu.
4. Select **Start** on the next menu.
5. Select one of the processes listed in the selector screen:
   - IP
   - IPX
   - XNS
   - DECnet
   - VINES
   - APPN
   - AppleTalk
   - DLSw
   - Source route bridge
   - Source route bridge spanning tree
   - Transparent bridge
   - Transparent bridge spanning tree
   - Translational bridge spanning tree
   - SNMP

   Depending on your selection, different sets of dialog screens are presented.

Fast-Path Command(s)

ip trace -on *trace_parameters*
ipx trace -on
xns trace -on
decnet trace -on *trace_level*
vines trace -on
appn trace -on *trace_parameters*
appletalk trace -on *trace_parameters*
dlsw trace -on
bridge srb trace -on [(-transmit)|-receive|-both] *number_frames interface*
bridge srb trace -spt -on
bridge tb trace -on *number_framesinterface*
bridge tb trace -spt -on
bridge tlb trace -spt -on
snmp trace -on *process*

Stop

To use System Manager to stop a trace:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Protocol and Process Traces** on the next menu.
3. Select **Stop** on the next menu.
4. Select one of the processes listed in the selector screen:
   - IP
   - IPX
   - XNS
   - DECnet
   - VINES
   - APPN
   - AppleTalk
   - DLSw
   - Source route bridge
   - Source route bridge spanning tree
   - Transparent bridge
   - Transparent bridge spanning tree
   - Translational bridge spanning tree
   - SNMP

Fast-Path Command(s)

ip trace -off
ipx trace -off
xns trace -off
decnet trace -off
vines trace -off
appn trace -off
appletalk trace -off
dlsw trace -off
bridge srb trace -off [(-transmit)|-receive|-both] *interface*
bridge srb trace -spt -off
bridge tb trace -off *interface* **bridge tb trace -spt -off**
bridge tlb trace -spt -off
snmp trace -off *process*

View

To use System Manager to view a trace:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Protocol and Process Traces** on the next menu.
3. Select **View** on the next menu.
4. Select the type of trace files to view on the selector screen:
   - IP
   - IPX
   - XNS
   - DECnet
   - VINES
   - APPN
   - AppleTalk
   - DLSw
   - SNMP
   - Source route bridge (SRB)
   - All spanning tree protocols (SPT)
   - Transparent bridge (TB)
   - LAN bridge (LB)
   - Point-to-Point Protocol (PPP)
   - X.25 Protocol
   - System Monitor Process (SYSMON)
5. The next step depends upon your previous selection.

   For source route bridge (SRB) and transparent bridge (TB):

   a. Select the interface on which to view bridging frame trace output on a selector screen.

   b. For SRB only, select the direction of the frames to trace:
      - **receive** allows you to trace the frames that the adapter receives.
      - **transmit** allows you to trace the frames that the adapter sends.
      - **both** allows you to trace all frames.

      The default is **receive**.

For APPN or DLSw:

Event ID filter action
Press **Tab** to select **include** or **exclude**. The default is **include**.

Event IDs on which to filter
Press **F4 (Esc+4)** to list, **F9 (Esc+9)** to select, and **Enter** to record selections. For APPN, the default values are 360 and 361. For DLSw, the default values are 000, 224, 240, 241, 242, 243, 244, 245, 246, 362, and 366.

Starting date and time
Type in **MMDDhhmmssYY** format.

Ending date and time
Type in **MMDDhhmmssYY** format.

For all other protocols, select the file name of the trace file that you want to view and the method of viewing it. Select **normal** to view the current version of the file. Select **continuous** to view the file as it is continuously updated.

6. If it is less than 512 kilobytes, a COMMAND STATUS screen displays the trace file. If the trace file is greater than 512 kilobytes, it is sent to the transfer directory and the name of the trace output file is shown in a message.

   The trace file can be viewed from the fast-path environment by issuing:

   files transfer view *file_name*

7. If the file does not exist, you will see a COMMAND STATUS screen with the message:

```
The "name of protocol" trace file could not be found.
```

Figure 5-36. Example of Missing Trace File Message

Fast-Path Command(s)

files transfer view *file_name*

Where *file_name* is the name of the trace file in the transfer directory

Status

To use System Manager to determine the status of all traces:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Protocol and Process Traces** on the next menu.
3. Select **Status** on the next menu.

Figure 5-37 on page 5-50 shows the output of this command.

```
Trace                      Status    File/Interface
-------------------------------------------------
System (inc. APPN, DLS)     OFF
IP                          OFF
IPX                         OFF     pd_ipxd.SAP
XNS                         OFF
DEC                         OFF
VINES                       OFF
AT                          OFF
SNMP                        OFF     pd_cfgd.log
                            OFF     pd_r66d.log
                             ON     pd_snmpd.log
SRB                          ON     tk0
                             ON     to1
TB                           ON     pd_brtrc.output.te0
SRB_SPT                     OFF     pd_sr-sptree
TB_SPT                      OFF     pd_tb-sptree
TLB_SPT                     OFFpd_srtb-sptree
PPP                         OFF
X25                          ON     pd_x25d.out
SYSMON                       ON     pd_sysmon.trc
Line_Trace                  OFF
```

Figure 5-37. Sample Protocol and Process Trace Status Output

Fast-Path Command(s)

system trace -status

Adapter Debug

The adapter debug facility is not used in normal operation of the 6611. This facility dumps adapter code for use by service representatives to troubleshoot problems with the peer-capable adapter software. The adapter line trace also can be used to determine data that flows to and from the 6611.

Table 5-1 lists the peer-capable adapters and explains the internal names for these adapters. The internal names are used throughout the adapter debug facility.

Table 5-1 (Page 1 of 2). Internal Adapter Name Table

Internal Adapter Name	Adapter
tktya#	1-port token-ring network 16/4 adapter
totya?	2-port serial adapter
tetya#	1-port Ethernet adapter
cetya+	serial/Ethernet combination adapter
cttya+	serial/token-ring combination adapter
detya?	2-port Ethernet adapter
dotya@	4-port serial adapter

Table 5-1 (Page 2 of 2). Internal Adapter Name Table

Internal Adapter Name	Adapter
dttya?	2-port token-ring network 16/4 adapter

Legend:

#	A number from 0 to 6
?	A number from 0 to 13
$	Either 0 or 1
+	A number from 0 to 20
@	A number from 0 to 27

Figure 5-38 shows the Adapter Debug menu.

```
IBM 6611                                                        hostname
                          Adapter Debug

Move cursor to desired item and press Enter

  Read Memory
  View Registers
  Start Line Trace
  Dump Memory









F1=Help            F2=Redraw screen    F3=Return          F4=SysID
F10=Main Menu                          Esc+L=Turn Log On
```

Figure 5-38. Adapter Debug Menu

Read Memory

To use the System Manager to read a specified part of the adapter memory:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **Adapter Debug** on the next menu.
4. Select **Read Memory** on the next menu.
5. Select an adapter from the selector screen. See Table 5-1 on page 5-50 for an explanation of the adapter name.
6. Select or provide the appropriate values on the dialog screen to specify what to read from the adapter memory:
   - Unit to read memory by

     word 4 bytes

short 2 bytes
byte 1 byte

- Address or symbol to start read

  The address can be any hexadecimal number or known symbol. If you specify an address, the read starts at that address. If you specify a symbol, the read starts at the address of that symbol. You can also enter an expression using a plus sign (+) or a minus sign (-). For example, you could enter **cat+100** and the read would start at 256 bytes beyond the address of cat.

- Length of read (based on unit to read by specified above).

  This is the specific amount of adapter memory you want to read.

7. A COMMAND STATUS screen displays the output.

   Figure 5-39 shows an example of read memory output. This example was obtained by specifying the following values on the dialog screen:

   - Unit to read by (word, short, byte): **word**
   - Address or symbol to start read: **0**
   - Length of read (in above units): **48**

Fast-Path Command(s)

adapter memory view *adapter start_addr num_words*

```
00000000:    06700003   000048A4   00004E0F   00002FE8    .p....H...N.../.
00000010:    2FF7DC80   00000000   00000000   0B000000    /...............
00000020:    0000283A   00000000   D00F22A8   0000D0B0    ..(:......".....
00000030:    00224000   D00F22A8   DEADBEEF   DEADBEEF    ."@..."."........
00000040:    DEADBEEF   00000000   00000000   01000000    ................
00000050:    30000000   40000000   200006A4   30000000    0...@... ...0...
00000060:    00000106   00000000   00000000   00000000    ................
00000070:    00000000   00000000   00000000   00000000    ................
00000080:    00000000   00000000   00000000   00000000    ................
00000090:    00000000   00000000   00000000   E01E0000    ................
000000A0:    40000707   40001A9A   40000666   007FFFFF    @...@...@..f....
000000B0:    007FFFFF   007FFFFF   007FFFFF   007FFFFF    ................
```

Figure 5-39. Example of Read Memory Output

View Registers

To use the System Manager to view the contents of the adapter registers on the screen:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **Adapter Debug** on the next menu.
4. Select **View Registers** on the next menu.
5. Select an adapter from the selector screen. See Table 5-1 on page 5-50 for an explanation of the adapter name.

6. A COMMAND STATUS screen displays the output. Figure 5-40 on page 5-53 shows an example of view registers output.

Fast-Path Command(s)

adapter registers view *adapter*

```
TCTL =   26aa3cH  ACTL = 3H PCTL =   267040H

                        ***GLOBAL REGISTERS***
G0   = deadbeefH  G1   =     2941H  G2   =        0H  G3   =   28aea0H
G4   =   2f0014H  G5   =       3fH  G6   =   26a614H  G7   =    18000H
G8   =        0H  G9   =      156H  G10  =      a18H  G11  =     1000H
G12  =        0H  G13  =   2f0000H  G14  =       20H  FP   =   26de50H

                        ***LOCAL REGISTERS***
PFP  =   267040H  SP   =        3H  RIP  = 3f000001H  R3   =   26aa3cH
R4   =    20000H  R5   =        0H  R6   =        0H  R7   =        0H
R8   =        0H  R9   =        0H  R10  =        0H  R11  =        0H
R12  =        0H  R13  =        0H  R14  =        0H  R15  =        0H
```

Figure 5-40. Example of View Registers Output

Start Line Trace

The adapter line trace can be used to trace data that comes into the adapter from the network or another adapter. Only one adapter line trace can be running at a time. The line trace record size is 1 K.

Note: Running this trace may degrade system performance.

To use the System Manager to start a line trace on an adapter:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **Adapter Debug** on the next menu.
4. Select **Start Line Trace** on the next menu.
5. Select an adapter from the selector screen. See Table 5-1 on page 5-50 for an explanation of the adapter name.
6. On the dialog screen, enter the number of packets to capture in the trace. The adapter trace stops when the specified number of packets are collected.
7. A COMMAND STATUS screen displays the output.

   An example of the message you receive when you start an adapter line trace is:

```
The line trace has been started. The line trace is collecting
in pd_trtya0.linetrace in the transfer directory.
```

Figure 5-41. Example of Start Line Trace Message

Fast-Path Command(s)

adapter trace -line -on *adapter num_packets*

Dump Memory

Select **Dump Memory** to dump the contents of the adapter memory.

Four files are placed in the transfer directory. The files contain DRAM memory, SRAM memory, PROM memory, and the contents of the registers (REGS). The output shows the dumped memory in hexadecimal with ASCII translation.

To use the System Manager to dump the memory of an adapter:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **Adapter Debug** on the next menu.
4. Select **Dump Memory** on the next menu.
5. Select an adapter from the selector screen. See Table 5-1 on page 5-50 for an explanation of the adapter name.
6. A COMMAND STATUS screen displays the output.

   An example of the message you receive when you issue an adapter dump request is:

```
SRAM dumped to /tmp/hold/transfer/pd_trtya0.sram
DRAM dumped to /tmp/hold/transfer/pd_trtya0.dram
PROM dumped to /tmp/hold/transfer/pd_trtya0.prom
REGS dumped to /tmp/hold/transfer/pd_trtya0.regs
The dump for adapter, trtya0, has been completed.
```

Figure 5-42. Example of Adapter Dump Message

Fast-Path Command(s)

adapter dump *adapter*

Protocol Debug

Figure 5-43 on page 5-55 shows the Protocol Debug menu.

```
IBM 6611                                                        hostname
                                Protocol Debug

Move cursor to desired item and press Enter.

  Source Route Bridge Adapter Table
  Network Management Subsystem Information
  DLSw General Information
  X.25 Traffic Monitor
  Protocol Debug Collection Facility









F1=Help            F2=Redraw screen    F3=Return          F4=SysID
F10=Main Menu                          Esc+L=Turn Log On
```

Figure 5-43. Protocol Debug Menu

Source Route Bridge Adapter Table

To use System Manager to view the source route bridge adapter table:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Protocol Debug** on the next menu.
3. Select **Source Route Bridge Adapter Table** on the next menu.
4. Select an interface from the selector screen. Refer to Table 4-1 on page 4-7 for an explanation about the interface name used to identify the adapters.
5. A COMMAND STATUS screen displays the output.

Fast-Path Command(s)

bridge srb view -interface_info *interface*

Figure 5-44 shows an example of the output. If source route bridging is not configured on the interface chosen, the output contains all zeros.

```
SRB Table MIB Data
 Ring Adap Port  MaxLen MaxFld Stat MaxHop Bridge DesRing DLCI LPort Type
  005   01   00    2052     20   47      7      1    ffff 0000     1  SRB
```

Figure 5-44. Example of Source Route Bridge Adapter Table Output

The field descriptions for source route bridge adapter table output are:

Ring Ring number

Adap Adapter number

Port Port number

MaxLen MTU (maximum transmission unit) size

MaxFld MTU designator

- **0x00** 516 bytes
- **0x10** 1500 bytes
- **0x20** 2052 bytes (maximum allowed by T1 connections)
- **0x30** 4472 bytes (maximum allowed for 4MB token-ring connections)
- **0x40** 8144 bytes
- **0x50** 11 407 bytes
- **0x60** 17 800 bytes (maximum allowed for 16MB token-ring connections)

Stat Status (this is a bit field)

- **0x01** Port is up and able to do bridging.
- **0x02** Single-route (limited) broadcast frames will be forwarded.
- **0x04** If set, this is a token-ring connection.

  If not set, the following bits apply:

  - **0x10** Connection is a remote bridge.
  - **0x08** Connection is Milford point-to-point connection.
  - **0x18** Connection is regular PPP connection.
  - **0x10 and 0x08** If both not set, represents frame relay connection.
  - **0x20** This ring represents the system unit.
  - **0x40** This ring is set for automatic mode with spanning tree.

MaxHop Maximum number of hops that a frame could have gone through to be allowed to go through this port.

Bridge Bridge number

DesRing Designated ring number

DLCI The DLCIs for frame relay

LPort Internal bridge number

Type SRB–source route bridging

Dual–translational bridging

Network Management Subsystem Information

Select **Network Management Subsystem Information** to create and view an SNMP process activity log, which may provide useful problem solving information. The displayed information includes:

- State of the SNMP process trace flags
- Maximum SNMP packet size
- SNMP query timeout
- SNMP subagent timeout
- All configured communities
- All configured views
- All configured subagents
- All configured SNMP trap destinations

To use the System Manager to obtain this information:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Protocol Debug** on the next menu.
3. Select **Network Management Subsystem Information** on the next menu.
4. A COMMAND STATUS screen displays the output.

   Figure 5-45 shows an example of network management subsystem information output.

Fast-Path Command(s)

snmp view -activity_log

```
 Logfile:         /tmp/hold/transfer/pd_snmpd.log
 Tracing:         ENABLED                  ACTIVE
 Debug level:     0
 Max Packet Size:9216
 Query Timeout:   60
 SMUX Timeout:    15
COMMUNITY:       public
  ADDRESS:       127.0.0.1
  NETMASK:       255.255.255.255
  PERMISSION:    readOnly
  VIEW:          1.3.6.1.3.11.2.2
VIEW NAME:       1.3.6.1.3.11.2.1
  SUBTREE(S):    iso
TRAP DESTINATION
public                        9.66.23.4
SMUX CLIENT:     1.3.6.1.4.1.2.3.1.2.1.2
  PASSWORD:      gated_password
  ADDRESS:       127.0.0.1
  NETMASK:       255.255.255.255
```

Figure 5-45. Example of Network Management Subsystem Information Output

DLSw General Information

To view selected information on the DLSw protocol:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **Protocol Debug** on the next menu.
4. Select **DLSw General Information** on the next menu.
5. On the selector screen, select an item on which to get information:

   message_queues Displays DLSw message queue usage. If you select this, you must select the queue on the next selector screen.

   semaphores Displays DLSw semaphore usage. If you select this, you must select the ID of the DLSw semaphore you want to view on the next selector screen.

   message_buffers Displays DLSw message buffer usage.

   general database Displays DLSw database information. If you select this, you can select the general database member you want to view and press **Enter**.

   conversation database Displays the complete DLSw conversation database.

6. A COMMAND STATUS screen displays the output.

   Figure 5-46 shows an example of DLSw message queue output.

Fast-Path Command(s)

dlsw debug view -message_queue *msg_que_num*
dlsw debug view -semaphore *semaphore_num*
dlsw debug view -message_buffer
dlsw debug view -general_database (-summary)
dlsw debug view -general_database *gen_db_num*
dlsw debug view -conversation_database

```
Message queue id is     : 12295
No. of bytes on queue   : 65520
No. of msgs. on queue   : 911
Max bytes on queue      : 65535
Last proc. to snd msg   : 19304
Last proc. to rcv msg   : 19326
Time of last msg snd    : 744649249
Time of last msg rcv    : 744647572
```

Figure 5-46. Example of DLSw Message Queue Output

X.25 Traffic Monitor

To view selected X.25 traffic monitor information:

1. Log in using a controlling user ID.
2. Select **Problem Determination** from the System Manager main menu.
3. Select **Protocol Debug** on the next menu.
4. Select **X.25 Traffic Monitor** on the next menu.
5. Select an adapter name from the selector screen.
6. Supply the following information on the dialog screen:
   - Packet Type

     The type of X.25 high-level data link control (HDLC) traffic that you want to monitor. The valid values are **packet**, **frame**, or **both**.
7. Press **Ctrl+C** to end the X.25 monitor. The output will be placed in the transfer directory with the file name `pd_x25mon.trc`.

Fast-Path Command(s)

x25 monitor [(-packet) &| -frame] *adapter*

Protocol Debug Collection Facility

To simplify the process of collecting pertinent debug information when the 6611 experiences a software problem, IBM created the Protocol Debug Collection Facility. The Protocol Debug Collection Facility gathers detailed debug information about bridging protocols, routing protocols, medium access control protocols, and adapter interfaces. The facility also allows you to set up and start debug traces for AppleTalk, APPN, DECnet, DLSw, and IP. The debug and trace information is stored in several files, which are then combined into one large file. For information about these files, refer to "Files Generated by the Protocol Debug Collection Facility" on page 5-61.

Note: IBM strongly urges that you only use the Protocol Debug Collection Facility when directed by IBM service representatives.

Starting Protocol Traces

To set up start protocol traces:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Protocol Debug** on the next menu.
3. Select **Protocol Debug Collection Facility** on the next menu.
4. Select the protocol from the selector screen:
   - AppleTalk
   - APPN
   - DECnet
   - DLSw
   - IP
5. Select **Set up** from the selector screen.

6. Enter the appropriate trace information on the dialog screen. This information will differ for each protocol.
7. A COMMAND STATUS screen will display the output file names for the trace and setup information.

Fast-Path Command(s)

appletalk debug set {*trace_parameters*}
appn debug set {*trace_parameters*} {*trace_IDs*}
decnet debug set {*trace_level*} {*trace_mask*}
dls debug set {*trace_IDs*}
ip debug set {*trace_log_size*} {*number_trace_files*} {*trace_parameters*}

Collecting Protocol Debug Information

To collect protocol debug information:

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Protocol Debug** on the next menu.
3. Select **Protocol Debug Collection Facility** on the next menu.
4. Select a protocol, Interface, or System from the selector screen. For a protocol, you can choose:
   - AppleTalk
   - APPN
   - DECnet
   - DLSw
   - Frame Relay (FR)
   - IP
   - IPX
   - LAN Bridge (LB)
   - PPP
   - SNMP
   - Source route bridge (SRB)
   - Transparent bridge (TB)
   - Translational bridge (TLB)
   - VINES
   - XNS
   - X.25
5. The next step depends upon your previous selection.

   For AppleTalk, APPN, DECnet, DLSw, and IP:

   a. Select **Collect** from the selector screen.

   b. Select whether to Collect additional system information on the dialog screen. The default is **no**.

   c. Select whether to stop the protocol trace on the dialog screen. The default is **yes**.

   d. Select the type of output file you want generated on the dialog screen. The default is **tar**.

   For frame relay, interface, and PPP:

a. Select a single interface or select all interfaces on the selector screen.

b. Select whether to Collect additional system information on the dialog screen. The default is **no**.

c. Select the type of output file you want generated on the dialog screen. The default is **tar**.

For system:

a. Enter the number of days you want saved in the error log. Any error log entries older than the number of days specified will be purged.

b. Select the type of output file you want generated on the dialog screen. The default is **tar**.

For all other protocols:

a. Select whether to Collect additional system information on the dialog screen. The default is **no**.

b. Select the type of output file you want generated on the dialog screen. The default is **tar**.

6. A COMMAND STATUS screen will display the output.

Fast-Path Command(s)

appletalk debug (collect) {-system} {-notrcstop} [(-tar)|-cat] {*output_file***}**
appn debug (collect) {-system} {-notrcstop} [(-tar)|-cat] {*output_file***}**
bridge debug (collect) [(-srb)|-tbl-tlbl-lb] {-system} [(-tar)|-cat] {*output_file***}**
decnet debug (collect) {-system} {-notrcstop} [(-tar)|-cat] {*output_file***}**
dls debug (collect) {-system} {-notrcstop} [(-tar)|-cat] {*output_file***}**
frame relay debug (collect) {-system} [(-tar)|-cat] {*interface***} {***output_file***}**
interface debug (collect) {-system} [(-tar)|-cat] {*interface***} {***output_file***}**
ip debug (collect) {-system} {-notrcstop} [(-tar)|-cat] {*output_file***}**
ipx debug (collect) {-system} [(-tar)|-cat] {*output_file***}**
ppp debug (collect) {-system} [(-tar)|-cat] {*interface***} {***output_file***}**
snmp debug (collect) {-system} [(-tar)|-cat] {*output_file***}**
system debug (collect) -paging_space [(-tar)|-cat] {*output_file***}**
system debug (collect) [(-tar)|-cat] {*number_days_errlog_clear***} {***output_file***}**
vines debug (collect) {-system} [(-tar)|-cat] {*output_file***}**
xns debug (collect) {-system} [(-tar)|-cat] {*output_file***}**
x25 debug (collect) {-system} [(-tar)|-cat] {*output_file***}**

Files Generated by the Protocol Debug Collection Facility

The Protocol Debug Collection Facility generates several individual files when collecting debug information for a protocol, an interface, or the system. These files appear in the transfer directory while the Protocol Debug Collection Facility assembles the debug information. After the information is assembled, the Protocol Debug Collection Facility creates a single output file using the individual files, then deletes the individual files from the transfer directory.

When setting up debug collection, you can specify the type of output file you want the Protocol Debug Collection Facility to generate. The choices are:

- **tar**–the Protocol Debug Collection Facility generates the output file using the AIX **tar** command. To retrieve the debug information:

1. Transfer the output file to an AIX or UNIX workstation using the binary mode of ftp
2. Restore the individual files using the command: **tar -xvf** *filename*.

- **cat**–the Protocol Debug Collection Facility generates the output file using the AIX cat command. To retrieve the debug information, transfer the output file to any workstation using the ASCII mode of ftp. The output file can be viewed using most workstation editors.

Refer to "Using the File Transfer Protocol" on page 4-67 for information about transferring files with FTP.

AppleTalk

Table 5-2 lists the name and description of each file created for the AppleTalk protocol. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_appletalk.debug`, where *hostname* is the host name of this 6611.

Table 5-2. Protocol Debug File Names - AppleTalk

File Name	Description
hostname.AT.adp.slots.db	6611 adapter list by slot
hostname.AT.adpinfo.db	Specific AppleTalk adapter information
hostname.AT.connections.db	Connection statistics
hostname.AT.framerelay.db	AppleTalk address to DLCI lookup table
hostname.AT.gen.adpinfo.db	General peer-capable adapter information
hostname.AT.if.status.db	Adapter interface status
hostname.AT.ifstat.db	AppleTalk interface information including traffic, connections, routes, statistics, and filters
hostname.AT.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.AT.net.options.db	Network options
hostname.AT.route.db	AppleTalk routes and zones
hostname.AT.setup.db	Output from the AppleTalk debug set command, including the trace parameters used
hostname.AT.sys.route.db	System route table
hostname.AT.trace.db	Messages for stopping AppleTalk trace and renaming the trace output to *hostname*.pd_appletalk.trc

Note:

hostname Host name of the 6611

Table 5-3 on page 5-63 lists the name and description of each file created if you choose to include additional system information.

Table 5-3. Additional System Files - AppleTalk

File Name	Description
hostname.AT.cfg.report.db	Detailed configuration report
hostname.AT.config.sysid.db	System configuration
hostname.AT.err.report.db	Detailed error report
hostname.AT.filesystems.db	File systems
hostname.AT.mem.man.db	Memory management statistics
hostname.AT.page.space.db	System paging space statistics
hostname.AT.proc.stat.db	Process status
hostname.AT.sw.his.db	Software history
hostname.AT.sysmon.db	System monitor trace log
hostname.AT.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

APPN

Table 5-4 lists the name and description of each file created for the APPN protocol. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_appn.debug`, where *hostname* is the host name of this 6611.

Table 5-4. Protocol Debug File Names - APPN

File Name	Description
hostname.APPN.config.db	APPN configuration information
hostname.APPN.dlsconv.db	DLSw conversation list
hostname.APPN.dump.db	Messages for saving old APPN dumps as *hostname*.pd_dump.APPN.d#.old and for dumping APPN into pd_dump.APPN.d# and renaming the dump to *hostname*.APPN.d#.
hostname.APPN.err.report.db	Detailed error report
hostname.APPN.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.APPN.setup.db	Output from the APPN debug set command, including the trace parameters used
hostname.APPN.sys.route.db	System route table
hostname.APPN.sysmon.db	System monitor trace log
hostname.APPN.trace.db	Messages for stopping APPN trace and renaming trace to *hostname*.pd_appn.trc

Note:

hostname Host name of the 6611

Table 5-5 on page 5-64 lists the name and description of each file created if you choose to include additional system information.

Table 5-5. Additional System Files - APPN

File Name	Description
hostname.APPN.cfg.report.db	Detailed configuration report
hostname.APPN.config.sysid.db	System configuration
hostname.APPN.connections.db	Connection statistics
hostname.APPN.filesystems.db	File systems
hostname.APPN.mem.man.db	Memory management statistics
hostname.APPN.page.space.db	System paging space statistics
hostname.APPN.proc.stat.db	Process status
hostname.APPN.sw.his.db	Software history
hostname.APPN.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

DECnet

Table 5-6 lists the name and description of each file created for the DECnet protocol. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_decnet.debug`, where *hostname* is the host name of this 6611.

Table 5-6 (Page 1 of 2). Protocol Debug File Names - DECnet

File Name	Description
hostname.DEC.adp.slots.db	6611 adapter list by slot
hostname.DEC.connections.db	Connection statistics
hostname.DEC.data.struct.db	DECnet routing table structures
hostname.DEC.ethernet.db	DECnet DLCSTAT Ethernet information
hostname.DEC.framerelay.db	DECnet address to DLCI lookup table
hostname.DEC.gen.adpinfo.db	General peer-capable adapter information
hostname.DEC.if.status.db	Adapter interface status
hostname.DEC.ifstat.db	DECnet interface information including traffic, connections, routes, statistics, and filters
hostname.DEC.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.DEC.net.options.db	Network options
hostname.DEC.setup.db	Output from the DECnet debug set command, including the trace parameters used
hostname.DEC.sys.route.db	System route table
hostname.DEC.tokenring.db	DECnet DLCSTAT Token-ring information

Table 5-6 (Page 2 of 2). Protocol Debug File Names - DECnet

File Name	Description
hostname.DEC.trace.db	Messages for stopping DECnet trace and renaming trace to *hostname*.pd_decnet.trc DECnet trace output

Note:

hostname Host name of the 6611

Table 5-7 lists the name and description of each file created if you choose to include additional system information.

Table 5-7. Additional System Files - DECnet

File Name	Description
hostname.DEC.cfg.report.db	Detailed configuration report
hostname.DEC.config.sysid.db	System configuration
hostname.DEC.err.report.db	Detailed error report
hostname.DEC.filesystems.db	File systems
hostname.DEC.mem.man.db	Memory management statistics
hostname.DEC.page.space.db	System paging space statistics
hostname.DEC.proc.stat.db	Process status
hostname.DEC.sw.his.db	Software history
hostname.DEC.sysmon.db	System monitor trace log
hostname.DEC.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

DLSw

Table 5-8 lists the name and description of each file created for the DLSw protocol. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_dls.debug`, where *hostname* is the host name of this 6611.

Table 5-8 (Page 1 of 2). Protocol Debug File Names - DLSw

File Name	Description
hostname.DLSW.conv.db	DLSw conversation list
hostname.DLSW.database.db	DLSw database summary
hostname.DLSW.dlsinfo.db	DLSw information file
hostname.DLSW.dump.db	Messages for saving old DLSw dumps as *hostname*.pd_dump.DLSW.d#.old and for dumping DLSw into pd_dump.APPN.d# and renaming the dump to *hostname*.DLSW.d#
hostname.DLSW.err.report.db	Detailed error report
hostname.DLSW.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.DLSW.msgbuf.db	DLSw message buffers

Table 5-8 (Page 2 of 2). Protocol Debug File Names - DLSw

File Name	Description
hostname.DLSW.msgque.db	DLSw message queues
hostname.DLSW.partner.db	DLSw partners
hostname.DLSW.procinfo.db	DLSw process information
hostname.DLSW.setup.db	Output from the DLSw debug set command, including the trace parameters used
hostname.DLSW.sys.route.db	System route table
hostname.DLSW.sysmon.db	System monitor trace log
hostname.DLSW.trace.db	Messages for stopping DLSw trace and renaming trace to *hostname*.DLSW.trc

Note:

hostname Host name of the 6611

Table 5-9 lists the name and description of each file created if you choose to include additional system information.

Table 5-9. Additional System Files - DLSw

File Name	Description
hostname.DLSW.cfg.report.db	Detailed configuration report
hostname.DLSW.config.sysid.db	System configuration
hostname.DLSW.connections.db	Connection statistics
hostname.DLSW.filesystems.db	File systems
hostname.DLSW.mem.man.db	Memory management statistics
hostname.DLSW.page.space.db	System paging space statistics
hostname.DLSW.proc.stat.db	Process status
hostname.DLSW.sw.his.db	Software history
hostname.DLSW.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

Frame Relay

Table 5-10 lists the name and description of each file created for the frame relay protocol. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_fr.debug` (where *hostname* is the host name of this 6611), or in `pd_hostname_fr.intf.debug` (where *intf* is the interface chosen).

Table 5-10 (Page 1 of 2). Protocol Debug File Names - Frame Relay

File Name	Description
hostname.FR.adp.slots.db	6611 adapter list by slot
hostname.FR.adpinfo.db	General peer-capable adapter information for frame-relay adapters
hostname.FR.appletalk.db	AppleTalk address to DLCI lookup table
hostname.FR.arpstat.db	ARP statistics

Table 5-10 (Page 2 of 2). Protocol Debug File Names - Frame Relay

File Name	Description
hostname.FR.bridge.db	Bridge address to DLCI lookup table
hostname.FR.connections.db	Connection statistics
hostname.FR.decnet.db	DECnet address to DLCI lookup table
hostname.FR.dropstat.db	Drop statistics
hostname.FR.error.db	Frame-relay error information
hostname.FR.flags.db	Other statistics and flags
hostname.FR.freebuf.db	Free buffer statistics
hostname.FR.ifstat.db	Interface packet traffic for frame-relay adapter
hostname.FR.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.FR.ip.db	IP address to DLCI lookup table
hostname.FR.ipx.db	IPX address to DLCI lookup table
hostname.FR.linkstat.db	Link statistics
hostname.FR.mib.db	Frame-relay MIB information
hostname.FR.mystat.db	My statistics
hostname.FR.numstat.db	Num statistics
hostname.FR.sys.route.db	System route table
hostname.FR.xns.db	XNS address to DLCI lookup table

Note:

hostname Host name of the 6611

Table 5-11 lists the name and description of each file created if you choose to include additional system information.

Table 5-11. Additional System Files - Frame Relay

File Name	Description
hostname.FR.cfg.report.db	Detailed configuration report
hostname.FR.config.sysid.db	System configuration
hostname.FR.err.report.db	Detailed error report
hostname.FR.filesystems.db	File systems
hostname.FR.mem.man.db	Memory management statistics
hostname.FR.page.space.db	System paging space statistics
hostname.FR.proc.stat.db	Process status
hostname.FR.sw.his.db	Software history
hostname.FR.sysmon.db	System monitor trace log
hostname.FR.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

Interface

Table 5-12 lists the name and description of each file created for interfaces. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_if.debug`, where *hostname* is the host name of this 6611.

Table 5-12. Protocol Debug File Names - Interface

File Name	Description
hostname.IF.adp.slots.db	6611 adapter list by slot
hostname.IF.adpinfo.db	General adapter information
hostname.IF.connections.db	Connection statistics
hostname.IF.dump.db	Messages for dumping the interfaces and the interface dump
hostname.IF.ifstat.db	Interface information including traffic, connections, routes, statistics, and filters
hostname.IF.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.IF.sys.route.db	System route table

Note:

hostname Host name of the 6611

Table 5-13 lists the name and description of each file created if you choose to include additional system information.

Table 5-13. Additional System Files - Interface

File Name	Description
hostname.IF.cfg.report.db	Detailed configuration report
hostname.IF.config.sysid.db	System configuration
hostname.IF.err.report.db	Detailed error report
hostname.IF.filesystems.db	File systems
hostname.IF.mem.man.db	Memory management statistics
hostname.IF.page.space.db	System paging space statistics
hostname.IF.proc.stat.db	Process status
hostname.IF.sw.his.db	Software history
hostname.IF.sysmon.db	System monitor trace log
hostname.IF.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

IP

Table 5-14 on page 5-69 lists the name and description of each file created for IP. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_ip.debug`, where *hostname* is the host name of this 6611.

Table 5-14. Protocol Debug File Names - IP

File Name	Description
hostname.IP.adp.slots.db	6611 adapter list by slot
hostname.IP.connections.db	Connection statistics
hostname.IP.dump.db	Messages for dumping IP into /tmp/gated_dump and renaming dump to *hostname*.IP.dump
hostname.IP.framerelay.db	IP address to DLCI lookup table
hostname.IP.gen.adpinfo.db	General peer-capable adapter information
hostname.IP.if.status.db	Adapter interface status
hostname.IP.ifstat.db	IP interface information including traffic, connections, routes, statistics, and filters
hostname.IP.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.IP.net.options.db	Network options
hostname.IP.ospf.db	IP OSPF information
hostname.IP.setup.db	Output from the IP debug set command, including the trace parameters used
hostname.IP.sys.route.db	System route table
hostname.IP.sysstat.db	IP system statistics
hostname.IP.trace.db	Messages for stopping IP trace and renaming trace to *hostname*.pd_ip.trc IP trace output

Note:

hostname Host name of the 6611

Table 5-15 lists the name and description of each file created if you choose to include additional system information.

Table 5-15. Additional System Files - IP

File Name	Description
hostname.IP.cfg.report.db	Detailed configuration report
hostname.IP.config.sysid.db	System configuration
hostname.IP.err.report.db	Detailed error report
hostname.IP.filesystems.db	File systems
hostname.IP.mem.man.db	Memory management statistics
hostname.IP.page.space.db	System paging space statistics
hostname.IP.proc.stat.db	Process status
hostname.IP.sw.his.db	Software history
hostname.IP.sysmon.db	System monitor trace log
hostname.IP.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

IPX

Table 5-16 lists the name and description of each file created for the IPX protocol. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_ipx.debug`, where *hostname* is the host name of this 6611.

Table 5-16. Protocol Debug File Names - IPX

File Name	Description
hostname.IPX.adp.slots.db	6611 adapter list by slot
hostname.IPX.config.db	IPX configuration information
hostname.IPX.connections.db	Connection statistics
hostname.IPX.dump.db	Messages for dumping IPX and the IPX dump
hostname.IPX.framerelay.db	IPX address to DLCI lookup table
hostname.IPX.gen.adpinfo.db	General peer-capable adapter information
hostname.IPX.if.status.db	Adapter interface status
hostname.IPX.ifstat.db	IPX interface information including traffic, connections, routes, statistics, and filters
hostname.IPX.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.IPX.net.options.db	Network options
hostname.IPX.swinfo.db	IPX software information
hostname.IPX.sys.route.db	System route table
hostname.IPX.sysstat.db	IPX system statistics
hostname.IPX.trace.db	Messages for stopping IPX trace and renaming trace to *hostname*.pd_ipx.trc IPX trace output

Note:

hostname Host name of the 6611

Table 5-17 lists the name and description of each file created if you choose to include additional system information.

Table 5-17 (Page 1 of 2). Additional System Files - IPX

File Name	Description
hostname.IPX.cfg.report.db	Detailed configuration report
hostname.IPX.config.sysid.db	System configuration
hostname.IPX.err.report.db	Detailed error report
hostname.IPX.filesystems.db	File systems
hostname.IPX.mem.man.db	Memory management statistics
hostname.IPX.page.space.db	System paging space statistics
hostname.IPX.proc.stat.db	Process status
hostname.IPX.sw.his.db	Software history
hostname.IPX.sysmon.db	System monitor trace log

Table 5-17 (Page 2 of 2). Additional System Files - IPX

File Name	Description
hostname.IPX.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

LAN Bridge

Table 5-18 lists the name and description of each file created for the LAN Bridge protocol. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_lb.debug`, where *hostname* is the host name of this 6611.

Table 5-18. Protocol Debug File Names - LAN Bridge

File Name	Description
hostname.LB.adp.slots.db	6611 adapter list by slot
hostname.LB.connections.db	Connection statistics
hostname.LB.framerelay.db	Bridge address to DLCI lookup table
hostname.LB.if.status.db	Adapter interface status
hostname.LB.ifstat.db	LAN Bridge interface information including traffic, connections, routes, statistics, and filters
hostname.LB.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.LB.ipcs.db	LAN bridgie kernet information
hostname.LB.log.db	LAN bridging log information
hostname.LB.procinfo.db	LAN bridging process information
hostname.LB.ser.adpinfo.db	General adapter information for serial adapters
hostname.LB.sys.route.db	System route table

Note:

hostname Host name of the 6611

Table 5-19 lists the name and description of each file created if you choose to include additional system information.

Table 5-19 (Page 1 of 2). Additional System Files - LAN Bridge

File Name	Description
hostname.LB.cfg.report.db	Detailed configuration report
hostname.LB.config.sysid.db	System configuration
hostname.LB.err.report.db	Detailed error report
hostname.LB.filesystems.db	File systems
hostname.LB.mem.man.db	Memory management statistics
hostname.LB.page.space.db	System paging space statistics
hostname.LB.proc.stat.db	Process status

Table 5-19 (Page 2 of 2). Additional System Files - LAN Bridge

File Name	Description
hostname.LB.sw.his.db	Software history
hostname.LB.sysmon.db	System monitor trace log
hostname.LB.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

PPP

Table 5-20 lists the name and description of each file created for PPP. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_ppp.debug` (where *hostname* is the host name of this 6611), or in `pd_hostname_ppp.intf.debug` (where *intf* is the interface chosen).

Table 5-20. Protocol Debug File Names - PPP

File Name	Description
hostname.PPP.adp.slots.db	6611 adapter list by slot
hostname.PPP.adpinfo.db	PPP serial adapter data structures
hostname.PPP.connections.db	Connection statistics
hostname.PPP.gen.adpinfo.db	General peer-capable adapter information
hostname.PPP.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.PPP.procinfo.db	PPP process information
hostname.PPP.readwrite.db	Serial adapter read and write addresses
hostname.PPP.swinfo.db	PPP software information
hostname.PPP.sys.route.db	System route table

Note:

hostname Host name of the 6611

Table 5-21 lists the name and description of each file created if you choose to include additional system information.

Table 5-21 (Page 1 of 2). Additional System Files - PPP

File Name	Description
hostname.PPP.cfg.report.db	Detailed configuration report
hostname.PPP.config.sysid.db	System configuration
hostname.PPP.err.report.db	Detailed error report
hostname.PPP.filesystems.db	File systems
hostname.PPP.mem.man.db	Memory management statistics
hostname.PPP.page.space.db	System paging space statistics
hostname.PPP.proc.stat.db	Process status
hostname.PPP.sw.his.db	Software history
hostname.PPP.sysmon.db	System monitor trace log

Table 5-21 (Page 2 of 2). Additional System Files - PPP

File Name	Description
hostname.PPP.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

SNMP

Table 5-22 lists the name and description of each file created for the SNMP protocol. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_snmp.debug`, where *hostname* is the host name of this 6611.

Table 5-22. Protocol Debug File Names - SNMP

File Name	Description
hostname.SNMP.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.SNMP.log.db	SNMP trace logs
hostname.SNMP.netstat.db	SMUX network statistics
hostname.SNMP.procinfo.db	SNMP process information
hostname.SNMP.sys.route.db	System route table
hostname.SNMP.sysmon.db	System monitor trace log

Note:

hostname Host name of the 6611

Table 5-23 lists the name and description of each file created if you choose to include additional system information.

Table 5-23. Additional System Files - SNMP

File Name	Description
hostname.SNMP.cfg.report.db	Detailed configuration report
hostname.SNMP.config.sysid.db	System configuration
hostname.SNMP.connections.db	Connection statistics
hostname.SNMP.err.report.db	Detailed error report
hostname.SNMP.filesystems.db	File systems
hostname.SNMP.mem.man.db	Memory management statistics
hostname.SNMP.page.space.db	System paging space statistics
hostname.SNMP.proc.stat.db	Process status
hostname.SNMP.sw.his.db	Software history
hostname.SNMP.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

Source Route Bridge

Table 5-24 lists the name and description of each file created for the source route bridge protocol. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_srb.debug`, where *hostname* is the host name of this 6611.

Table 5-24. Protocol Debug File Names - Source Route Bridge

File Name	Description
hostname.SRB.adp.slots.db	6611 adapter list by slot
hostname.SRB.connections.db	Connection statistics
hostname.SRB.framerelay.db	Bridge address to DLCI lookup table
hostname.SRB.if.status.db	Adapter interface status
hostname.SRB.ifstat.db	Source route bridge interface information including traffic, connections, routes, statistics, and filters
hostname.SRB.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.SRB.log.db	Source route bridge log information
hostname.SRB.mib.db	Source route bridge MIB information
hostname.SRB.procinfo.db	Source route bridge process information
hostname.SRB.ser.adpinfo.db	General adapter information for serial adapters
hostname.SRB.sys.route.db	System route table
hostname.SRB.tr.adpinfo.db	General adapter information for token-ring network 16/4 adapters

Note:

hostname Host name of the 6611

Table 5-25 lists the name and description of each file created if you choose to include additional system information.

Table 5-25 (Page 1 of 2). Additional System Files - Source Route Bridge

File Name	Description
hostname.SRB.cfg.report.db	Detailed configuration report
hostname.SRB.config.sysid.db	System configuration
hostname.SRB.err.report.db	Detailed error report
hostname.SRB.filesystems.db	File systems
hostname.SRB.mem.man.db	Memory management statistics
hostname.SRB.page.space.db	System paging space statistics
hostname.SRB.proc.stat.db	Process status
hostname.SRB.sw.his.db	Software history
hostname.SRB.sysmon.db	System monitor trace log

Table 5-25 (Page 2 of 2). Additional System Files - Source Route Bridge

File Name	Description
hostname.SRB.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

System

Table 5-26 lists the name and description of each file created for the system debug commands. After collecting the necessary debug information, the files are compressed and placed in an output file. If you use the **system debug collect -paging_space** commmand, the output is placed in `pd_hostname_pagingspace.debug`; otherwise, the output is placed in `pd_hostname_system.debug`. *hostname* is the host name of this 6611.

Table 5-26. Protocol Debug File Names - System

File Name	Description
hostname.SYS.cfg.report.db	Detailed configuration report
hostname.SYS.config.sysid.db	System configuration
hostname.SYS.connections.db	Connection statistics
hostname.SYS.err.report.db	Detailed error report
hostname.SYS.filesystems.db	File systems
hostname.SYS.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.SYS.iostat.db	Input or Output statistics
hostname.SYS.mem.man.db	Memory management statistics
hostname.SYS.net.options.db	Network options
hostname.SYS.page.space.db	System paging space statistics
hostname.SYS.proc.stat.db	Process status
hostname.SYS.processes.db	Process list
hostname.SYS.socket.db	Socket information
hostname.SYS.sys.proto.stat.db	System protocol statistics
hostname.SYS.sys.route.db	System route table
hostname.SYS.sysmon.db	System monitor trace log
hostname.SYS.trans.dir.db	Listing of transfer directory
hostname.SYS.vmstat.db	Virtual memory statistics

Note:

hostname Host name of the 6611

Translational Bridge

Table 5-27 on page 5-76 lists the name and description of each file created for the translational bridge protocol. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_tlb.debug`, where *hostname* is the host name of this 6611.

Table 5-27. Protocol Debug File Names - Translational Bridge

File Name	Description
hostname.TLB.adp.slots.db	6611 adapter list by slot
hostname.TLB.connections.db	Connection statistics
hostname.TLB.en.adpinfo.db	General adapter information for Ethernet adapters
hostname.TLB.en.ifstat.db	Translational bridge Ethernet interface information including traffic, connections, routes, statistics, and filters
hostname.TLB.framerelay.db	Bridge address to DLCI lookup table
hostname.TLB.if.status.db	Adapter interface status
hostname.TLB.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.TLB.log.db	Translational bridge log information
hostname.TLB.mib.db	Translational bridge MIB information
hostname.TLB.procinfo.db	Translational bridge process information
hostname.TLB.ser.adpinfo.db	General adapter information for serial adapters
hostname.TLB.ser.ifstat.db	Translational bridge serial interface information including traffic, connections, routes, statistics, and filters
hostname.TLB.sys.route.db	System route table
hostname.TLB.tr.adpinfo.db	General adapter information for &trad.s
hostname.TLB.tr.ifstat.db	Translational bridge token-ring interface information including traffic, connections, routes, statistics, and filters

Note:

hostname Host name of the 6611

Table 5-28 lists the name and description of each file created if you choose to include additional system information.

Table 5-28 (Page 1 of 2). Additional System Files - Translational Bridge

File Name	Description
hostname.TLB.cfg.report.db	Detailed configuration report
hostname.TLB.config.sysid.db	System configuration
hostname.TLB.err.report.db	Detailed error report
hostname.TLB.filesystems.db	File systems
hostname.TLB.mem.man.db	Memory management statistics
hostname.TLB.page.space.db	System paging space statistics
hostname.TLB.proc.stat.db	Process status
hostname.TLB.sw.his.db	Software history
hostname.TLB.sysmon.db	System monitor trace log

Table 5-28 (Page 2 of 2). Additional System Files - Translational Bridge

File Name	Description
hostname.TLB.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

Transparent Bridge

Table 5-29 lists the name and description of each file created for the transparent bridge protocol. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_tb.debug`, where *hostname* is the host name of this 6611.

Table 5-29. Protocol Debug File Names - Transparent Bridge

File Name	Description
hostname.TB.adp.slots.db	6611 adapter list by slot
hostname.TB.connections.db	Connection statistics
hostname.TB.en.adpinfo.db	General adapter information for Ethernet adapters
hostname.TB.framerelay.db	Bridge address to DLCI lookup table
hostname.TB.if.status.db	Adapter interface status
hostname.TB.ifstat.db	Transparent bridge interface information including traffic, connections, routes, statistics, and filters
hostname.TB.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.TB.log.db	Transparent bridge log information
hostname.TB.mib.db	Transparent bridge MIB information
hostname.TB.procinfo.db	Transparent bridge process information
hostname.TB.ser.adpinfo.db	General adapter information for serial adapters
hostname.TB.sys.route.db	System route table

Note:

hostname Host name of the 6611

Table 5-30 lists the name and description of each file created if you choose to include additional system information.

Table 5-30 (Page 1 of 2). Additional System Files - Transparent Bridge

File Name	Description
hostname.TB.cfg.report.db	Detailed configuration report
hostname.TB.config.sysid.db	System configuration
hostname.TB.err.report.db	Detailed error report
hostname.TB.filesystems.db	File systems
hostname.TB.mem.man.db	Memory management statistics

Table 5-30 (Page 2 of 2). Additional System Files - Transparent Bridge

File Name	Description
hostname.TB.page.space.db	System paging space statistics
hostname.TB.proc.stat.db	Process status
hostname.TB.sw.his.db	Software history
hostname.TB.sysmon.db	System monitor trace log
hostname.TB.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

VINES

Table 5-31 lists the name and description of each file created for the VINES protocol. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_vines.debug`, where *hostname* is the host name of this 6611.

Table 5-31. Protocol Debug File Names - VINES

File Name	Description
hostname.VINES.adp.slots.db	6611 adapter list by slot
hostname.VINES.arp.db	System ARP table
hostname.VINES.config.db	VINES configuration information
hostname.VINES.connections.db	Connection statistics
hostname.VINES.daemon.db	VINES daemon information
hostname.VINES.dump.db	Messages for dumping VINES and the VINES dump
hostname.VINES.gen.adpinfo.db	General peer-capable adapter information
hostname.VINES.if.status.db	Adapter interface status
hostname.VINES.ifstat.db	VINES interface information including traffic, connections, routes, statistics, and filters
hostname.VINES.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.VINES.net.options.db	Network options
hostname.VINES.swinfo.db	VINES software information
hostname.VINES.sys.route.db	System route table
hostname.VINES.sysstat.db	VINES system statistics
hostname.VINES.trace.db	Messages for stopping VINES trace and renaming trace to *hostname*.pd_vines.trc VINES trace output

Note:

hostname Host name of the 6611

Table 5-32 on page 5-79 lists the name and description of each file created if you choose to include additional system information.

Table 5-32. Additional System Files - VINES

File Name	Description
hostname.VINES.cfg.report.db	Detailed configuration report
hostname.VINES.config.sysid.db	System configuration
hostname.VINES.err.report.db	Detailed error report
hostname.VINES.filesystems.db	File systems
hostname.VINES.mem.man.db	Memory management statistics
hostname.VINES.page.space.db	System paging space statistics
hostname.VINES.proc.stat.db	Process status
hostname.VINES.sw.his.db	Software history
hostname.VINES.sysmon.db	System monitor trace log
hostname.VINES.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

XNS

Table 5-33 lists the name and description of each file created for the XNS protocol. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_xns.debug`, where *hostname* is the host name of this 6611.

Table 5-33. Protocol Debug File Names - XNS

File Name	Description
hostname.XNS.adp.slots.db	6611 adapter list by slot
hostname.XNS.config.db	XNS configuration information
hostname.XNS.connections.db	Connection statistics
hostname.XNS.framerelay.db	XNS address to DLCI lookup table
hostname.XNS.gen.adpinfo.db	General peer-capable adapter information
hostname.XNS.if.status.db	Adapter interface status
hostname.XNS.ifstat.db	XNS interface information including traffic, connections, routes, statistics, and filters
hostname.XNS.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.XNS.net.options.db	Network options
hostname.XNS.swinfo.db	XNS software information
hostname.XNS.sys.route.db	System route table
hostname.XNS.sysstat.db	XNS system statistics
hostname.XNS.trace.db	Messages for stopping XNS trace and renaming trace to *hostname*.pd_xns.trc XNS trace output

Note:

hostname Host name of the 6611

Table 5-34 on page 5-80 lists the name and description of each file created if you choose to include additional system information.

Table 5-34. Additional System Files - XNS

File Name	Description
hostname.XNS.cfg.report.db	Detailed configuration report
hostname.XNS.config.sysid.db	System configuration
hostname.XNS.err.report.db	Detailed error report
hostname.XNS.filesystems.db	File systems
hostname.XNS.mem.man.db	Memory management statistics
hostname.XNS.page.space.db	System paging space statistics
hostname.XNS.proc.stat.db	Process status
hostname.XNS.sw.his.db	Software history
hostname.XNS.sysmon.db	System monitor trace log
hostname.XNS.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

X.25

Table 5-35 lists the name and description of each file created for the X.25 protocol. After collecting the necessary debug information, the files are compressed and placed in `pd_hostname_x25.debug`, where *hostname* is the host name of this 6611.

Table 5-35. Protocol Debug File Names - X.25

File Name	Description
hostname.X25.adp.slots.db	6611 adapter list by slot
hostname.X25.config.sysid.db	System configuration
hostname.X25.connections.db	Connection statistics
hostname.X25.ifstat.db	X.25 adapter interface status
hostname.X25.intro.db	Debug collection creation date, software level, and summary of commands and output files
hostname.X25.log.db	X.25 trace log
hostname.X25.sysmon.db	System monitor trace log

Note:

hostname Host name of the 6611

Table 5-36 lists the name and description of each file created if you choose to include additional system information.

Table 5-36 (Page 1 of 2). Additional System Files - X.25

File Name	Description
hostname.X25.cfg.report.db	Detailed configuration report
hostname.X25.err.report.db	Detailed error report
hostname.X25.filesystems.db	File systems

Table 5-36 (Page 2 of 2). Additional System Files - X.25

File Name	Description
hostname.X25.mem.man.db	Memory management statistics
hostname.X25.page.space.db	System paging space statistics
hostname.X25.proc.stat.db	Process status
hostname.X25.sw.his.db	Software history
hostname.X25.trans.dir.db	Listing of transfer directory

Note:

hostname Host name of the 6611

Concurrent Hardware Diagnostics

Select **Concurrent Hardware Diagnostics** to perform hardware problem determination. Refer to *IBM 6611 Network Processor Maintenance Information* for detailed information about analyzing a suspected hardware problem.

All of the menu items on the Problem Determination menu lead to another menu screen or group of menu screens for the System Manager, except for Concurrent Hardware Diagnostics. When you select **Concurrent Hardware Diagnostics**, control is passed to the Hardware Diagnostics Facility. You are no longer in the System Manager.

Concurrent hardware diagnostics can be run while the system is in operation. They are designed to test as much of the system, or specified resource, as possible without interfering with system operations. These are the only type of diagnostics that can be run from the System Manager. For information about stand-alone diagnostics, refer to the *IBM 6611 Network Processor Maintenance Information*.

To test as much of the system or specified resource as possible without interfering with system operations, it is necessary to limit diagnostic testing. If the resource cannot be totally tested in this mode because the resource is in use by the system, a message is displayed informing you of this. You can stop some of the system to free the resource for more complete testing. You can use the facilities of the System Manager to perform an orderly shutdown of the system and test the resource in stand-alone mode.

Running diagnostics requires one of the following:

- An ASCII terminal or terminal emulator attached directly to the S1 or S2 EIA 232 serial ports.
- An ASCII terminal or terminal emulator attached via a modem to the S1 or S2 EIA 232 serial ports.
- A remote workstation attached through the IP network.

Note: Only a controlling user can run hardware diagnostics.

Running from a Direct-Attached ASCII Terminal

When an ASCII terminal or terminal emulator is attached directly to the S1 or S2 serial port of an operational 6611, a login screen appears. Log in to the 6611 using a controlling user ID and password. Select the correct terminal type when prompted. The System Manager main menu appears.

1. Select **Problem Determination** from the System Manager main menu.
2. Select **Concurrent Hardware Diagnostics** from the next menu.
3. The Diagnostic Operating Instructions screen (refer to Figure 5-47) is displayed. After reading the screen, press **Enter** to continue.

```
LICENSED MATERIALS - PROPERTY OF IBM.
IBM 6611 Network Processor DIAGNOSTICS VERSION 2.0
(C) COPYRIGHTS BY IBM AND BY OTHERS 1982, 1994.
ALL RIGHTS RESERVED.
US GOVERNMENT USERS RESTRICTED RIGHTS -
USE, DUPLICATION OR DISCLOSURE RESTRICTED
BY GSA ADP SCHEDULE CONTRACT WITH IBM CORP.

DIAGNOSTIC OPERATING INSTRUCTIONS


These programs contain diagnostics and service aids for the system. These
procedures should be used whenever problems with the system occur which
have not been corrected by any software application procedures available.
In general, the procedures will run automatically.  However, sometimes you
will be required to select options, inform the system when to continue,
do simple tasks, and exchange diskettes.

Several keys are used to control the procedures:
- The Enter key continues the procedure or performs an action
- The Backspace key allows keying errors to be corrected.
- The cursor keys are used to select an option.

Press the F3 key to exit or press Enter to continue.
```

Figure 5-47. Diagnostic Operating Instructions Screen

4. On the FUNCTION SELECTION screen (refer to Figure 5-48 on page 5-83 for an example), select **Diagnostic Routines**.

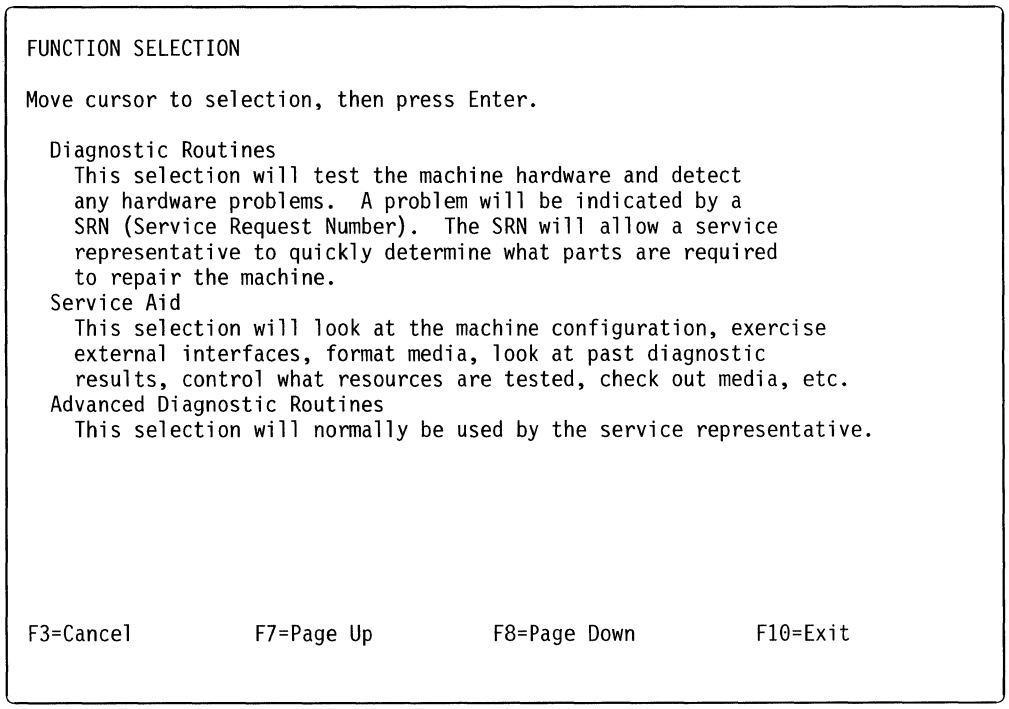


Figure 5-48. FUNCTION SELECTION Screen

5. The DIAGNOSTIC MODE SELECTION screen (refer to Figure 5-49 for an example) is displayed. Select one of the following:
   - **System Verification** to check the correct operation of the system after repairs have been completed.
   - **Problem Determination** to test the system when a problem is suspected. In addition to running the hardware diagnostics, it analyzes the error log to determine whether there have been system errors over the past 24 hours.

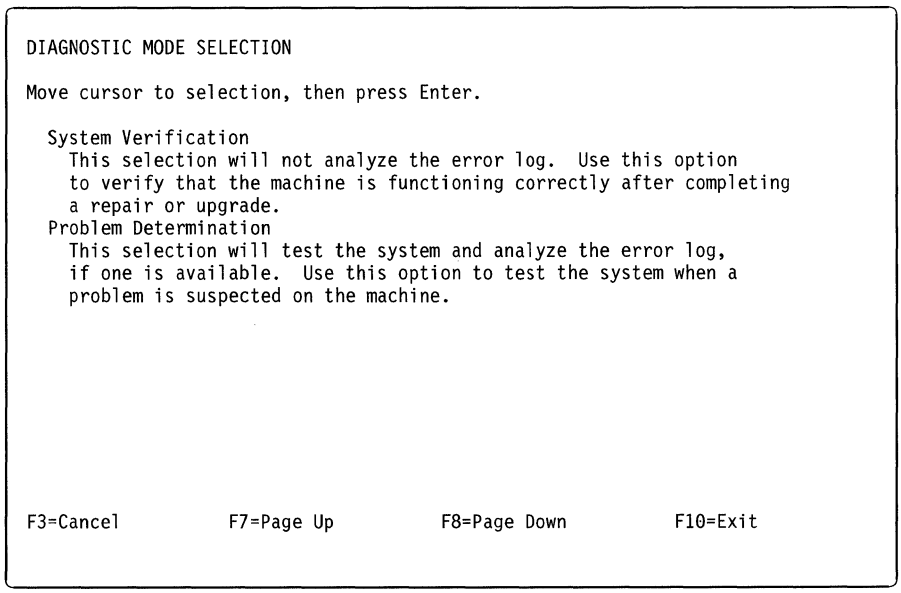


Figure 5-49. Diagnostic Mode Selection Screen

Whichever mode you select, the next menu (DIAGNOSTIC SELECTION) provides a list of the components that can be tested.

6. On the DIAGNOSTIC SELECTION screen (refer to Figure 5-50 for an example), select the resources that you want to test.

```
DIAGNOSTIC SELECTION

An * in front of the resource shows that the test has been performed.

To choose the test, move cursor to selection, then press Enter.

   Base System    00-00          CPU, fpa, memory, I/O planar, op panel
   fd0            00-00-0D-00    Diskette Drive
   tty0           00-00-S1-00    Serial Port
   tty1           00-00-S2-00    Serial Port
   trtya0         00-01          token-ring network 16/4 adapter
   entya0         00-03          Ethernet adapter
   trtya1         00-04          token-ring network 16/4 adapter
   entya1         00-05          Ethernet adapter
   scsi0          00-08          SCSI I/O Controller
   hdisk0         00-08-00-00    355 MB SCSI Disk Drive



F3=Cancel   F7=Page Up        F8=Page Down       F10=Exit
```

Figure 5-50. Example of Diagnostic Selection Screen in the Diagnostics Program

7. Select the component to be tested by moving the cursor up or down using the up-arrow or the down-arrow keys, and press **Enter** when the cursor is at the correct position.

   To exit from any menu to the DIAGNOSTIC OPERATING INSTRUCTIONS screen, press **F3 (Esc+3)**.

Running from a Modem-Attached ASCII Terminal

To run diagnostics testing from a modem-attached terminal, there must be at least one 6611 on the IP network with a modem attached to either its S1 or S2 serial port. This does not have to be the same 6611 needing to be tested. The modem-attached terminal must be an ASCII terminal or terminal emulator with a communication package capable of dialing out to the 6611 with the modem. The telephone number, baud rate, a configured user ID, and password must be known for the 6611 with the modem. The host name or IP address and a controlling user ID and password must be known for the 6611 to be tested.

To test a 6611 without a modem:

1. With the terminal or terminal emulator and its modem set to the same baud rate and settings as the modem attached to the 6611, use the instructions for the modem and terminal to dial into the 6611 as you would a remote host. See "Using a Modem" on page 3-12 for information about using a modem.
2. Log in to the 6611 as a controlling user.
3. Specify the correct terminal type.
4. Select **Operations** on the System Manager main menu.
5. Select **Remote Access to Other Nodes** from the next menu.

6. Select **rlogin - Remote login** from the next menu. You receive a dialog screen. Specify the host name or IP address of the 6611 needing to be tested. Specify a user ID configured at that 6611. Press **Enter** and you are prompted for the password. After entering the password, you are logged in to the 6611 needing to be tested.
7. The rest of the procedure is the same as the numbered steps for a direct-attached ASCII terminal (refer to "Running from a Direct-Attached ASCII Terminal" on page 5-82).

To test a 6611 with a modem:

1. With the terminal or terminal emulator and its modem set to the same baud rate and settings as the modem attached to the 6611, use the instructions for the modem and terminal to dial into the 6611 as you would a remote host. See "Using a Modem" on page 3-12 for information about using a modem.
2. Log in to the 6611 as a controlling user.
3. Specify the correct terminal type.
4. The rest of the procedure is the same as the numbered steps for a direct-attached ASCII terminal (refer to "Running from a Direct-Attached ASCII Terminal" on page 5-82).

Running from a Workstation on the IP Network

From any workstation on the IP network, you can remotely run concurrent diagnostics on a 6611 using a Telnet session. The host name or IP address and a controlling user ID and password must be known for the 6611 to be tested.

1. Type **telnet <hostname or IP address>** to begin the Telnet session.
2. Log in using the controlling user ID and password when prompted. Specify the terminal type, if prompted. See "Using Telnet" on page 3-4 for more details about Telnet sessions.
3. Control is passed to the System Manager, which displays a login screen.
4. The rest of the procedure is the same as the numbered steps for a direct-attached ASCII terminal (refer to "Running from a Direct-Attached ASCII Terminal" on page 5-82).

Chapter 6. Configuration

About This Chapter

This chapter explains how to use the System Manager to configure the 6611.

To enter the System Manager configuration facility, select **Configuration** from the System Manager main menu. The Configuration menu (Figure 6-1) appears.

```
IBM 6611                                                          hostname
                                  Configuration

Move cursor to desired item and press Enter.

  System Manager Configuration Utility
  User IDs and Passwords

  Apply Changes
  Commit Changes
  Reject Uncommitted Changes

  Configuration Reports

  Receive and Apply Configuration
  Send Configuration
  Reinstate a Saved Configuration









F1=Help             F2=Redraw Screen    F3=Return           F4=SysID
F10=Main Menu                           Esc+L=Turn Log On
```

Figure 6-1. Configuration Menu

Refer to the following for information about the individual menu items:

- "System Manager Configuration Utility" on page 6-7
- "User IDs and Passwords" on page 6-17
- "Apply Changes" on page 6-20
- "Commit Changes" on page 6-21
- "Reject Uncommitted Changes" on page 6-22
- "Configuration Reports" on page 6-22
- "Receive and Apply Configuration" on page 6-24
- "Send Configuration" on page 6-26
- "Reinstate a Saved Configuration" on page 6-26

Configuring with the System Manager

You can configure the 6611 using either the Configuration Program or the System Manager. The *primary method* of configuring the 6611 is with the Configuration Program. The System Manager is an alternate method of configuring the 6611, used mainly for backup purposes if the Configuration Program is not available.

Warning: The System Manager method of configuring the 6611 is *not* designed to be the primary method to configure the 6611 because System Manager provides minimal error checking and no dependency checking. If a parameter or set of parameters is dependent on another set of parameters, no checks are made to see that both sets are configured at the same time. Only experienced 6611 configuration experts should use this method for configuring the 6611.

Most of the configuration parameters that exist in the Configuration Program also exist in the dialogs under the Configuration menu.

There are two types of configuration files:

Binary configuration file
This file contains the actual configuration. It is created when a user defines configuration parameters from either the Configuration Program or the System Manager. It is transferred between the Configuration Program and the 6611 using one of the following methods:

- Direct connection over an IP network, when the configuration station is an IBM RISC System/6000 workstation.
- The File Transfer Protocol (FTP), when the configuration station is connected to the same IP network as the 6611.
- The Xmodem Protocol, when the configuration station has a modem and a connection to the 6611 through the public switched network.
- A diskette, when there is no remote method available to transfer the file.

Configuration reports
There are two types of configuration reports:

- Summary
- Detailed

The configuration reports contain descriptive information about the current configuration as it exists at the user ID from which it is viewed.

There are three System Manager configuration tasks:

1. It can be used to update configuration parameters, when the Configuration Program is not available.
2. It is involved in the transfer of the binary configuration file from the Configuration Program to the 6611.
3. It is used to view and transfer the configuration reports.

Note: You must be a controlling user to use the System Manager for most of these configuration tasks.

Configuration Troubleshooting

Errors in the Configuration Program may cause different types of problems. A problem with configuration may appear initially to be a hardware problem because the IBM 6611 will not start or data will not flow through an adapter port. In addition, problems with configuration may not result in an error initially; an error may occur only when specific conditions are encountered or when heavy network traffic occurs.

If you cannot resolve a problem after making a few changes to your configuration, generate a new configuration. Endless changes to a configuration often compound the problem, whereas a new configuration can usually be generated and tested within a few hours.

Updating Configuration Parameters Overview

Only a controlling user can use the System Manager to update configuration parameters.

The System Manager method of configuring the 6611 includes an apply, test, and either commit or reject scenario. The configuration changes are *applied* and *tested* in an actual test environment, and then either *committed* if the changes are approved, or *rejected* if the changes are not approved. Refer to "System Manager Configuration Utility" on page 6-7 for the details of this scenario.

When you begin modifying the system configuration using the System Manager, a local copy of the configuration data is created in the home directory of your user ID. The local copy acts as a work file in which any additional configuration modifications are recorded. The changes in the local copy are not yet part of the system configuration database.

If you want to try out the changes, but want to be able to restore the original configuration, select **Apply Changes** from the Configuration menu. At some time later you can commit these changes. You can make additional modifications to the configuration, and apply these changes in an incremental fashion.

If you want to commit the changes to the configuration database, select **Commit Changes**. You have the choice of committing only the previously applied changes or both the previously applied changes and the unapplied changes made from this controlling user ID. The System Manager then makes the configuration changes described in the work file a permanent part of the current configuration.

If you want to remove uncommitted configuration changes, select **Reject Uncommitted Changes**. You can undo all your configuration changes since the last commit operation (both applied and unapplied changes), or simply discard any changes made since the last apply or commit operation (only unapplied changes).

When you begin to modify the configuration data from a specific user ID and a local copy is made, the System Manager displays the modified version, not the current version. Because the local copy is user-specific, changes that have not been applied or committed can only be seen using that particular user ID. When the changes have been committed or applied, the System Manager returns to showing the current configuration. This may be confusing if multiple users are modifying or importing configuration data.

Warning: Make all System Manager configuration changes from the same controlling user ID to minimize the possibility of overriding another user's configuration changes.

Press **F4 or Esc+4** from any System Manager menu to view the status of your configuration changes. An example of this screen is shown in Figure 6-2 on page 6-5. When viewing this screen, press **Enter** to return to the System Manager menu screen.

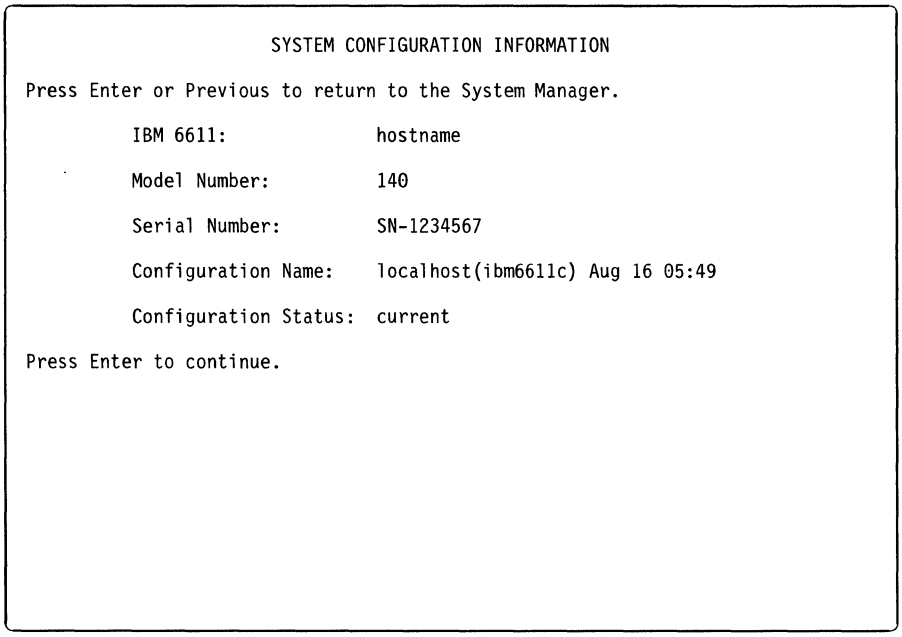


Figure 6-2. System Configuration Information Screen

When the System Manager is used to create the latest applied or committed configuration changes, the configuration name has the following format:

`localhost(userid) Date Time`

The user ID is the name of the user who made the latest applied or committed configuration changes at the date and time specified.

The configuration status presented is from the perspective of the user who pressed **F4 (Esc+4) = SysID** to view this information. The configuration status is either current, applied, unapplied, or partially applied.

- If the status is current, then all configuration changes made from the user ID that you are logged in to have been committed. However, there may be unapplied or applied configuration changes made by a different user. If another user has some applied, but not committed changes, the configuration name will have the local host format. The user ID will contain the name of the user who has applied, but not committed, the last configuration changes. Log in with each controlling user ID and press **F4 (Esc+4) = SysID** to view its configuration status to determine if there are unapplied configuration changes.
- When the status is applied, the user ID that you used to log in has some applied, but not committed configuration changes.
- When the status is unapplied, the user ID that you used to log in has some unapplied configuration changes.
- When the status is partially applied, the user ID that you used to log in has some applied and unapplied configuration changes.

If you want to view only the applied or committed changes, log off and log back in with another user ID. The configuration output produced from the different user ID does not reflect the unapplied changes made from the previous user ID. It reflects all applied changes made from the previous user ID.

Warning: Please make all System Manager configuration changes from the same controlling user ID to minimize the chance of overriding another user's configuration changes.

Performing System Configuration Changes

Select **Configuration** to make changes to the system configuration. This menu is shown in Figure 6-1 on page 6-2. All of the tasks shown on the Configuration menu can also be performed using the Configuration Program.

Configuration Objects

The configuration parameters are separated into logical configuration objects. The configuration parameters associated with any object are related by function and by data structure type. The System Manager groups these configuration objects both by function and by data structure type.

If the configuration object is not adapter dependent, it is considered to be a *box-level parameter*. If the configuration object is adapter dependent, it is considered to be a *port-level parameter*. If the configuration object is a single entity, not containing lists, it is called a *single object*. If the configuration object contains multiple occurrences of the same set of parameters, it is called a *list object*.

There are two sets of System Manager configuration commands. The set you choose depends on the type of configuration object data structure. When selecting the correct set of commands, you choose its high-level functional grouping, either box-level or port-level.

Each configuration object in the System Manager is updated as a complete entity on the same dialog screen.

APPN Configuration Objects

The following box level APPN configuration objects can be accessed through the System Manager only. These objects are intended for use by IBM service personnel.

Table 6-1 (Page 1 of 2). APPN Configuration Objects Accessible Via System Manager

Parameter Information	
Parameter	Constrained threshold
Valid Values	0 to 100 percent. If 0 is specified, APPN uses the default value.
Default Value	70 percent
Description	This parameter sets a threshold at which APPN begins to limit any new usage of shared memory allocated to the node. The percentage specified for this parameter should be less than the percentage specified for the Critical threshold parameter.

Table 6-1 (Page 2 of 2). APPN Configuration Objects Accessible Via System Manager

Parameter Information	
Parameter	Critical threshold
Valid Values	0 to 100 percent. If 0 is specified, APPN uses the default value.
Default Value	85 percent
Description	This parameter sets a threshold at which APPN begins to reduce the existing usage of shared memory allocated to the node. For example, the APPN node will establish a window size of one to restrict the flow of messages from connection partners. The percentage specified for this parameter should be greater than the percentage specified for the Constrained threshold parameter.
Parameter	Retry counter
Valid Values	1 to 255
Default Value	3
Description	This parameter specifies the number of times the APPN network node attempts to restart node processes after a failure has occurred.

System Manager Configuration Utility

Only a controlling user can change the configuration from the System Manager. To change the values of the configuration parameters using the System Manager, perform the following steps after logging in as a controlling user.

To select the System Manager Configuration Utility and start the configuration procedure:

Step 1 Select **Configuration** from the System Manager main menu.

Step 2 Select **System Manager Configuration Utility** from the next menu. The first screen you receive is a warning screen, shown in Figure 6-3. This screen warns you to exit if you are not familiar with the configuration parameters or the System Manager method of configuring the 6611.

Step 3 Press **Enter** to go to the main System Manager Configuration Utility menu. This menu is shown in Figure 6-4 on page 6-8.

```
IBM 6611                                                          hostname
                  System Manager Configuration Utility

Move cursor to desired item and press Enter

  System Manager Configuration Utility

  ┌──────────────────────────────────────────────────────────────┐
       WARNING --- WARNING --- WARNING --- WARNING --- WARNING
    This System Manager Configuration Facility provides little or no
    error checking and no dependency verification.  Use of this
    facility requires detailed knowledge regarding the configuration
    internals.  DO NOT PROCEED unless you have this knowledge.  You
    must be a controlling user to use the System Manager Configuration
    Facility.  DO NOT PROCEED unless you are a controlling user.

             Press F3 (Esc+3) to abort, ENTER to continue.
  └──────────────────────────────────────────────────────────────┘



F1=Help            F2=Redraw Screen    F3=Return          F4=SysID
F10=Main Menu                          Esc+L=Turn Log On
```

Figure 6-3. Warning Screen for the Configuration Menu Item

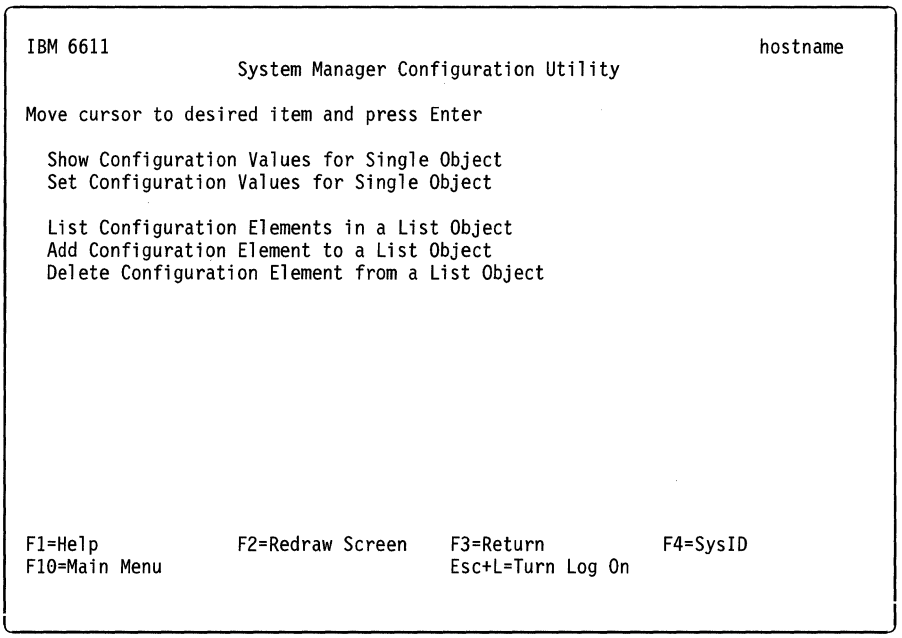


Figure 6-4. System Manager Configuration Utility Menu

Step 4 Determine whether the configuration parameter is a single object or a list object, and whether it is a box-level object or a port-level object. If you select a port-level object, you also need to know the slot number of the adapter and the port number for which the configuration parameter is being changed.

To determine if a parameter is a box-level or port-level object, see the Configuration Worksheets for the protocol with which you are working.

To determine if a parameter is a single or list object, see the port-level and box-level worksheets in the *IBM Multiprotocol Network Program Configuration Guide*. If the table heading says they are **List Item Parameters**, then the parameter is a list object. If the table heading does *not* say that, then the parameter is a single object.

If you are updating a single object, continue with Step 5. If you are updating a list object, go to Step 6.

Step 5 For a single object, select **Set Configuration Values for Single Object** to change the values of its parameters. The Select Parameter Level selector screen appears as shown in Figure 6-5 on page 6-9, requesting you to select the functional level of the configuration object. If you are updating a box-level parameter, go to Step 7. If you are updating a port-level parameter, go to Step 8.

```
                        Select Parameter Level

Move cursor to desired item and press Enter.

  Box Level Parameters
  Port Level Parameters


F1=Help                 F2=Redraw Screen        F3=Return
F5=Top                  F6=Bottom               F7=Page Up
F8=Page Down            F10=Main Menu
```

Figure 6-5. Select Parameter Level Selector Screen

Step 6 For a list object, select **Add Configuration Element to a List Object** to add a new element to the list object. Select **Delete Configuration Element from a List Object** to delete an existing element from the list. A selector screen appears requesting you to select the functional level of the configuration object. Figure 6-5 shows the selector screen for choosing the type of parameter. If you are updating a box-level parameter, continue with Step 7. If you are updating a port-level parameter, go to Step 8.

Step 7 Select **Box Level Parameters**. Go to Step 9.

Step 8 Select **Port Level Parameters**. Two more selector screens appear requesting the slot number and the port number for the adapter you are configuring. Only the slots containing installed adapters are shown. Only the possible port numbers for the chosen adapter are shown. See Figure 6-6 and Figure 6-7 for a sample of these selector screens. Select the correct values based on your hardware configuration.

```
                          Adapter Slot Number

Move cursor to desired item and press Enter.

  Slot 1 :: 6611 X.25
  Slot 2 :: 6611 4-Port SDLC
  Slot 3 :: 6611 2-Port Serial
  Slot 4 :: 6611 Ethernet
  Slot 5 :: 6611 Token-Ring
  Slot 6 :: 6611 Ethernet
  Slot 7 :: 6611 Token-Ring

F1=Help                 F2=Redraw Screen        F3=Return
F5=Top                  F6=Bottom               F7=Page Up
F8=Page Down            F10=Main Menu
```

Figure 6-6. Sample Adapter Slot Number Selector Screen

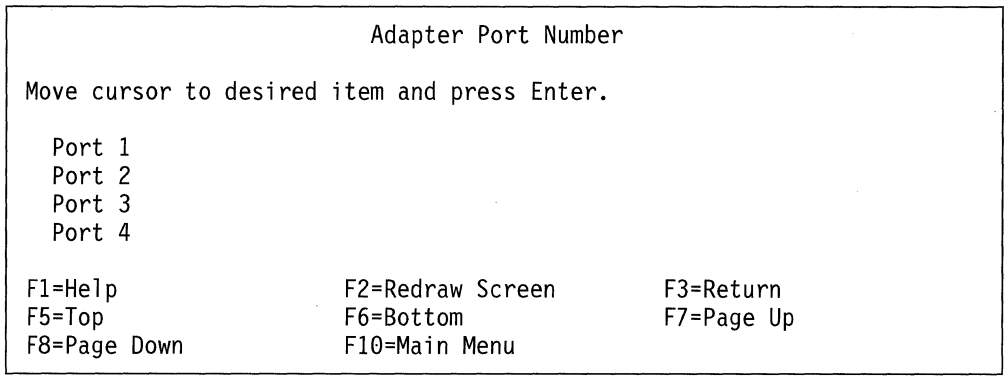


Figure 6-7. Sample Adapter Port Number Selector Screen

Step 9 Select the configuration object from the **Configuration Data Type to Set** selector screen. You have a long list from which to select.

Step 10 A dialog screen appears. The parameters presented depend on the selected object. Press **F1 (Esc+1)** for references to locate details about each parameter. Press **Enter** after changing the parameters.

Step 11 A COMMAND STATUS screen appears. If the process is successful, a `Command: OK` message is displayed. Press **F3 (Esc+3)** until you return to the Configuration menu. If you receive error messages, try to correct the problem, if you can, or call your IBM service personnel for assistance.

Step 12 At this point you may want to view the configuration changes that you have made. If the configuration object is a single object, that is, the changes were made using the Set Configuration Values for Single Object menu item, select **Show Configuration Values for Single Object** to view the changes. Follow the same path through the Parameter Level selector screen(s) to the Configuration Data Type to Show selector screen to view the configuration object.

If the configuration object is a list object, that is, if the changes were made using either the Add Configuration Element to a List Object or Delete Configuration Element from a List Object menu items, select **List Configuration Elements in a List Object** to view the changes. Follow the same path through the selector screen(s) to the Configuration Data Type to List selector screen to view the configuration object.

Step 13 If you agree with the new configuration changes that you made, and you want to make them the new configuration, select **Apply Changes** from the Configuration menu. This selection applies the configuration changes and the changed configuration values become the new configuration. The previous settings of the configuration values are saved.

Warning: If you updated any configuration parameters that cannot be changed dynamically, either the 6611 is restarted or the protocol with the changed configuration is restarted. Wait a few minutes after selecting **Apply Changes** to apply the configuration changes and before executing other 6611 commands, in case the 6611 is restarted.

Step 14 After operating with the changed configuration, you can accept the new values by committing the new configuration or return to the previous configuration by rejecting the new configuration. To commit the configuration changes, select **Commit Changes** from the Configuration

menu. Any new changes to the configuration that have not been applied are also committed. To reject the configuration changes, select **Reject Uncommitted Changes** from the Configuration menu. On the resulting selector screen, you can choose to reject only the unapplied changes or both the unapplied changes and applied changes. When you choose the applied and unapplied changes option, the current configuration is restored to the last committed state. When you choose the only unapplied changes option, the current configuration is not affected. You cannot reject a configuration that has a time delay configured.

Initial Configuration Using a Diskette

To initially configure the 6611 using the Configuration Program:

1. Create the configuration file with the Configuration Program and place it on a diskette. See the *IBM Multiprotocol Network Program Configuration Guide* for instructions about using the Configuration Program.
2. Insert the diskette in the 6611 diskette drive.
3. Set the key mode switch on the front panel in the Normal position and turn the power switch to **On**.

The configuration file is read and the new parameters are used as the current configuration.

Note: To prevent subsequent configurations from this diskette or accidental overwriting of the configuration data, remove the diskette from the diskette drive.

Initial Configuration without Using a Diskette

The System Manager can be used to minimally configure the 6611 so that it can be initially configured from the Configuration Program without using a diskette. There are three methods to transfer the configuration file from the Configuration Program to the 6611 without using a diskette.

1. Direct IP Connection

   This method is available only when using a RISC System/6000 workstation to perform configuration.

2. Modem Attachment

   - A modem must be attached to the configuration workstation and to an 6611 on the network.
   - The configuration workstation must also have a communication package that supports CALLOUT and the Xmodem Protocol.
   - This method could be used with a PS/2* configuration workstation that has a supported communication package.

3. FTP
   - The configuration workstation must be attached to the 6611 through the IP network.
   - This method could be used with a PS/2 configuration workstation that has TCP/IP installed.

One of these methods must be available, if you want to perform initial configuration on the 6611 from the Configuration Program without using a diskette.

Direct IP Connection

Direct IP connection is available only when using a RISC System/6000 configuration workstation attached to the same IP network as the 6611 needing initial configuration. Perform the following steps to configure the 6611 initially over the IP network.

1. The 6611 must be minimally configured for IP. See "Minimal Configuration Using the System Manager" on page 6-15 for details about minimal configuration.
2. See the *IBM Multiprotocol Network Program Configuration Guide* for the details about sending the configuration file from the Configuration Program over the direct connection.

Modem Attachment

When you are using the modem-attachment method to configure the 6611 initially and the modem is attached to the 6611 needing to be configured, minimal configuration is not necessary. Perform the following steps to configure the 6611 initially using the modem connection to send the configuration file.

1. Attach a 2400-bps modem to the EIA 232 S2 serial port on the 6611 (labelled S2 on the Model 120 and the Model 170, and labelled Serial 2 on the Model 140). The S2 serial port is initially configured for 2400-bps modem support. See "Using a Modem" on page 3-12 for details about using a modem.
2. From the configuration station, establish the modem connection to the 6611 using the directions supplied with the communication package.
3. Log in to the 6611 using the default controlling user ID and password:

   Default userid: ibm6611c

   Default password: ibm6611c
4. Prepare the 6611 to receive the configuration file and use it as the new configuration after it has been received:
   a. Select **Configuration** from the System Manager main menu.
   b. Select **Receive and Apply Configuration** from the Configuration menu.
   c. Select **modem** as the import method on the Import method selector screen.

   See "Using the Xmodem Protocol" on page 4-69 for further details about using the Xmodem Protocol to transfer files.
5. Determine the location and name of the configuration file at the configuration workstation. You must determine in which subdirectory the file has been placed. It will be marked as a **.cfg** file. Instruct the configuration workstation to send the configuration file.

If the modem is attached to a different 6611 on the IP network than the 6611 needing to be initially configured, the 6611 has to be minimally configured for an IP connection. Perform the following steps to configure the 6611 initially using the modem connection to send the configuration file.

1. Minimally configure the 6611 using the directions provided in "Minimal Configuration Using the System Manager" on page 6-15.
2. From the configuration workstation, establish a modem connection to the 6611 with a modem that is on the same IP network as the 6611 that you minimally configured. See "Using a Modem" on page 3-12 for details about using a modem. Use the directions supplied with the communication package on the configuration workstation for modem connection.
3. Log in to the 6611 with the modem from the configuration workstation. Establish an rlogin session from the 6611 with the modem to the 6611 needing to be configured. See "Using Remote Login" on page 3-6 for details about using rlogin.
4. Prepare the 6611 that needs to be configured to receive the configuration file and use it as the new configuration when received.
   a. Select **Configuration** from the System Manager main menu.
   b. Select **Receive and Apply Configuration** from the next menu.
   c. Select **modem** as the receive method on the Import method selector screen.

   See "Using the Xmodem Protocol" on page 4-69 for further details about using the Xmodem Protocol to transfer files.
5. Determine the location and name of the configuration file at the configuration workstation. You must determine in which subdirectory the file has been placed. It will be marked as a **.cfg** file. Instruct the configuration workstation to send the configuration file.

FTP Transfer Method

The configuration file may be sent using FTP, if the configuration workstation is on the IP network and it supports FTP. Use the following steps to configure the 6611 initially using FTP to transfer the file.

1. Minimally configure the 6611 using the directions provided in "Minimal Configuration Using the System Manager" on page 6-15.
2. Know the location and file name of the configuration file on the configuration station. In this procedure, the configuration file name is *config*.
3. From the directory that has the configuration file in the configuration station, use the following scenario to place the configuration file in the transfer directory of the 6611 needing to be configured. What you are expected to input from the configuration station is provided under "**Type in**". What you should expect to see displayed on the screen is provided under "**Output displayed**".

   Type in:

   ```
   ftp hostname
   ```

   where hostname is the host name of the 6611 needing to be configured. The IP address can be used in place of the host name to identify the 6611 to which the configuration files is sent.

Output displayed:

```
Connected to hostname.domainname
220 hostname FTP server (Version 4.1 Date) ready.
Name (hostname):
```

Type in:

6611_userid

Output displayed:

```
331 Password required for 6611_userid.
Password:
```

Type in: (Type the password. It will not be displayed.)

Output displayed:

```
230 User 6611_userid logged in.
/transfer is read-write and /static is read-only.
ftp>
```

Type in:

cd /transfer

Output displayed:

```
250 CWD command successful.
ftp>
```

Type in:

binary

Output displayed:

```
200 Type set to I.
ftp>
```

Type in:

put "file_name"

Output displayed:

```
200 PORT command successful.
150 Opening BINARY mode data connection for filename1.
226 Transfer complete.
local: "file_name" remote: "file_name"
13029 bytes sent in 0.07388 seconds (172.2 Kbytes/s)
ftp>
```

Type in:

quit

Output displayed:

```
221 Goodbye.
```

Note: The numbers associated with the FTP messages are standard message numbers for this protocol. They have no significance other than to identify the message.

4. The configuration file is now in the transfer directory of the 6611. Receive the file and use it as the new configuration:

   a. Select **Configuration** from the System Manager main menu.

b. Select **Receive and Apply Configuration** from the next menu.

c. Select **transfer directory** as the import method on the resulting selector screen.

d. A dialog screen appears requesting you to enter the name of the binary configuration file. The default configuration file name is *config*. If this is not the name of the configuration file that you are importing from the transfer directory, press **F4 (Esc+4)** to list the files in the transfer directory and select the configuration file from the list. Optionally, you can type the file name in the entry field. Press **Enter** after you have selected or typed the name.

See "Using the File Transfer Protocol" on page 4-67 for further details about using FTP to transfer files.

Minimal Configuration Using the System Manager

To minimally configure the 6611, you must have either an Ethernet adapter or a token-ring network 16/4 adapter configured for IP. The procedure for minimal configuration can be performed by the IBM service representative when the 6611 is installed. You need to know the slot number and the IP address for the adapter. If a token-ring network 16/4 adapter is used, you also need to know the ring speed. There must be a terminal attached directly to the EIA 232 S1 serial port, that is a supported terminal type or can emulate a supported terminal type. See the *IBM 6611 Network Processor Introduction and Planning Guide* for a list of the supported terminal types.

Step 1 Log in to the 6611. Type user ID **ibm6611c** and password **ibm6611c**. (These are the defaults.) Select the terminal type. See "Logging In to a 6611" on page 3-13 for details about logging in and selecting terminal types.

Step 2 The main menu of the System Manager is displayed. Select **Configuration** from the System Manager main.

Step 3 Select **System Manager Configuration Utility** on the next menu and press **Enter** twice to get to the System Manager Configuration Utility menu and beyond the warning screen.

If you are performing the minimal configuration for an Ethernet adapter, continue with Step 4. If you are performing the minimum configuration for a token-ring network 16/4 adapter, go to Step 5.

Step 4 To configure a Ethernet adapter for IP connection minimally:

1. Select **Set Configuration Values for Single Object** from the Configuration main menu.
2. Select **Port Level Parameters** from the selector screen.
3. Select the slot number of the Ethernet adapter from the Adapter Slot Number selector screen.
4. Select **Port 1** from the Adapter Port Number selector screen.
5. Select **Ethernet Adapter Parameters** from the Configuration Data Type to Set selector screen.

6. A dialog screen appears. Press **Tab** to select **yes** for the Enable interface parameter. Use the defaults of the other parameters. Press **Enter** to update the configuration changes for the Ethernet adapter.
7. A COMMAND STATUS screen is displayed. If the process is successful, a `Command: OK` message displays. Press **F3 (Esc+3)** until you return to the Configuration menu. If you receive error messages, try to correct the problem, or call IBM service personnel for assistance.
8. Go to Step 6.

Step 5 To minimally configure a token-ring network 16/4 adapter for IP connection:

1. Select **Set Configuration Values for Single Object** from the Configuration main menu.
2. Select **Port Level Parameters** from the selector screen.
3. Select the slot number of the token-ring network 16/4 adapter from the Adapter Slot Number selector screen.
4. Select **Port 1** from the Adapter Port Number selector screen.
5. Select **Token-Ring Adapter Parameters** from the Configuration Data Type to Set selector screen.
6. A dialog screen appears. Press **Tab** to select **yes** for the Enable interface parameter. Press **Tab** to select the correct ring speed for the Token ring data rate parameter. You must also specify a valid MAC address (a locally-administered address). Use the defaults for the other parameters. Press **Enter** to update the configuration changes for the token-ring network 16/4 adapter.
7. A COMMAND STATUS screen displays. If the process is successful, a `Command: OK` message displays. Press **F3 (Esc+3)** until you return to the Configuration menu. If you receive error messages, try to correct the problem, or call IBM service personnel for assistance.

Step 6 To configure the correct IP address:

1. Select **Set Configuration Values for Single Object** from the Configuration main menu.
2. Select **Port Level Parameters** from the selector screen.
3. Select the slot number of the adapter you configured from the selector screen.
4. Select **Port 1** from the selector screen.
5. Select **IP Parameters** from the Configuration Data Type to Set selector screen.
6. A dialog screen is displayed. Enter the IP address of the adapter in the IP Address entry field. Enter the address mask of the IP address in the Subnet mask entry field. Press **Tab** to select **yes** for the Enable IP routing on this port parameter. Use the defaults for the other parameters. Press **Enter** to add the configuration changes for the IP address.

7. A command status screen is displayed. If the process is successful, a *Command: OK* message is displayed. Press **F3 (Esc+3)** until you return to the Configuration menu. If you received any error messages, try to correct the problem or call IBM service personnel for assistance.

Step 7 Select **Apply Changes** from the Configuration menu to apply the configuration changes.

Note: These changes are not dynamic. The 6611 is stopped and restarted. Do not execute any other IBM 6611 tasks until the system has been restarted.

When the 6611 is restarted, it is possible for the Configuration Program to either transfer the configuration file directly to the 6611 or to use FTP to transfer the file to the 6611. See "Direct IP Connection" on page 6-12 or "FTP Transfer Method" on page 6-13 for further information about initial configuration using the Configuration Program.

User IDs and Passwords

To log into the 6611 you are required to have a user ID and password. There are two classes of users:

- Controlling
- Viewing

Viewing users can only perform a subset of the operations of the 6611. Refer to "Tasks Restricted to Controlling Users" on page 3-16 for more information.

From the System Manager you can list all the users, add a user, delete a user, and change user passwords. Only a controlling user can change user IDs or passwords. The only exception is the ability of any user to change his or her own password. When adding or deleting system users, the configuration change must be applied or committed before it becomes part of the base configuration. When a user changes his or her own password, the apply is done automatically.

Figure 6-8 on page 6-18 shows the User IDs and Passwords menu.

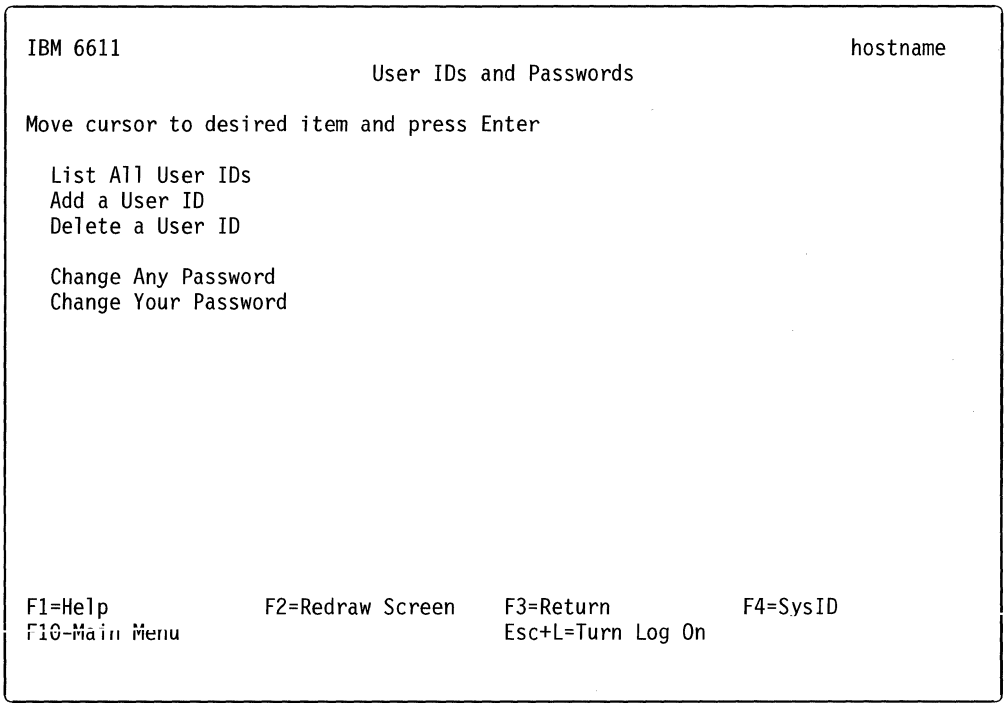


Figure 6-8. User IDs and Passwords Menu

List All User IDs

To list all configured users:

1. Log in using a controlling user ID.
2. Select **Configuration** from the System Manager main menu.
3. Select **User IDs and Passwords** from the next menu.
4. Select **List All User IDs** from the next menu.
5. A COMMAND STATUS screen displays all of the configured user IDs. For example,

```
Controlling users:
ibm6611c

Viewing users:
ibm6611v
```

Fast-Path Command(s)

user (id) list

Add a User ID

To add a controlling or viewing user ID and password:

1. Log in using a controlling user ID.
2. Select **Configuration** from the System Manager main menu.
3. Select **User IDs and Passwords** from the next menu.

4. Select **Add a User ID** from the next menu.
5. Type in the user name on the dialog screen. A user name is a unique string of 8 or fewer alphanumeric lowercase characters.
6. Select the privilege class using the **Tab** on the dialog screen. The privilege class is either viewing or controlling. The default is **viewing**.
7. System Manager prompts you for a password for the new user ID. Enter the password twice. System Manager will not display the password.
8. Press **Enter** to return to the dialog screen.
9. Press **F3 (Esc+3)** twice to return to the Configuration menu.
10. Select **Apply Changes** to apply the configuration change.

Fast-Path Command(s)

user add -controlling *userID passwd*
user add -viewing *userID passwd*

Delete a User ID

To delete a controlling or viewing user ID and password:

1. Log in using a controlling user ID.
2. Select **Configuration** from the System Manager main menu.
3. Select **User IDs and Passwords** from the next menu.
4. Select **Delete a User ID** from the next menu.
5. Select the user ID to be deleted from the selector screen.
6. A COMMAND STATUS screen will display any output.
7. Press **F3 (Esc+3)** until you get to the Configuration menu.
8. Select **Apply Changes** to apply the configuration change.

Fast-Path Command(s)

user id delete *userID*

Change Any Password

To change any user password:

1. Log in using a controlling user ID.
2. Select **Configuration** from the System Manager main menu.
3. Select **Change Any Password** from the next menu.
4. Select a user ID from the selector screen.
5. System Manager prompts you for the new password for the user. Enter the password twice. System Manager does not display the password.
6. Press **Enter** to return to System Manager.
7. Press **F3 (Esc+3)** until you get back to the Configuration menu.

8. Select **Apply Changes** to apply the configuration change.

Fast-Path Command(s)

user password change *userID passwd new_passwd*

Change Your Password

To change your password:

1. Select **Configuration** from the System Manager main menu.
2. Select **User IDs and Passwords** from the next menu.
3. Select **Change Your Password** from the next menu.
4. System Manager prompts you with the message:

   ```
   You have requested to change your password.
   Are you sure you want to do this? (y or n)
   ```

   If you type **n**, you will be told to press **Enter** to return to System Manager.

   If you type **y**, System Manager then prompts you for your old and new password. Enter the old password once and the new password twice. Neither password is displayed.
5. Press **Enter** to return to System Manager.

Apply Changes

The System Manager method of configuring the 6611 includes an apply, test, and either commit or reject scenario. The configuration changes are *applied* and *tested* in an actual test environment, and then either *committed* if the changes are approved, or *rejected* if the changes are not approved.

Whenever you make a configuration change, the System Manager Configuration Facility updates a local configuration copy which is stored in the home directory of your user ID. The System Manager Configuration Facility adds the configuration changes to the global configuration copy, when you apply the change. The configuration change becomes a part of the running configuration only after you apply it. If you log off your user ID before applying the changes, you have not lost them. The local configuration copy retains the unapplied changes, along with all your applied changes. Applied changes that have not been committed, have a saved backup version associated with them.

Warning: Make all System Manager configuration changes from the same controlling user ID to minimize the chance of overriding another user's configuration changes.

To apply changes to a configuration database using the System Manager:

1. Log in using a controlling user ID.
2. Select **Configuration** on the System Manager main menu.
3. Select **Apply Changes** from the next menu.
4. You will see an "Are you sure?" menu from which you can cancel the operation or choose to continue. If you continue, a COMMAND STATUS screen displays the following message:

```
Waiting for acknowledgment from config daemon ...  done.
Command completed successfully
```

Fast-Path Command(s)

config apply

Note: Most configuration changes are not done dynamically. The 6611 is stopped and restarted. Do not execute any other 6611 tasks until the system has been restarted.

Commit Changes

The System Manager Configuration Facility deletes the local backup copy of the configuration when the configuration is committed. You cannot reject a committed configuration change. If you commit your configuration changes, you will not be able to return to the previous configuration, unless you manually undo each change you made. You have the choice of committing only your applied changes or both your applied and unapplied changes.

To commit changes to a configuration database using the System Manager:

1. Log in using a controlling user ID.
2. Select **Configuration** on the System Manager main menu.
3. Select **Commit Changes** from the next menu.
4. On the selector screen, select **only applied changes** to commit only the applied changes. Select **applied and unapplied changes** to commit both the applied and unapplied changes.
5. You will see an "Are you sure?" menu from which you can cancel the operation or choose to continue. If you continue, a COMMAND STATUS screen displays the message:

```
Waiting for acknowledgment from config daemon ...  done.
Command completed successfully
```

Fast-Path Command(s)

config commit -applied
config commit -both

Note: Most configuration changes are not done dynamically. The 6611 is stopped and restarted. Do not execute any other 6611 tasks until the system has been restarted.

Reject Uncommitted Changes

When you issue a reject, the System Manager Configuration Facility removes the configuration changes you choose to reject. You have the choice of rejecting only your unapplied changes or both your applied and unapplied changes. The unapplied changes are removed from your local copy of the configuration and the applied changes are removed from the local copy and the global copy of the configuration. The Configuration Facility replaces the local copy of the configuration with the local backup copy.

To cancel uncommitted changes to a configuration database using the System Manager:

1. Log in using a controlling user ID.
2. Select **Configuration** on the System Manager main menu.
3. Select **Reject Uncommitted Changes** from the next menu.
4. On the selector screen, select **only unapplied changes** to reject only the unapplied changes. Select **applied and unapplied changes** to reject both the applied and unapplied changes.
5. A COMMAND STATUS screen displays the following message:

   ```
   The configuration is rejected.
   ```

Fast-Path Command(s)

config reject -unapplied
config reject -both

Configuration Reports

The configuration report contains information about the current configuration. It is provided in both summary and detailed formats.

These configuration reports can be viewed with the System Manager or transferred from the 6611 for remote viewing.

1. Select **Configuration** on the System Manager main menu.
2. Select **Configuration Reports** from the next menu.
3. On the selector screen, select **summary** or **detailed** as the type of report.
4. A COMMAND STATUS screen displays the report type chosen.

The configuration report generated by a user shows the current running configuration unless the user has made some unapplied configuration changes. The configuration report shows all unapplied configuration changes updated by the user who generates the configuration report. It is possible for different users to produce different configuration reports. It is also possible to produce a configuration report that does not accurately reflect the running configuration. To produce a configuration report that accurately reflects the running configuration, either:

- Apply all configuration changes, or
- Reject all unapplied changes.

Configuration reports may be sent to the System Manager log. First, the log must be turned on (**Esc+L**).

Summary Configuration Report

The summary configuration report contains a few system level configuration parameters, such as host and domain name. The adapter type in each of the slots is listed along with the protocols configured for that adapter.

Fast-Path Command(s)

config view -summary

See Figure 6-9 for an example of a summary configuration report.

```
Brief Configuration Report
IBM 6611 '6611host' on Mon Aug 30 14:09:57 1993

    IBM 6611 Host Name: 6611host
    IBM 6611 Domain name:
    System contact:
    System name:
    System location:

DECnet is enabled
   Local DECnet address (1 - 63 .1 - 1025):2.2
Bridging is enabled
   Bridge number (0-15):  14
IPX is enabled
XNS is enabled
Slot 1 contains a 6611 X.25 Adapter

Slot 2 contains a 6611 Ethernet Adapter

Configuration data for slot 2, port 1
Ethernet is enabled
IP is enabled
    IP Address: 9.66.31.8
    Subnet mask: 255.255.255.0

Slot 4 contains a 6611 Token-Ring Adapter

Configuration data for slot 4, port 1
Token-Ring is enabled
IP is enabled
    IP Address: 9.66.23.8
    Subnet mask: 255.255.255.0
```

Figure 6-9. Summary Configuration Report Example

Detailed Configuration Report

The detailed format contains a listing of the configured configuration objects and the values of each of the parameters.

Fast-Path Command(s)

config view -detail

See Figure 6-10 on page 6-24 for an example of a portion of a detailed configuration report.

```
Detailed Configuration Report
IBM 6611 '6611host' on Mon Jul 13 14:10:21 1992
Configuration: UNNAMED CONFIG

--------------------------------------------------------------------------------
Object: Protocol Independent Parameters
 (slot 255, port 255, id 21500, count 1, size 100)

IBM 6611 Host Name: 6611host
IBM 6611 Domain name:
Enable name resolution by remotename servers: no
Enable time service by remote time servers: no

--------------------------------------------------------------------------------
Object: List of Controlling User Names and Passwords
 (slot 255, port 255, id 22400, count 1, size 20)

User id: ibm6611c
Password: *

--------------------------------------------------------------------------------
Object: List of Viewing User Names and Passwords
 (slot 255, port 255, id 22401, count 1, size 20)

User id: ibm6611v
Password: *

--------------------------------------------------------------------------------
Object: IP Parameters
 (slot 255, port 255, id 21000, count 1, size 35)

Connection Decay Interval (5 - 20 minutes): 10
Status Of All Defined IP Filters: enable

--------------------------------------------------------------------------------
Object: Ethernet Adapter Parameters
 (slot 2, port 1, id 2600, count 1, size 19)

Enable interface: yes
MAC Address: Use card MAC address
Alternate Ethernet MAC Address (Canonical format): 00-00-00-00-00-00
Allow multicasting: no
```

Figure 6-10. Part of a Detailed Configuration Report Example

Receive and Apply Configuration

Besides initial configuration, there are other situations in which it is necessary for the System Manager to either receive the configuration file from the Configuration Program or another 6611. These tasks can be performed from the Configuration menu.

Only a controlling user can receive the binary configuration file and use it as the current configuration.

To receive the configuration file and use it as the current configuration:

1. Select **Configuration** on the System Manager main menu.

2. Select **Receive and Apply Configuration** from the next menu.
3. On the selector screen (Figure 6-11), select the import (or receive) method. Select a method, depending on the location of the configuration file.

```
                              Import method

Move cursor to desired item and press Enter.

  FTP
  modem
  DOS diskette
  transfer directory


F1=Help                 F2=Redraw Screen        F3=Return
F5=Top                  F6=Bottom               F7=Page Up
F8=Page Down            F10=Main Menu
```

Figure 6-11. Import Method Selector Screen

FTP

Select **FTP** if the configuration file is located in the transfer directory of another 6611 and has the file name *config*. You are required to provide the following input on the dialog screen:

- Host name or IP address of the node containing the configuration file
- User ID configured at that node.
- Import method is shown as FTP. It cannot be changed on the dialog screen.

Press **Enter** after typing in the entry fields. You will be prompted for the password of the specified user ID.

modem

Select **modem** (using the Xmodem Protocol) if the configuration file is located at a node that is connected to the 6611 over a modem connection. You will get a message screen stating the system is ready to receive the configuration file.

DOS diskette

Select **DOS diskette** if the configuration file is located on a DOS diskette that is in the diskette drive of the 6611 and has the file name *config*. You will see a command status screen.

transfer directory

Select **transfer directory** if the configuration file is located in the transfer directory of the 6611. It could have been sent to the transfer directory using FTP or Xmodem. The configuration file can have any name. You are required to supply the name of the binary configuration file on the dialog screen. The default configuration file name is *config*. If this is not the name of the configuration file that you are importing from the transfer directory, press **F4 (Esc+4)** to list the files in the transfer directory. Select the correct configuration file from the list. Optionally, you can type the file name in the entry field. Press **Enter** after you have selected or typed the name.

The import method is shown as transfer directory. It cannot be changed on the dialog screen.

4. After selecting the import method and entering any dialog information, the configuration file is added as the current configuration.

Fast-Path Command(s)

files transfer receive via some method
and
config apply

Send Configuration

To send the binary configuration file using the System Manager:

1. Select **Configuration** from the System Manager main menu.
2. Select **Send Configuration** on the next menu.
3. Select an export method from the Export method selector screen.
   - FTP
   - Modem
   - DOS diskette
   - Transfer directory
4. With each of these file transfer methods, the current configuration file is transferred with the name *config*. In addition:
   - Transferring the file with FTP requires you to give the host name or IP address and a user ID at the destination node on the dialog screen. You are prompted for the password for the user ID.
   - Transferring the file to the transfer directory requires you to specify the name of the file in the transfer directory. The default file name is *config*.

Fast-Path Command(s)

files transfer send -ftp *host_name*
files transfer send -modem *file_name*
files transfer send -dos *file_name DOS_file_name*

Reinstate a Saved Configuration

The 6611 saves the last ten configurations that it receives from either the System Manager or the Configuration Program.

To reinstate a saved configuration file and use it as the current configuration:

1. Select **Configuration** from the System Manager main menu.
2. Select **Reinstate a Saved Configuration** on the next menu.
3. On the selector screen, select the configuration file to reinstate. Locate the file you want to reinstate and press **Enter**. Depending on the configuration parameters being changed, the IBM 6611 may be restarted.

Fast-Path Command(s)

config list -cfgfile
config reinstate *cfgfile_number*

Chapter 7. Software Installation and Maintenance

About This Chapter

This chapter describes the Software Installation and Maintenance Facility, which is used to install software updates for the Multiprotocol Network Program. It is also a tracking utility that maintains status and history information about the Multiprotocol Network Program software. There is a multiphase commit and reject capability for software updates. This allows you to test specific software updates on the system for a period of time before you decide whether to make the changes permanent.

This chapter also describes the automatic software installation and maintenance facility that lets you install software changes on one or more 6611s from a single control point.

Figure 7-1 shows the Software Installation and Maintenance menu.

```
IBM 6611                                                          hostname
                  Software Installation and Maintenance

Move cursor to desired item and press Enter.

  Receive Installation File(s)
  List Installation Files
  List All Problems Fixed by Software Updates

  Apply Software Updates
  Clean up After a Failed Installation

  List All Applied but Not Committed Software
  Commit Applied Updates
  Reject Applied Updates

  View Software Vital Product Data



F1=Help            F2=Redraw Screen    F3=Return          F4=SysID
F10=Main Menu                          Esc+L=Turn Log On
```

Figure 7-1. Software Installation and Maintenance Menu

Refer to the following for information about the individual menu items:

Software Updates

A software update provides either:

- A program temporary fix (PTF)
- A new level of code

Software updates are sent as self-contained packages including:

- Update instructions
- Prerequisite and corequisite information
- Authorized program analysis report (APAR) information
- Files containing fixed code

Each software update contains instructions explaining how the update is installed on the system. This includes programs invoked during installation. In addition, information, such as the available storage required to apply the update, is embedded within the update instructions.

Each software update also contains information about all updates that are prerequisite or corequisite. A prerequisite update must be applied to the Multiprotocol Network Program before the installation of another software update that designates it as a prerequisite. Corequisite software updates must be applied during the same installation session. The Software Installation and Maintenance Facility ensures that the software updates are applied correctly using the prerequisite and corequisite information supplied.

The APAR information is also included to tell you the problems that are fixed by the software update. One software update can fix one or more APARs.

Transferring Software Updates

Software updates are sent to you on a diskette or tape. The files need to be sent to the transfer directory of the 6611 before the update can be installed. There are four methods available to move the software update from either a diskette or tape to the transfer directory:

- **Method A:**

  Place the software diskettes or tape in the appropriate drive for the 6611 needing the software change. Copy the files on the diskettes or tape into the transfer directory. Refer to "From a Diskette to an IBM 6611" on page 7-5 for information about importing files from a diskette. Refer to "From Tape to an IBM 6611" on page 7-6 for information about importing files from tape. This is the IBM-recommended method.

- **Method B:**

  Place the software diskettes or tape in the appropriate drive for another 6611 on the same IP network as the 6611 needing the software change. Copy the files on the diskettes or tape into the transfer directory. Refer to "From a Diskette to an IBM 6611" on page 7-5 for information about importing files from a diskette. Refer to "From Tape to an IBM 6611" on page 7-6 for information about importing files from tape.

Use FTP to transfer the software changes to the transfer directory of the 6611 needing the software change. Refer to "From a 6611 to a 6611 Using FTP" on page 7-11 for information about using FTP.

- **Method C:**

  Place each of the software diskettes or the tape in the appropriate drive of an RISC System/6000 workstation on the same IP network as the 6611 needing the software change. Copy the files on the diskettes or the tape to a directory on the RISC System/6000 workstation. Refer to "From Diskette to the RISC System/6000 Workstation" on page 7-7 and "From Tape to an IBM 6611" on page 7-6 for information about importing files to a RISC System/6000 workstation.

  Use FTP to transfer the software changes to the transfer directory in the 6611. Refer to "From a RISC System/6000 Workstation to a 6611 Using FTP" on page 7-8 for information about using FTP.

- **Method D:**

  Place each of the software diskettes or tape in the appropriate drive of a RISC System/6000 workstation that has CALLOUT modem access to the public switch network. Copy them to a directory on the RISC System/6000 workstation. Refer to "From Diskette to the RISC System/6000 Workstation" on page 7-7 and "From Tape to an IBM 6611" on page 7-6 for information about importing files to a RISC System/6000 workstation.

  Establish a connection to a RISC System/6000 workstation or to a 6611 on the same IP network as the 6611 needing the software changes. Transfer the software to the transfer directory of the 6611 using the Xmodem Protocol. Refer to "From a RISC System/6000 Workstation to a 6611 Using Xmodem" on page 7-10 for information about using the Xmodem Protocol.

From a Diskette to an IBM 6611

The software changes are sent to you on a diskette or several diskettes depending on the size of the software installation package. (If you received the software changes on tape, refer to "From Tape to an IBM 6611" on page 7-6 for details.)
Use the following scenario to place the software updates into the transfer directory of the 6611 using the System Manager:

Step 1 Place the software diskette in the diskette drive of the 6611.

Step 2 Select **Software Installation and Maintenance** from the System Manager main menu.

Step 3 Select **Receive Installation File(s)** from the next menu.

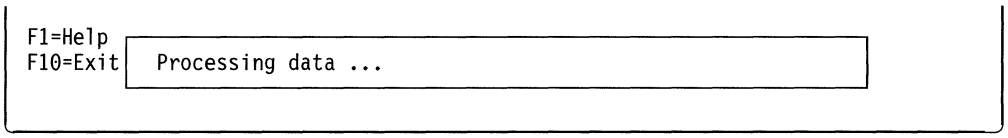
Step 4 Select **diskette** on the Import method selector screen.

Step 5 Select the desired software you want to transfer. You can press **Enter** on the dialog screen to use the default of **all** to indicate all the software is to be transferred.

You may also use **F4 (Esc+4)** to get a list of the software on the diskette. Use **F9 (Esc+9)** to select the software to be transferred. Press **Enter** to record the selections.

Step 6 Follow any messages that appear requesting you to insert the next diskette, if more than one.

If the installation command becomes suspended, press **Ctrl+C** to end the suspension. The bottom of the dialog screen will have the `Processing data ...` message as shown.



A possible cause for the problem is the wrong diskette is in the diskette drive or there is no diskette in the diskette drive. Retry to import the software. You may need to delete the partially imported software from the transfer directory and start again from the beginning. Refer to "Delete Transfer Directory Files" on page 4-43 for details on using System Manager to do this.

From Tape to an IBM 6611

In this instance, the software changes are sent to you on tape. (If you received the software changes on diskette or diskettes, refer to "From a Diskette to an IBM 6611" on page 7-5 for details.) Use the following scenario to place the software updates into the transfer directory of the 6611 using the System Manager:

Step 1 Place the software tape in the tape drive of the 6611.

Step 2 Select **Software Installation and Maintenance** from the System Manager main menu.

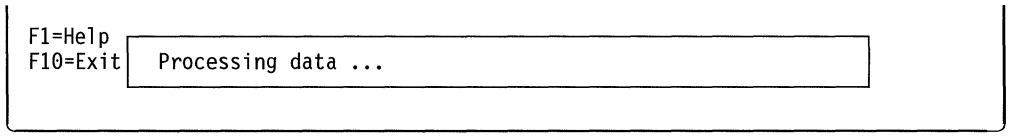
Step 3 Select **Receive Installation File(s)** from the next menu.

Step 4 Select **tape** on the Import method selector screen.

Step 5 Select the desired software you want to transfer. You can press **Enter** on the dialog screen to use the default of **all** to indicate all the software is to be transferred.

You may also use **F4 (Esc+4)** to get a list of the software on the tape. Use **F9 (Esc+9)** to select the software to be transferred. Press **Enter** to record the selections.

If the installation command becomes suspended, press **Ctrl+C** to end the suspension. The bottom of the dialog screen will have the `Processing data ...` message as shown below.



Retry to import the software. You may need to delete the partially imported software from the transfer directory and start again from the beginning. Refer to "Delete Transfer Directory Files" on page 4-43 for details on using System Manager to do this.

From Diskette to the RISC System/6000 Workstation

If you want to perform your software distribution tasks from a central location, you can either import the software from a RISC System/6000 workstation or from another 6611 and distribute the files using FTP. The remote stations must be on the same IP network as the 6611 needing the software change. If you are using another 6611, refer to "From a Diskette to an IBM 6611" on page 7-5 or "From Tape to an IBM 6611" on page 7-6. You can use the following scenario to copy the software diskettes to the */usr* directory of a RISC System/6000 workstation that is used for remote installation (/usr is used as an example. You are not required to use that directory).

Note: These instructions assume that the RISC System/6000 workstation is using AIX Version 3.2, and that you are the root user.

Step 1 Place the software diskette in the diskette drive of the RISC System/6000 workstation on the same IP network as the 6611 needing the software change.

Step 2 Import the software from the diskettes to the directory */usr*, using either the System Management Interface Tool or using a command from the shell prompt:

- Using the System Management Interface Tool:
  1. Select **Software Installation and Maintenance** from the main menu.
  2. Select **Install/Update Software** from the next menu.
  3. Select **Copy Software to Hard Disk for Future Installation** from the next menu.
  4. Press **F4 (Esc+4)** to get a selection list for INPUT device/directory for software.
  5. Select **/dev/fd0** for the diskette drive from the list and press **Enter**.
  6. Change the DIRECTORY for storing software from */usr/sys/inst.images* to */usr* and use the defaults for the other entry fields.
  7. Respond to any messages that appear requesting you to insert the next diskette, if there is more than one diskette.
- Using the command line:
  1. Enter the following command from the shell prompt on the RISC System/6000 workstation:

     bffcreate -qv -d /dev/fd0 -t /usr -X all

  2. Follow any messages that appear requesting you to insert the next diskette, if there is more than one diskette.

From Tape to the RISC System/6000 Workstation

If you want to perform your software distribution tasks from a central location, you can either import the software from a RISC System/6000 workstation or from another 6611 and distribute the files using FTP. The remote stations must be on the same IP network as the 6611 needing the software change. If you are using another 6611, refer to "From a Diskette to an IBM 6611" on page 7-5 or "From Tape to an IBM 6611" on page 7-6. You can use the following scenario to copy

the software tape to the */usr* directory of a RISC System/6000 workstation that is used for remote installation (/usr is used as an example. You are not required to use that directory).

Note: These instructions assume that the RISC System/6000 workstation is using AIX Version 3.2, and that you are the root user.

Step 1 Place the software tape in the tape drive of the RISC System/6000 workstation on the same IP network as the 6611 needing the software change.

Step 2 Import the software from the tape to the directory */usr*, using either the System Management Interface Tool or using a command from the shell prompt:

- Using the System Management Interface Tool:
  1. Select **Software Installation and Maintenance** from the main menu.
  2. Select **Install/Update Software** from the next menu.
  3. Select **Copy Software to Hard Disk for Future Installation** from the next menu.
  4. Press **F4 (Esc+4)** to get a selection list for INPUT device/directory for software.
  5. Select **/dev/rmt#.1** from the list, where # may be a value from 0 on up and indicates which tape drive is being used. Where only one tape drive is being used, for example, the value would be **rmt0.1**.
  6. Press **Enter**.
  7. Change the DIRECTORY for storing software from */usr/sys/inst.images* to */usr* and use the defaults for the other entry fields.
- Using the command line:
  1. Enter the following command from the shell prompt on the RISC System/6000 workstation:

     bffcreate -qv -d /dev/rmt#.1 -t /usr -X all

     where # may be a value from 0 on up and indicates which tape drive is being used. Where only one tape drive is being used, for example, the value would be **rmt0.1**.

From a RISC System/6000 Workstation to a 6611 Using FTP

You can use the following scenario to copy the software installation package from the RISC System/6000 workstation to the 6611 needing the software change using FTP. This scenario assumes that you have previously copied the software installation package to the hard disk of the */usr* directory of the RISC System/6000 workstation using "From Diskette to the RISC System/6000 Workstation" on page 7-7 or "From Tape to the RISC System/6000 Workstation" on page 7-7. (/usr is used as an example. You are not required to use that directory.) The information you are expected to type in is provided under the heading, "**Type in**". The information you should see displayed on the screen is provide under the heading, "**Output displayed**".

Type in:

```
cd /usr
ftp hostname
```

The IP address of the 6611 can be used instead of the host name.

Output displayed:

```
Connected to hostname.
220 hostname FTP server (Version 4.1 Date) ready.
Name (hostname: risc_userid):
```

Type in:

```
6611_userid
```

Output displayed:

```
331 Password required for 6611_userid.
Password:
```

Type in:

(Enter the password. It will not be displayed.)

Output displayed:

```
230 User 6611_userid logged in.
/transfer is read-write and /static is read-only.
ftp>
```

Type in:

```
cd /transfer
```

Output displayed:

```
250 CWD command successful.
ftp>
```

Type in:

```
binary
```

Output displayed:

```
200 Type set to I.
ftp>
```

Type in:

```
mput *
```

Output displayed:

Each file in the directory is displayed and you are given the opportunity to state whether or not you want to send it.

```
mput filename1?
```

Type in:

Type **y** for each file in the software installation package that you want to send to the 6611. Type **n** for those files you do not want to send.

```
y
```

Output displayed:

```
200 PORT command successful.
150 Opening BINARY mode data connection for filename1.
226 Transfer complete.
13029 bytes sent in 0.07388 seconds (172.2 Kbytes/s)
mput filename2?
```

Type in:

```
y
```

Output displayed:

```
200 PORT command successful.
150 Opening BINARY mode data connection for filename2.
226 Transfer complete.
13029 bytes sent in 0.07388 seconds (172.2 Kbytes/s)
ftp>
```

Type in:

```
quit
```

Output displayed:

```
221 Goodbye.
```

Note: The numbers associated with the FTP messages are standard message numbers for this protocol. They have no significance other than to identify the message. Refer to "Using the File Transfer Protocol" on page 4-67 for more information about FTP.

From a RISC System/6000 Workstation to a 6611 Using Xmodem

Use the following scenario to copy the software installation package from the */usr* directory of the RISC System/6000 workstation to the 6611 needing the software change using the Xmodem Protocol (/usr is used as an example. You are not required to use that directory).

1. List the files in the */usr* directory and write down the file names. In this scenario, the file names are filename1, filename2 ....
2. Establish a switched connection from the RISC System/6000 workstation containing the software images in the */usr* directory to any 6611 that is attached to the public switched network through a modem connected to one of its EIA 232 serial ports. Refer to the RISC System/6000 documentation for information about using the Asynchronous Terminal Emulator (ATE) to perform this function.

3. Log in to the 6611 and select the correct terminal type.
4. You are now in the 6611's System Manager. From the System Manager, setup the 6611 to receive the software:
   - Select **Software Installation and Maintenance** from the System Manager main menu.
   - Select **Receive Installation File(s)** from the next menu.
   - Select **modem** from the selector screen.
   - Type **filename1** for "Software to be imported" on the dialog screen.

   You receive the following messages on the System Manager screen:

```
You can return to the local machine and begin file transmission.
The system is ready to receive file filename1.
              Use Ctrl+X to stop xmodem.
```

5. Press **Ctrl+V** at the RISC System/6000 workstation. Instruct the RISC System/6000 workstation to send the file by selecting **Send** or typing the following command on the command line of the Connected Main Menu:

   s /usr/filename1

   The software files are transferred to the transfer directory of the 6611.

Refer to "Using a Modem" on page 3-12 and "Transferring Files between a RISC System/6000 and a 6611" on page 4-70 for more details about using modems and transferring files between a RISC System/6000 workstation and a 6611.

From a 6611 to a 6611 Using FTP

The following scenario can be used to copy the software placed in the transfer directory from one 6611 to another 6611 needing the software change using FTP. This scenario assumes that you have previously copied the software installation package into the transfer directory of the remote 6611 using "From a Diskette to an IBM 6611" on page 7-5 or "From Tape to an IBM 6611" on page 7-6. This process uses the System Manager.

Step 1 Write down the names of the software changes that have previously been placed in the transfer directory of the remote 6611:

- Select **Software Installation and Maintenance** on the System Manager main menu.
- Select **List Installation Files** on the next menu.
- Write down the names of the software changes that you want to transfer to the 6611 needing the software change, and any matching patterns in the names of the software changes. For example, the following two software subcomponents contain the pattern "mpnp".

  ```
  mpnp.obj.01.01.0001.0000
  mpnp.data.01.01.0001.0000
  ```

- Press **F3 (Esc+3)** until you reach the System Manager main menu.

Step 2 Transfer these files to the 6611 needing the software changes using FTP.

1. Select **Operations** on the System Manager main menu.
2. Select **File and Diskette Operations** on the next menu.
3. Select **Send Transfer Directory File** on the next menu.

4. Select **remote host via FTP** as the transfer method from the selector screen.
5. Type the host name or IP address of the 6611 needing the software changes on the dialog item.
6. Press **Enter**. Use the following scenario to transfer the software to the transfer directory of the 6611 needing the software changes. The information you are expected to type in from the remote 6611 is provided under the heading "**Type in**". The output you should expect to see on the screen is provided under the heading "**Output displayed**".

   Type in:

   (From the System Manager screen.)

   ftp hostname

   The IP address of the 6611 can be used in the place of the host name.

   Output displayed:

   ```
   Connected to hostname.
   220 hostname FTP server (Version 4.1 Date) ready.
   Name (hostname: local_userid):
   ```

   Type in:

   6611_userid

   Output displayed:

   ```
   331 Password required for 6611_userid.
   Password:
   ```

   Type in:

   (Enter the password. It will not be displayed.)

   Output displayed:

   ```
   230 User 6611_userid logged in.
   /transfer is read-write and /static is read-only.
   ftp>
   ```

   Type in:

   cd /transfer

   Output displayed:

   ```
   250 CWD command successful.
   ftp>
   ```

   Type in:

   binary

Output displayed:

```
200 Type set to I.
ftp>
```

Type in:

mput *pattern*

where *pattern* is "mpnp" in the example above.

Output displayed:

```
mput filename1?
```

Type in:

y

Output displayed:

```
200 PORT command successful.
150 Opening BINARY mode data connection for filename1.
226 Transfer complete.
13029 bytes sent in 0.07388 seconds (172.2 Kbytes/s)
```

Output displayed:

```
mput filename2?
```

Type in:

y

Output displayed:

```
200 PORT command successful.
150 Opening BINARY mode data connection for filename2.
226 Transfer complete.
53349 bytes sent in 0.09288 seconds (579.8 Kbytes/s)
ftp>
```

Type in:

quit

Output displayed:

```
221 Goodbye.
```

As an alternative to the above scenario, from the receiving 6611 you may either:

- Issue the **software receive -ftp** command with the appropriate parameters, or
- Select the System Manager **Receive Installation File(s)** path from the Software Installation and Maintenance menu.

Fast-Path Command(s)

files transfer send -ftp *host_name*

Installing Software Updates

Software updates are installed from the transfer directory using the Software Installation and Maintenance Facility of the Multiprotocol Network Program. This is a multiphase process that permits the software updates to be tested before making them a permanent part of the Multiprotocol Network Program.

When software updates are first installed, they are applied to the system. The files that are replaced by the software update are saved, in case you want to reject the software update. The applied update becomes part of the running system and can be tested. The files are saved until you commit the software update. When you commit the software update, the saved files are deleted, eliminating the possibility of returning to the previous version. If you reject the applied, but not committed, software update, the saved files are restored and the applied update files are deleted. You cannot reject a software update that has been committed.

Warning: When you commit the software update, the change is permanent.

There are several rules to consider when installing software updates that have dependencies:

- Software updates cannot be applied until their prerequisite software updates have been applied.
- Corequisite software updates must be applied during the same installation step.
- Applied software updates cannot be committed until their prerequisite software updates have been committed.
- Corequisite software updates must be committed during the same installation step.

Storage Space Management for Updates

A software update is also known as a program temporary fix (PTF). PTF installation has been enhanced to determine, at installation time, if there is sufficient storage space available to allow PTF installation to complete. If there is not sufficient space, and the install procedure would fail, all installation activity stops. The advantages of storage space management are:

- PTF processing occurs when it has been determined that sufficient storage space is available for successful completion. This avoids failures because space is exhausted, later service is not possible, and the hard disk might possibly have to be replaced.
- Using the selections available at load and apply time, any PTF package can be broken up into sections that *can* be processed. This is provided no single PTF exceeds the space available. This avoids a deadlock problem in which a package with multiple PTFs is too large to be processed.

  Refer to "Receive Installation File(s)" on page 7-25 for details on using the System Manager to receive files and on how to select updates using **F4 (Esc+4)**. Selecting a specific PTF automatically selects all of its prerequisites.

During PTF installation, the installation process determines for the selected PTFs:

- How much storage space is available.
- The highest-level PTF that can be installed, given the space requirements for it and its prerequisites. In general, a higher-numbered PTF includes lower-numbered PTFs as its prerequisites.

For example, if the list of selected PTFs and their size requirements are:

Table 7-1. Example of PTFs and Size Requirements

PTF Number	Size Requirement	Prerequisite PTF
PTF 5	10 MB	PTF 4
PTF 4	6 MB	PTF 3
PTF 3	8 MB	PTF 2
PTF 2	12 MB	PTF 1
PTF 1	14 MB	

and 36 MB of space is available, then PTF 3 is the highest-level PTF that can successfully be installed. (PTF 3 and its prerequisites, PTF 1 and PTF 2, require a total of 34 MB, which can successfully be contained in the 36 MB space available.)

When all PTFs cannot be applied at once (that is, a highest-level PTF was indicated beyond which DASD space failure occurred), you can take other action. At this point, nothing has been processed. You can free additional space to allow the PTFs to fit, or can make different software installation selections.

When you receive PTFs that fit, and then apply and commit the PTFs, storage space becomes free again. Then the entire installation process can be repeated, picking up where the just-completed process left off. Only the PTFs still waiting to be applied will be processed.

For example, using Table 7-1 again, assume that PTFs 1 through 3 have already been applied. When the PTFs are committed, storage space becomes free and 36 MB is again available. Selecting PTF 5 results in processing both it and its prerequisite, PTF 4. Their storage requirements of 10 MB and 16 MB total 26 MB, which fits in the 36 MB available. These PTFs can now be applied. In effect, the PTF service package has been divided into manageable subsets, avoiding failure of a lengthy installation process.

Possible Messages When Receiving Files in Transfer Directory: When you attempt to receive the files into the transfer directory of the 6611, you are presented with messages indicating:

- If the selected service can be applied
- The highest-level PTF that can successfully be applied

such as:

```
Image mpnp.obj 1.1.1.2.NP00601 requires 5491712 bytes.
Space in /tmp/hold/transfer is sufficient to install mpnp.obj 1.1.1.2.NP00601
```

or:

```
Image mpnp.obj 1.1.1.2.NP00602 requires 6507520 bytes.
bffcreate failed.  It needs 3500 more 1K blocks in /tmp filesystem.
```

In the case of insufficient space, you will be told to make more disk space available and to press **Return** or **Enter** to return to the System Manager.

Based on the messages displayed, you must decide whether or not to continue with the receive operation. If you decide to continue and complete the receive

operation, then the apply operation may begin. Refer to "Apply Software Updates" on page 7-27 for details on using System Manager.

Possible Messages When Applying PTFs: When you decide to apply the PTFs that have been successfully loaded into the transfer directory, you should check first that the:

- /usr
- /tmp
- /root

file systems have at least 2000 1K blocks free in each of them. If this much space is not available, you will see a system message similar to:

```
Installation cannot be started at this time because the
free space available on the disk is not sufficient.
Please press enter to view the detailed information.

(Assuming Enter is pressed, the detailed
message is displayed:)

installp could not complete because there is not enough
space in file system /usr. and it needs 476 more 1024-character
blocks.
The space available in /usr is less than the minimum required
for this operation.
The selected install operation will not be started now.
Press Enter to continue.
```

Note: If you know you have insufficient space in the file systems, or later receive messages stating so, you must contact IBM service. IBM service will make the appropriate adjustments to the file systems.

If there are more than 2000 1K blocks free in each file system, then you will see different messages depending on whether there was sufficient room for the PTFs you selected to apply. For example, if you selected PTFs to apply for which more room is needed, you will still see informational messages describing the processes being performed. Then you will see messages similar to this for each PTF:

```
The number of restored files is 1.

Software product mpnp.obj 01.01.01.02.NP00601 cannot be applied because
the following file systems have insufficient free space.

/ requires 305 more 1K Blocks to complete this operation.
/usr requires 5325 more 1K Blocks to complete this operation.
```

If you select multiple PTFs to be applied and there is room for some, but not all, none will be applied. You will be informed of this. You may receive messages similar to:

```
The number of restored files is 1.

The existing file system spaces are sufficient to apply software
product mpnp.obj 01.01.01.02.NP00601

The number of restored files is 1.

Software product mpnp.obj 01.01.01.02.NP00602 cannot be applied because
the following file systems have insufficient free space.

/usr requires 2965 more 1K Blocks to complete this operation.

Press Enter to continue.
Press Enter to return to System Manager.
```

If there is sufficient space for all PTFs, you will see messages similar to:

```
The selected updates will now be applied.
You will not see any message on this screen until the installation
completes.  The output is being collected in the file
pd_update.log.10227 in the transfer directory.  If the installation
fails, you will be provided an opportunity to view that file, otherwise
this IBM 6611 will shutdown and restart automatically.

Press Enter to broadcast a message to all users of this IBM 6611 and
continue.
Press Enter to return to System Manager.
```

Interruptions to the Installation Process

During the installation process, status and error messages are written to the screen. If the installation fails, a reason for the failure should be displayed on the screen. If failures are detected, or if the installation process is interrupted, the Software Installation and Maintenance Facility attempts to automatically "clean up" by removing software updates that were partially installed and restoring the component to its previous state before attempting to install the software update.

In most cases, the Software Installation and Maintenance Facility's automatic cleanup is successful. Normally, you must perform a manual cleanup only when the system shuts down or loses power during the installation. If you have a problem with your installation that results in a partial installation and the automatic cleanup is not successful, select **Clean Up after a Failed Installation** to clean up the partial installation and restore the saved file.

If the system successfully returns to the previous state, you may apply software updates to the Multiprotocol Network Program. If the system does not return to the previous state, the Multiprotocol Network Program is marked as broken. IBM recommends that you call your service representative if the Multiprotocol Network Program is broken.

A summary report is provided at the end of the installation step that lists the status of each of the software updates that were installed.

Correcting Installation Failures

The installation of software updates can fail for several reasons:

- There is insufficient space in the file system where the saved files are stored, when the update is applied. To create more space, you can commit applied software updates. Refer to "Commit Applied Updates" on page 7-29 for details.
- The software update failed its verification during the installation step. The software update files were damaged during the transfer to the 6611. You can attempt to recover by resending the files. Refer to"Checking for Corrupted Data" for information on what to do if you suspect this problem will occur before beginning installation.
- Software updates that are a prerequisite to the one being applied have not already been applied and are not part of the software package being applied.
- Software updates that are a corequisite to the one being applied are not part of the software package being applied.

When installing software updates from the transfer directory, the software update images are removed from the directory after installation.

Recommended Software Pre-Installation Actions

Potential problems or delays in the installation procedure can be avoided if you perform certain actions first. These actions do not need to be performed before every software change, but rather when certain problem situations are suspected.

Cleaning Up the 6611 Transfer Directory

Receiving installation files results in their transfer into the transfer directory of the 6611. If you know you have unnecessary files in the transfer directory (such as outdated dumps or code), delete the files before beginning the installation. Refer to "Delete Transfer Directory Files" on page 4-43 for details.

Committing previously applied updates, if appropriate, will also free space. Refer to "Commit Applied Updates" on page 7-29 for details.

Checking for Corrupted Data

Checking for corrupted data need not be performed every time files are received. However, if installation files were received through FTP, or you have reason to think data may have been corrupted in the transfer, you may want to check for corrupted data.

When installing a software update, refer to installation directions shipped with the update for the *blocksize* values.

After you have received the software installation files:

1. Issue the **files transfer checksum** command for the appropriate file name in the transfer directory. (Refer to 9-67 for details.)

   You will see output displayed similar to:

   ```
   552544952 21236736 /tmp/hold/transfer/mpnp.obj 1.1.00.002.NP61002
   ```

   for the file name you specified on the command. The first number is the checksum; the second is the file size (bytes).

2. Compare these two numbers to those in your documentation. If they match, you know the installation files were received in good condition.

   If the numbers do not match, reissue the **files transfer checksum** command and repeat this verification procedure. If the numbers still do not match, call your IBM service representative.

Stopping Traces

Before beginning the installation process for any component or update, stop all trace activities. Active trace activities might cause installation to fail because of insufficient space. Refer to "Stop" on page 5-47 for information about stopping protocol and process traces. Refer to "Stop" on page 5-43 for information about stopping the system trace.

Handling Development PTFs

Before beginning the installation process for any software update, check to see if you have any development PTFs on your system. Development PTFs may be identified as containing the characters *FX* in their names, for example:

```
mpnp.obj   01.01.0001.0002.FX10014
```

If you know that you have development PTFs on your system, call your IBM Support Center with information on:

- Which development PTFs are already on your system
- What software update(s) you wish to install

You will receive directions on how to proceed. If the software change you want to make incorporates the fixes of the development PTF, you will be directed to reject the development PTF before making any software change. Your IBM Support Center may also send you a new development PTF to apply *after* making your desired software changes.

This is important because any development PTF you have has been tailored to your system environment. After you make any other changes to your system, the development PTF is no longer appropriate. If you try to reapply the development PTF to your system after making changes, other problems may occur.

If you are not sure and want to check if there are any development PTFs already on your system:

1. Select **Software Installation and Maintenance** on the System Manager main menu.
2. Select **List All Applied but Not Committed Software** on the next menu. (Refer to "List All Applied but Not Committed Software" on page 7-29 for details.) Check for any development PTFs.
3. After you have identified any development PTFs (and have checked with your IBM Support Center for direction), you are free to continue with the installation procedure for other software changes. (If you perform the rejection of the development PTFs now, instead of as part of the overall installation process, you will shut down the 6611 unnecessarily.)

If your IBM Support Center finds it necessary to supply a new development PTF, you should install it *after* the software update is installed.

Software Installation Procedure

To perform software installation from the System Manager:

1. Log in to the System Manager using a controlling user ID.
2. Select **Software Installation and Maintenance** on the System Manager main menu.

Follow this procedure to install your software installation package using the System Manager:

Step 1 Your software installation package is sent to you on diskettes or tape. The software package must be moved to the transfer directory for installation.

Before proceeding, refer to "Recommended Software Pre-Installation Actions" on page 7-19 for suggested actions if you have not already done so.

Step 2 Select **Receive Installation File(s)** from the Software Installation and Maintenance menu to move the installation files to the transfer directory in the 6611. These import methods are available:

- FTP
- Modem
- Tape
- Diskette

Before receiving any installation files, the system validates that enough space is available in the transfer directory. To ensure that enough space is available in the transfer directory using System Manager:

1. Select **Operations** from the main System Manager menu.
2. Select **File and Diskette Operations** from the next menu.
3. Select **View Transfer Directory File** from the selector screen.

A screen displays the files in the transfer directory. At the top of the screen, you can find the free space available in the transfer directory. The software package documentation should state how much space is needed. If the transfer directory does not have enough space, you need to delete all unnecessary files from that directory. Refer to "Delete Transfer Directory Files" on page 4-43 for information about deleting files in the transfer directory.

Refer to "Transferring Software Updates" on page 7-4 for more information about receiving the software files.

Press **F3 (Esc+3)** until you return to the main System Manager menu and again select **Software Installation and Maintenance**.

Fast-Path Command(s)

software receive [-diskette|-tape] -all
software receive [-diskette|-tape] *software_name*
software receive -ftp *host_name userID passwd software_files*

Step 3 If you want to view a list of the software in the transfer directory of the 6611, select **List Installation Files** to list the software.

Fast-Path Command(s)

software list -transfer

Sample output from this command is shown in Figure 7-2.

```
 Option Name                Level                     I/U Q Content
 ============================================================================

  mpnp.obj                  01.01.0000.0003.NP61003    U  Y usr,root
#   Multiprotocol Network Program

  mpnp.obj                  01.01.0000.0002.NP61002    U  Y usr,root
#   Multiprotocol Network Program

  mpnp.obj                  01.01.0000.0001.NP61001    U  Y usr,root
#   Multiprotocol Network Program
```

Figure 7-2. Sample List of Installation Files in Transfer Directory

Press **F3 (Esc+3)** to return to the Software Installation and Maintenance menu.

Step 4 If you want to view the problems fixed by the updates in the transfer directory, and select from that list:

1. Select **List All Problems Fixed by Software Updates** to list the problems fixed by the software updates in the transfer directory.
2. Specify the update name on the dialog screen that follows. To select the update name, you can press **Enter** on the dialog screen to use the default of **all**. This lists the problems fixed by all the software updates in the transfer directory.

   You may also use **F4 (Esc+4)** to get a list of the possible values. Use **F9 (Esc+9)** to select the specific update whose problems you want to list. Press **Enter** to record the selections.
3. Specify a specific update. Select the software update in the transfer directory whose problems you want to list. Or, press **F4 (ESC+4)** to get a list of possible values.

   Software updates are in the form:

   ```
   mpnp.obj.01.01.0000.0000.NP12345
   mpnp.data.01.01.0000.0000.NP12345
   ```

   Press **Enter** to record the selections.

   Fast-Path Command(s)

   software update view -fixes -all
   software update view -fixes *update_name*

See Figure 7-3 on page 7-23 for sample output.

```
Fix information
------------------------------------------------------------------------
    files restored: 2

        usr/share fix information for
        mpnp.obj 1.1.00.003.NP61003
NP61003  Test software update3

Required 1.1 update.

        root fix information for
        mpnp.obj 1.1.00.003.NP61003
NP61003  Test software update3

Required 1.1 update.


    files restored: 2

        usr/share fix information for
        mpnp.obj 1.1.00.002.NP61002
NP61002  Test software update2

Required 1.1 update.

        root fix information for
        mpnp.obj 1.1.00.002.NP61002.
NP61002  Test software update2

Required 1.1 update.


    files restored: 2

        usr/share fix information for
        mpnp.obj 1.1.00.001.NP61001
NP61001  Test software update1

Required 1.1 update.

        root fix information for
        mpnp.obj 1.1.00.001.NP61001
NP61001  Test software update1
Required 1.1 update.
```

Figure 7-3. Sample List of Problems Fixed by Software Updates

4. Press **F3 (Esc+3)** until you return to the Software Installation and Maintenance menu.

Step 5 This step installs the software updates in the package.

1. Select **Apply Software Updates** to install the software updates in the package.
2. Press **F9 (Esc+9)** to select **Update names** on the selector screen. There are two methods for selecting the update name. Select one of the following:

mpnp.all
Apply all the software updates.

Any number of the listed updates
Apply each of the selected software updates.

Software updates are in the form:

```
mpnp.obj.01.01.0000.0000.NP12345
mpnp.data.01.01.0000.0000.NP12345
```

Press **Enter** to record the selections.

Fast-Path Command(s)

software update apply (-transfer) {-all} {*update_name*}
software update apply (-transfer) -noprecheck {-all}

If you receive error messages during the software installation, the installation may have failed. If there is an error in the installation, you will receive informational messages stating why the installation failed. Press **Enter** to view the detailed information. When all the messages have displayed, press **Enter** to return to System Manager.

A summary report is provided at the end of the installation step that lists the status of each of the software updates that have been installed. Figure 7-4 is an example of the summary report generated after installation of some Multiprotocol Network Program updates.

```
Install Summary
---------------
Name                          Fix Id  Part    Event       Result      State
-------------------------------------------------------------------------
mpnp.obj                     NP61003  USR     APPLY       SUCCESS     APPLIED
mpnp.obj                     NP61003  ROOT    APPLY       SUCCESS     APPLIED
mpnp.obj                     NP61002  USR     APPLY       SUCCESS     APPLIED
mpnp.obj                     NP61002  ROOT    APPLY       SUCCESS     APPLIED
mpnp.obj                     NP61001  USR     APPLY       SUCCESS     APPLIED
mpnp.obj                     NP61001  ROOT    APPLY       SUCCESS     APPLIED
```

Figure 7-4. Software Update Installation Output

Press **F3 (Esc+3)** until you return to the Software Installation and Maintenance menu.

Step 6 After installing a new version of software, that version becomes the current version (whether it has been applied or committed). If you decide to commit the applied update at this time, refer to "Commit Applied Updates" on page 7-29 for details.

Immediately after the installation of software changes, the 6611 will be automatically restarted. It is important to schedule the installation of software changes at a time of low usage for the 6611.

There is a command to stop and restart the 6611. Refer to 9-129 for details of the **system stop** command. This command stops all operations in the base operating system, including all routing to access the main system and all user sessions.

If one of the peer-capable adapters was disabled before the system is restarted, it remains disabled after the system is restarted. When this occurs, any new adapter code destined for that adapter is not downloaded. The 6611 should be powered off and back on again after a minute to restart the adapter and to download the new code to the adapter.

Before the beginning of the system restart, users are notified with a message stating the number of minutes before the system will be shut down. There are a series of messages that are displayed during the shutdown process. These messages vary slightly depending on whether you are connected over an EIA 232 serial port or a remote network connection, such as Telnet. See Figure 7-5 for an example of the system restart messages received over a direct connection. The last line is not displayed, if the system restart is issued from a remote user over a Telnet session.

```
SHUTDOWN PROGRAM
Sun Dec 22 18:07:50 1991


Broadcast message from ibm6611c on tty ...

PLEASE LOG OFF NOW !!!

System maintenance in progress.
All processes will be killed in 3 minutes.

Broadcast message from ibm6611c on tty ...

THE SYSTEM IS BEING BROUGHT DOWN NOW

Process accounting has stopped.
Error reporting has stopped.
Stopping NFS/NIS Daemons
The Subsystem or Group, nfsd, is currently inoperative.
The Subsystem or Group, biod, is currently inoperative.
The Subsystem or Group, rpc.lockd, currently inoperative.
The Subsystem or Group, rpc.statd, currently inoperative.
The Subsystem or Group, rpc.mountd, currently inoperative.
The Subsystem or Group, yppasswdd, currently inoperative.
The Subsystem or Group, ypupdated, currently inoperative.
All processes currently running will now be killed.
```

Figure 7-5. System Restart Messages

Receive Installation File(s)

Select **Receive Installation File(s)** to import software updates to the 6611 when using FTP over the IP network, using a modem, or copying from a diskette or tape.

To use the System Manager to receive installation files:

1. Select **Software Installation and Maintenance** from the System Manager main menu.
2. Select **Receive Installation File(s)** on the next menu.

3. From the selector screen, select the import method to be used. The supported methods are:

   FTP — On the dialog screen, specify the host name or IP address of the remote IP station from which software is sent using FTP.

   Specify the user ID at the remote IP station from which software was sent. You will be prompted for the password of the user ID.

   Specify the name of the software update to be imported. The name is the same at the remote node and at the 6611 where it arrives.

   Modem — Specify the software to be imported. This is the name as it appears in the 6611

   Tape — Specify the software to be imported. You may use the default of *all* to import all the software from the tape. Or you may use **F4 (Esc+4)** to get a list of software.

   Diskette — Specify the software to be imported. You may use the default of *all* to import all the software from the diskette. Or you may use **F4 (Esc+4)** to get a list of software.

   Press **F9 (Esc+9)** to make your selections.

   Press **Enter** to register your selections.

4. From the next selector screen, select the files to be imported.

If you use FTP to receive the files, you will see messages indicating the transfer is complete. You will be directed to press **Enter** to return to the System Manager.

Fast-Path Command(s)

software receive [-diskettel-tape] -all
software receive [-diskettel-tape] *software_name*
software receive -ftp *host_name userID passwd software_files*

List Installation Files

System Manager allows you to display a list of all software updates that are in the transfer directory and available for installation.

To list all software updates using System Manager:

1. Select **Software Installation and Maintenance** from the System Manager main menu.
2. Select **List Installation Files** on the next menu.
3. A COMMAND STATUS screen displays the list.

Fast-Path Command(s)

software list -transfer

Figure 7-6 on page 7-27 is an example of the output received.

```
  Option Name    Level                  I/U   Q   Content
  -------------- ----------------       ----- --- -----------------
  mpnp.obj       01.01.0000.0003.NP610003  U     Y  usr,root
#   Multiprotocol Network Program
  mpnp.obj       01.01.0000.0003.NP610002  U     Y  usr,root
#   Multiprotocol Network Program
  mpnp.obj       01.01.0000.0003.NP610001  U     Y  usr,root
#   Multiprotocol Network Program
```

Figure 7-6. Example of List Installation Files Output

List All Problems Fixed by Software Updates

To list all code problems fixed by a software update:

1. Select **List All Problems Fixed by Software Updates**.
2. A dialog screen is displayed. Select the software updates in the transfer directory whose problems you want to list. You may select the default, *all,* for the update name. Or press **F4 (Esc+4)** to get a list of updates.
3. Press **F9 (Esc+9)** to select each software component on the screen that follows. Press **Enter** to record the selections.
4. Press **Enter** to execute the function.
5. A COMMAND STATUS screen displays the output.

   The software updates selected are listed along with a problem description abstract.

Fast-Path Command(s)

software update view -fixes -all
software update view -fixes *update_name*

Figure 7-3 on page 7-23 provides a sample list of problems.

Apply Software Updates

Note: You cannot install updates until all prerequisite software is installed.

To install software updates:

1. Select **Software Installation and Maintenance** from the System Manager main menu.
2. Select **Apply Software Updates** on the next menu.
3. Press **F9 (Esc+9)** to select updates on the Update name selector screen. There are two methods for selecting the update name. Select one of the following:

   mpnp.all
   Apply *all* the software updates.

Any number of the listed updates

Apply each of the selected software updates.

Software updates are in the form:

```
mpnp.obj.01.01.0000.0000.NP12345
mpnp.data.01.01.0000.0000.NP12345
```

Press **Enter** to record the selections.

Fast-Path Command(s)

software update apply (-transfer) {-all} {*update_name*}
software update apply (-transfer) -noprecheck {-all}

Post Software Installation Functions

There are several software installation-related functions that may need to be performed after the software has been installed. The following sections explain how and when to perform these functions:

- "Clean Up after a Failed Installation"
- "Commit Applied Updates" on page 7-29
- "Reject Applied Updates" on page 7-31

Clean Up after a Failed Installation

During the installation process, status and error messages are written to the screen. If the installation fails, a reason for the failure should display. If failures are detected or, if the installation process is interrupted, the Software Installation and Maintenance Facility attempts to "clean up" by removing software updates that were partially installed. The facility also attempts to restore the component to the state it was in before it attempted installing the software update.

In most cases, the Software Installation and Maintenance Facility's automatic cleanup is successful. Normally, you might perform a manual cleanup only when the system shuts down or loses power during the installation. If you have a problem with your installation that results in a partial installation and the automatic cleanup is not successful, you want to clean up the partial installation and restore the saved file.

Note: Any manual cleanup operation should be done at the direction of IBM service.

To perform cleanup:

1. Select **Software Installation and Maintenance** from the System Manager main menu.
2. Select **Clean Up after a Failed Installation** on the next menu.
3. A COMMAND STATUS screen is displayed reporting the success or failure of the manual cleanup attempt.

Fast-Path Command(s)

software cleanup

If the system successfully returns to the previous state, you may apply software updates to the Multiprotocol Network Program. If the system does not return to the previous state, the Multiprotocol Network Program is marked as broken. IBM recommends that you call your service representative if the Multiprotocol Network Program is broken.

List All Applied but Not Committed Software

You may choose to list all software updates that have not been committed. This option is useful:

- If you need to free disk space by deleting files saved when the update is applied. You can commit the applied update.
- If you need to revert to the previous version of a file saved when the update is applied. You can reject an applied update.

To list software:

1. Select **Software Installation and Maintenance** from the System Manager main menu.
2. Select **List All Applied but Not Committed Software** on the next menu.
3. A COMMAND STATUS screen is displayed reporting the success or failure of the command. Figure 7-7 on page 7-30 shows sample output of a successful search.

Fast-Path Command(s)

software update list -nocommit

Commit Applied Updates

Note: You must have a minimum of 2000 1K blocks of free space in your /usr, /tmp, and root file systems. Use the **file system (view)** command to view the used and available space in the 6611 file systems. (Refer to 9-67 for details.) If you do not have this space, contact your IBM service representative before rejecting PTFs.

After running a new applied software update, you can decide to commit the update as permanent or to reject the update and use the previously saved files. The commit and reject functions are valid only for software updates that are applied, and not already committed.

Committing software updates removes the files that were saved when the update was applied. This frees space so that other software updates can be applied.

Warning: When you commit the software update, the change becomes permanent.

Before committing a software update:

- Determine all the updates that are a prerequisite to the update you are committing. Select the **View Software Vital Product Data** menu item on the Software Installation and Maintenance menu for that determination. (See "View Software Vital Product Data" on page 7-32 for more information.) If an update is a prerequisite to the one being committed, it also will be committed, if not already committed.
- Determine all the updates that have been applied but not yet committed. Select **List All Applied but Not Committed Software** to list all the software that has been applied, but not committed. Press **Enter** to view the list. See Figure 7-7 for an example of this list.

```
Name                 Part    Level                          State
-------------------------------------------------------------------
mpnp.obj             USR     01.01.0000.0003.NP61003          APPLIED
mpnp.obj             ROOT    01.01.0000.0003.NP61003          APPLIED
mpnp.obj             USR     01.01.0000.0002.NP61002          APPLIED
mpnp.obj             ROOT    01.01.0000.0002.NP61002          APPLIED
mpnp.obj             USR     01.01.0000.0001.NP61001          APPLIED
mpnp.obj             ROOT    01.01.0000.0001.NP61001          APPLIED
```

Figure 7-7. Example of List of Applied But Not Committed Software Output

- Evaluate the effect of the update and its uncommitted prerequisites on your system's performance.

If, after careful examination of the situation, you decide to commit the software update:

1. Select **Software Installation and Maintenance** from the System Manager main menu.
2. Select **Commit Applied Updates**.
3. Press **F9 (Esc+9)** to select the update name on the selector screen that follows. There are two methods for selecting the update name. Select one of the following:

   mpnp.all
   Commit all the software updates that are applied.

   Any number of the listed updates
   Commit each of the selected software updates.

   Software updates are in the form:

   ```
   mpnp.obj.01.01.0000.0000.NP12345
   mpnp.data.01.01.0000.0000.NP12345
   ```

   Press **Enter** to record the selections.

Fast-Path Command(s)

software update commit -all
software update commit *update_name*

An error message screen displays if there are no applied updates to be committed. Press **Enter** or **F3 (Esc+3)** to return to the System Manager.

Reject Applied Updates

After running a new applied software update, you can decide to commit the update as permanent or to reject the update and use the previously saved files. The commit and reject functions are valid only for software updates that are applied, but not committed.

Rejecting software updates removes the update files from the current system and replaces them with the files that were saved when the update was applied. This frees space so that other software updates can be applied.

Before rejecting a software update:

1. Determine all the updates that are dependents of the update you are rejecting.
2. Select the **View Software Vital Product Data** menu item on the Software Installation and Maintenance menu for that determination. Refer to "List Software Dependents" on page 7-36 for the steps involved. If an update is a dependent of the one being rejected, it also will be rejected.
3. Return to the Software Installation and Maintenance menu.
4. Select **List All Applied but Not Committed Software** to list all the software that has been applied, but not committed. (Refer to "List All Applied but Not Committed Software" on page 7-29 for information.) See Figure 7-7 on page 7-30 for an example of this list.
5. Evaluate the effect of rejecting the update and its dependents on your system's performance.

If, after careful examination of the situation, you decide to reject the software update:

1. Select **Software Installation and Maintenance** from the System Manager main menu.
2. Select **Reject Applied Updates**.
3. Press **F9 (Esc+9)** to select the update name on the selector screen that follows. There are two methods for selecting the update name. Select one of the following:

   mpnp.all
   Reject all the software updates that are applied.

   Any number of the listed updates
   Reject each of the selected software updates.

   Software updates are in the form:

   ```
   mpnp.obj.01.01.0000.0000.NP12345
   mpnp.data.01.01.0000.0000.NP12345
   ```

   Press **Enter** to record the selections.

Fast-Path Command(s)

software update reject *update_name*

An error message screen displays if there are no applied updates to be rejected. Press **Enter** or **F3 (Esc+3)** to return to the System Manager.

View Software Vital Product Data

Select this option to get selected information on MPNP. You can select any of the following functions:

- View software history
- List software updates
- List software prerequisites
- List software dependents
- View software product IDs

View Software History

This option presents you with all installation actions for the Multiprotocol Network Program since the current release was installed.

To show the entire installation history information:

1. Select **Software Installation and Maintenance** from the System Manager main menu.
2. Select **View Software Vital Product Data** from the next menu.
3. Select **history** from the selector screen.

Fast-Path Command(s)

software view -history

The output displays:

- The software name and its path
- Fix IDs (number)
- Release level
- Fix status
- Last action taken
- Date of last action
- Time of last action
- ID of user who performed the last action

Figure 7-8 on page 7-33 is an example showing history information for the mpnp.obj component.

```
  Name
  --------------------
    Fix Id  Release         Status     Action     Date       Time     User Name
    ------- --------------- ---------- ---------- ---------- -------- ----------
Path: /usr/lib/objrepos
  mpnp.obj
            00.01.0200.9343 COMPLETE   COMMIT     10/21/93   16:48:55 root
            00.01.0200.9343 COMPLETE   APPLY      10/21/93   16:32:34 root
    F102201 00.01.0200.9343 COMPLETE   COMMIT     10/28/93   07:29:15 root
            00.01.0200.9343 COMPLETE   APPLY      10/28/93   07:04:29 root

  mpnp.obj
    F102501 00.01.0200.9344 COMPLETE   APPLY      10/28/93   08:03:49 root

Path: /etc/objrepos
  mpnp.obj
            00.01.0200.9343 COMPLETE   COMMIT     10/21/93   16:48:56 root
            00.01.0200.9343 COMPLETE   APPLY      10/21/93   16:43:49 root
    F102201 00.01.0200.9343 COMPLETE   COMMIT     10/28/93   07:29:17 root
            00.01.0200.9343 COMPLETE   APPLY      10/28/93   07:07:35 root

  mpnp.obj
    F102501 00.01.0200.9344 COMPLETE   APPLY      10/28/93   08:08:00 root

Path: /usr/share/lib/objrepos
  mpnp.data
            00.01.0200.9343 COMPLETE   COMMIT     10/21/93   16:48:56 root
            00.01.0200.9343 COMPLETE   APPLY      10/21/93   16:48:36 root
```

Figure 7-8. Sample List of History Information for Software Components

List Software Updates

You may list all software updates installed for the current version. To perform this function:

1. Select **Software Installation and Maintenance** from the System Manager main menu.
2. Select **View Software Vital Product Data** from the next menu.
3. Select **updates** from the selector screen.

Fast-Path Command(s)

software update list
software update list -nocommit

The output contains information on:

- The software name and its path
- PFT name (number)
- State (applied, committed, or available)
- Fix information

Figure 7-9 on page 7-34 provides an example of listing software updates.

```
Path: /usr/lib/objrepos

 LPP NAME: mpnp.obj
 PTF Name:  NP02201
 State:   COMMITTED
 Fix information:
   NA00123

   The system manager only allows installing software from
   transfer directory or diskette.  We also need support for
   installing from tape.


 LPP NAME: mpnp.obj 01.02.0000.0000
 PTF Name:  NP02501
 State:   APPLIED
 Fix information:
   NA00123

   The system manager only allows installing software from
   transfer directory or diskette.  We also need support for
   installing from tape.


  NA00456

   If AppleTalk is disabled on last adapter that
   had AppleTalk enabled, then is enabled again,
   AppleTalk does not come up on that adapter.

Path: /etc/objrepos

 LPP NAME: mpnp.obj
 PTF Name:  NP02201
 State:   COMMITTED
 Fix information:
   NA00123

   The system manager only allows installing software from
   transfer directory or diskette.  We also need support for
   installing from tape.

 LPP NAME: mpnp.obj 01.02.0000.0000
 PTF Name:  NP02501
 State:   APPLIED
 Fix information:
   NA00123

   The system manager only allows installing software from
   transfer directory or diskette.  We also need support for
   installing from tape.
Path: /usr/share/lib/objrepos
```

Figure 7-9. List Software Updates Sample Output

List Software Prerequisites

You may list all software updates that are prerequisites for all software updates. Any prerequisites must be installed before the specified update. To perform this function:

1. Select **Software Installation and Maintenance** from the System Manager main menu.
2. Select **View Software Vital Product Data** from the next menu.
3. Select **prerequisites** from the selector screen.

Fast-Path Command(s)

software view -prerequisites

The output lists:

- The software name and its path
- Fix ID (number)
- State (applied, committed, or available)
- Prerequisites

Figure 7-10 shows a sample of software prerequisites output:

```
  Name                  Fix Id   State        Prerequisites
  --------------------  -------  -----------  --------------------------------
Path: /usr/lib/objrepos
  mpnp.obj                       COMMITTED
                                              *prereq mpnp.obj v=01 r=02 m=
                                                0000
  mpnp.obj 01.02.0000.0000
                         NP02501  APPLIED
                                              *prereq mpnp.obj v=01 r=02 m=
                                                0000
Path: /etc/objrepos
  mpnp.obj                       COMMITTED
                                              *prereq mpnp.obj v=01 r=02 m=
                                                0000
  mpnp.obj 01.02.0000.0000
                         NP02501  APPLIED
                                              *prereq mpnp.obj v=01 r=02 m=
                                                0000
Path: /usr/share/lib/objrepos
  mpnp.data                      COMMITTED    *prereq mpnp.obj v=01 r=02
```

Figure 7-10. Sample Output of Prerequisite Information for Software Component

List Software Dependents

You may obtain a listing of all software components or updates that depend on a listed software component or update. (The listed component or update must be installed before the dependent software.) To perform this function:

1. Select **Software Installation and Maintenance** from the System Manager main menu.
2. Select **View Software Vital Product Data** from the next menu.
3. Select **dependents** from the selector screen.

Fast-Path Command(s)

software view -dependents

The output (shown in Figure 7-11) lists:

- The software name and its path
- Dependents
- Dependents state

```
  Name                  Dependents                          Dependents State
  --------------------  ----------------------------------  ---------------
<Name> is a prerequisite of <Dependents>
Path: /usr/lib/objrepos
  mpnp.obj              mpnp.obj 01.02.0000.0000.NP02201    COMMITTED
                        mpnp.obj 01.02.0000.0000.NP02501    APPLIED
  mpnp.obj 01.02.0000.0000.NP02201
                        NONE
  mpnp.obj 01.02.0000.0000.NP02501
                        NONE

Path: /etc/objrepos
  mpnp.obj              mpnp.obj 01.02.0000.0000.NP02201    COMMITTED
                        mpnp.obj 01.02.0000.0000.NP02501    APPLIED
  mpnp.obj 01.02.0000.0000.NP02201
                        NONE
  mpnp.obj 01.02.0000.0000.NP02501
                        NONE

Path: /usr/share/lib/objrepos
  mpnp.data             NONE
```

Figure 7-11. Sample Output of Dependents Information for Software Component

List Software Product ID

You may show the product ID number of a software component. IBM software services uses unique IDs for each licensed program. To perform this function:

1. Select **Software Installation and Maintenance** from the System Manager main menu.
2. Select **View Software Vital Product Data** from the next menu.

3. Select **product ID** from the selector screen.

Fast-Path Command(s)

software view -product_ID

The output (a sample of which is shown in Figure 7-12) lists:

- The software name and its path
- Fix ID (number)
- Vendor code
- Product ID
- Feature ID
- Product name

```
                                Vendr Product    Feature
  Name                  Fix Id  Code  Id         Id         Product Name
  --------------------- ------- ----- ---------- ---------- --------------------
Path: /usr/lib/objrepos
  mpnp.obj                              5648-01600 0000       mpnp
                        NP02201         5648-01600 0000       mpnp
  mpnp.obj 01.02.0000.0000
                        NP02501         5648-01600 0000       mpnp

Path: /etc/objrepos
  mpnp.obj                              5648-01600 0000       mpnp
                        NP02201         5648-01600 0000       mpnp
  mpnp.obj 01.02.0000.0000
                        NP02501         5648-01600 0000       mpnp

Path: /usr/share/lib/objrepos
  mpnp.data                             5648-01600 0000       mpnp
```

Figure 7-12. Sample Output of Product ID Information for Software Component

Automating Software Installation and Maintenance Facility Functions

The installation of software updates on one or more 6611s can be managed from a single control point. This control point may be either a RISC System/6000 workstation or an 6611 working as a network installation server, and connected to the client 6611s' IP network. (A *client* is any operational 6611 containing network installation code and connected to an IP network.)

Note: IBM recommends that you synchronize the time on the control point and all clients before you begin an automatic installation.

Software installation can be automated in different ways:

- You may write and use your own scripts, or use individual commands or the System Manager to transfer and install files.
- You may use fast-path commands or scripts provided with the 6611 to perform overall installation:

- From the RISC System/6000 workstation, you may use the scripts provided: rimon, rinstall, and ristop
- From the 6611, you may use the fast-path software commands (as described in Chapter 9 on page 9-1)

When you use the provided scripts, you must first ensure the required .netrc and control files are defined appropriately. Refer to "Using the .netrc File" on page 7-40 and "Using Control Files as Part of the Installation Process" on page 7-41 for details.

IBM recommends that you use the scripts provided with the 6611 if you are going to automate software installation.

Using Your Own Commands and Scripts

From the RISC System/6000 workstation, FTP can be used to transfer the software to the 6611. After the software is on the 6611, you have two options to install the changes:

- Use the **telnet** command to access the 6611 and use the System Manager or the fast-path commands to install the software.
- Use the **rexec** or **rsh** commands to install the software, either by issuing single commands or by issuing multiple commands included in rsh scripts.

The noninteractive **ftp** command (which must be run from the 6611) and the **rsh** and **rexec** commands can be combined into scripts that automate the software installation process. Several commands can apply software updates. There are additional commands to commit, reject, remove, and reinstate the software and to list the software and its vital product data. For detailed information on the available set of software commands, refer to "Software Commands" on page 9-112 or use help in the fast-path environment.

Sample Noninteractive FTP Command

The noninteractive **ftp** command has the following format on the 6611 in the fast-path environment:

```
ftp -c userid password action filename filetype hostname
```

Where:

-c Allows the user ID, password, and transfer command to be placed on the command line.

userid User ID at the node to which the **ftp** command is sent.

password Password of the user ID at the node to which the **ftp** command is sent.

action One of the following transferring actions:

- get or mget - Retrieve a file from the node to which the **ftp** command is sent.
- put or mput - Send a file to the node to which the **ftp** command is sent.

filename File name or file name group of the file(s) being sent or received.

filetype Specify either ascii or binary.

hostname Host name of the node to which the **ftp** command is sent.

Sample Rexec and Rsh Commands

Rexec and **rsh** commands are typically used as part of a shell script. Such scripts may be used to transfer and apply software changes from a remote host. For example, to start the transfer of installation files using rexec, you could issue:

```
cmd="software receive -ftp -remote $thisaddr $thisid $thispw $filelist"
rexec $client $cmd
```

where the `software` command is used to transfer the files from the remote host to the transfer directory of the 6611. In this example, the first line defines the `$cmd` parameter specified on the rexec command. The other parameters (`$thisaddr`, `$thisid`, `$thispw`, `$filelist`, and `$client`) must also be defined with real values.

To start an installation process using rsh, you might issue:

```
cmd="software update apply -noprecheck -remote"
rsh $client -l ibm6611c ibm6611c $cmd
```

where the `software` command begins applying the update immediately, without prechecking and without committing it upon completion. In this example, `$cmd` is defined in the first line and `$client` must be defined with a real value.

Using the 6611-Provided Commands and Scripts

Three installation-related scripts are provided with the 6611. If you are using a RISC System/6000 as the network installation server, you would use these scripts:

- rimon
- rinstall
- ristop

Refer to "Sending Software Changes to One or Multiple 6611s" on page 7-47 for the definition and use of these scripts.

Use of these scripts requires prior definition of both .netrc and control files. (Refer to "Using the .netrc File" on page 7-40 and "Using Control Files as Part of the Installation Process" on page 7-41 for details.)

Using the provided scripts also provides automatic recovery for installation failures.

If you are using a 6611 as the network installation server, you would use the commands:

- **software rimon** *control_file_name*
- **software rinstall {-quiet} {-verbose}** *control_file_name*
- **software ristop** *control_file_name*

Refer to "Software Commands" on page 9-112 for details on these commands.

The network installation server must have sufficient space to store the installation files (up to 35 MB). The installation files can be located:

1. On diskette

   A diskette drive must be on the network installation server.
2. On tape

A tape drive must be on the network installation server.
3. In the transfer directory of a 6611 in the network
4. In a directory accessible from the network installation server

In the first three cases, the transfer of the installation files to a directory on the network installation server is done automatically.

If you are using a 6611 as the network installation server, the 6611 acting as the server cannot also be a client 6611.

If you are using a RISC System/6000 workstation as the network installation server, the network installation scripts must be installed and your network administrator must have a user ID. (Refer to "Sending Software Changes to One or Multiple 6611s" on page 7-47 for information on the IBM-supplied installation scripts.)

Using the .netrc File

Access to 6611s is controlled by user IDs and passwords. For the network installation process to work, it must know the passwords of the user IDs on the 6611s with which it works. You must specify the:

- Host name
- User ID
- Password

of all client 6611s in a .netrc file. (This file might or might not already exist in your home directory.)

The .netrc file is defined by AIX and is used by the ftp and rexec commands. If the file does not contain the needed 6611 information, then you will be prompted for the user ID and password of each client 6611 during the installation process.

To therefore make effective use of the rinstall script, ensure that:

- The .netrc file is indeed named `.netrc`.
- If a RISC System/6000 is the network installation server, the file is in the user's home directory.

  The file must be owned by the current user and must have a permission of 600 (chmod 600 .netrc).
- If a 6611 is the network installation server, the file is in the transfer directory
- The format for each entry is:

  machine *host_name* **login** *userID* **password** *passwd*

  where the values in italics should specify the client 6611's name, user ID, and password.

Note: The alternative to this scenario, if you do not want to store passwords in the file, is to manually enter the passwords each time you are prompted by the remote installation process.

Installation States and Phases

The overall installation process goes through different states and phases.

The **software state view** command displays the installation state of the 6611 Additionally, output from the provided scripts contains messages related to the different phases occurring during the overall installation process. For this output to be as informative as possible, you should be aware of these states and phases.

The installation phases are:

- Idle
- Transfer
- Setup
- Install

Within each phase, installation proceeds through these states:

Idle	Installation has not yet started
Transfer prepared	The client 6611 has been prepared for transfer
Transfer started	The transfer of installation files is in progress
Transfer complete	Installation files have been transferred
Transfer failed	The transfer of the installation files failed
Setup started	Precheck and setup have started
Setup complete	Ready to activate the installation
Setup failed	Precheck or setup has failed
Install pending	The installation timer has been set
Install started	The installation timer has expired, and installation is running
Install complete	Installation was successful
Install recover	Installation failed, and recovery is in progress
Install failed	Installation failed, and recovery (if any) was successful
Install broken	Installation and recovery have both failed

Using Control Files as Part of the Installation Process

You must create a control file containing the instructions for the network installation process.

Note: You must use separate control files for each version of software change being installed.

The control file must:

- Be an ASCII file containing statements separated by new line characters
- Begin each statement with a keyword
- Contain the names of any drives and the addresses of any 6611s involved in the installation process
- Specify when the installation should start

A sample control file template is provided in the static directory of the 6611. This template, which you can extract from the directory and modify, is named `ri_tmplt` and looks like:

```
# Network Install Control File Template
# Remove the # on the statements to be used.
# Replace the parts in <> with your parameters.

# update <NP00xxx>
#
# directory <server_path>
# source </dev/fd0 | /dev/rmt0.1 | ip_address path>
#
# option clear yes
# option fixes nocommit
# option patches keep
# option continue no
# option commit yes
# option monitor no
# option timeout <minutes>
# option interval <seconds>
# option manyxfer <number>
#
# client <client_address> <+mm | MMDDhhmm[.ss] | (blank)>
```

You can, of course, create your own control file.

Control File Keywords

Each statement in a control file must start with a keyword. The valid keywords are:

A comment; the rest of the line is ignored.

update The fix ID of an update to be installed. There can be more than one of these statements in the file; however the order of the statements is the order in which the updates are transferred to each client 6611

An example of a fix ID is NP00288.

directory The full path of the network installation server directory that contains or will contain the installation files. If the server is a 6611, a directory statement is not needed. If the server is a RISC System/6000, only *one* directory statement should be used in the control file.

source The source of the installation files. You may omit this statement if the installation files are already in the directory specified with the directory keyword.

option Sets an installation option. Refer to "Option Keywords in a Control File" on page 7-43 for details.

client Specifies a client and the time at which the installation should be activated. You must have at least one of these in a control file, or else no transfer or installation occurs.

This keyword must be followed by:

- The IP address of the client 6611. This can either be a name (such as router1) or a decimal address. (In this case, the name used is an alias for the IP address.)
- The time that the installation should be activated. The time may be *relative* from the time at which all the client 6611s have completed

precheck. The format for relative is +mm, where *mm* represents minutes.

The time may also be *absolute*, reflecting the time on that 6611. The format for absolute is MMDDhhmm[.ss].

If no time is specified, the default is +0, which means installation starts immediately.

The order in which client statements appear is significant. The order of the statements is the order in which:

- Files will be transferred to the client 6611(s)
- Installation timers will be started on the client 6611s. When specifying values on the client statements, the network administrator must either:
  - Set timers so that there is time for commands to reach all the client 6611s involved in the process, or
  - Arrange the client statements so that the most distant client 6611s are on the statements listed first

Option Keywords in a Control File

The option keyword is followed by an option name and a value. Table 7-2 shows the valid options and values. Default values are highlighted.

Table 7-2 (Page 1 of 2). Options for the Option Keyword

Option	Value	Value Description
clear	yes	Clear the client 6611s' transfer directory before transferring files. This will help prevent failures due to lack of space.
	no	Do not clear the transfer directory.
fixes	**commit**	Commit the applied, but not committed, PTFs.
	nocommit	Do not commit any PTFs. If any uncommitted PTFs exist, and a component is being installed, the installation will be stopped.
patches	**reject**	Automatically reject any applied development PTFs before installation.
	keep	Do not reject applied development PTFs before installation. If any exist, installation will be stopped on this 6611. This option is ignored if all the updates being applied are development PTFs.
continue	**yes**	Continue installation on other client 6611s if installation on one fails.
	no	Do not continue. If installation on one client 6611 fails, the network installation process will be stopped.
commit	**yes**	Apply and commit the installation files.
	no	Apply, but do not commit, the installation files. This value is not valid for development PTFs.
monitor	yes	Continue to monitor the client 6611s after the network installation server starts the installation timer.
	no	Do not continue monitoring activities.

Table 7-2 (Page 2 of 2). Options for the Option Keyword

Option	Value	Value Description
timeout	*minutes*	The amount of time to allow for each phase of the installation. (Refer to "Installation States and Phases" on page 7-41 for definitions of the phases.) If the time that the client 6611 is in any one phase exceeds this value, the installation is considered to have failed.
	60	The default time, in minutes.
interval	*seconds*	The polling interval for the installation monitor.
	20	The default polling interval, in seconds.
manyxfer	#	The number of installation file transfers to be done in parallel. You supply this value.
	1	Transfer files to one client 6611 at a time.

Sample Control File

A sample control file is shown in Figure 7-13.

```
update NP00284
directory /u/mydir/images/1112/ptfs/ptf284
option clear yes
option fixes commit
option patches reject
option commit no
option continue yes
option interval 15
client router1 +2
client router2 +5
client router3 +15
```

Figure 7-13. Example of a Control File

As an example, this sample control file:

- Specifies only one update (NP00284) to be handled
- Shows the installation file is in the directory on a RISC System/6000
- Clears the 6611's transfer directory before transferring begins
- Requests that applied, but not committed, PTFs be committed
- Automatically rejects any development PTFs before installation
- Requests that the specified update be applied, but not committed
- Requests that installation continue on the remaining client 6611s even if it fails on one
- Specifies a polling interval of 15 seconds for the installation monitor
- Does not include an *option timeout* statement. This results in the default (60 minutes) being used. This means that 60 minutes will be allowed for each phase of the installation
- Identifies three client 6611s (whose IP addresses are known to the IP network) and the relative time, in minutes, at which installation should be activated

Any options not shown are defaulted.

Obtaining Remote Installation Output

The control file must be specified before you use any of the scripts from the network installation server. In this scenario, assume you have defined a control file like that in Figure 7-13 on page 7-44. If you are using a RISC System/6000 network installation server, type:

rinstall -v *control_file_name*

If you are using a 6611 network installation server, type:

software rinstall -verbose *control_file_name*

In either case, specifying the -verbose option results in output as shown in Figure 7-14. Refer to "Installation States and Phases" on page 7-41 for definitions of the various phases for which messages are issued.

```
Please enter the password for mydir at 19.7.195.39
Files to transfer are:
/u/mydir/images/1112/ptfs/ptf284/mpnp.B.01.01.0001.0002.NP00284.bff
Total size of files to transfer=12059 (1K blocks).
Getting current states of clients...
 Update mismatch - resetting state for router1 to idle.
 Update mismatch - resetting state for router2 to idle.
 Update mismatch - resetting state for router3 to idle.
Preparing clients...
 Preparing client router1
  Free space on router1 = 48492 (1K blocks).
 Preparing client router2
  Free space on router2 = 36545 (1K blocks).
 Preparing client router3
  Free space on router3 = 43896 (1K blocks).
Transferring files...
 Issuing transfer command to client router1
 Client router1 is now in state transfer started
 Client router1 is now in state transfer complete
 Issuing transfer command to client router2
 Client router2 is now in state transfer started
 Client router2 is now in state transfer complete
 Issuing transfer command to client router3
 Client router3 is now in state transfer started
 Client router3 is now in state transfer complete
Setup phase...
 Issuing setup command to client router1
 Issuing setup command to client router2
 Issuing setup command to client router3
 Client router1 is now in state setup started
 Client router2 is now in state setup started
 Client router3 is now in state setup started
 Client router1 is now in state setup complete
 Client router2 is now in state setup complete
 Client router3 is now in state setup complete
Install phase...
 Issuing install command to client router1
 Issuing install command to client router2
 Issuing install command to client router3
 Client router1 is now in state install pending
 Client router2 is now in state install pending
 Client router3 is now in state install pending
 Client router1 is now in state install started
 Client router2 is now in state install started
 Client router1 is now in state install complete
 Client router2 is now in state install complete
 Client router3 is now in state install started
 Client router3 is now in state install complete
```

Figure 7-14. Output of Remote Installation Command (Verbose)

If you specified the same commands without the -verbose option, you would get output as shown in Figure 7-15 on page 7-47.

```
Please enter the password for mydir at 19.7.195.39
Files to transfer are:
/u/mydir/images/1112/ptfs/ptf284/mpnp.B.01.01.0001.0002.NP00284.bff
Getting current states of clients...
Preparing clients...
Transferring files...
Setup phase...
Install phase...
```

Figure 7-15. Output of Remote Installation Command (without Verbose)

Sending Software Changes to One or Multiple 6611s

The static directory of the 6611 already contains the provided scripts that you can use to more easily automate remote installation of software updates. These scripts are:

rimon Starts remote monitoring of all client 6611s.

rinstall Starts remote installation of an update on multiple client 6611s.

ristop Stops a pending installation on one or more client 6611s specified in a control file.

Scripts may be executed from a RISC System/6000 workstation or from the 6611, depending on which is being used as the network installation server. If you are using a RISC System/6000 as the network installation server, you must transfer the scripts from the static directory of the 6611 to the RISC System/6000 using FTP. At the workstation, create the necessary control file, containing the software update file names and the necessary information about each of the 6611s requiring the software installation. (Refer to "Using Control Files as Part of the Installation Process" on page 7-41 for details.) If you are using a 6611 as the network installation server, no transfer is needed.

To send a file from the static directory:

1. Select **Operations** on the System Manager main menu.
2. Select **File and Diskette Operations** on the next menu.
3. Select **&flstat1.** on the next menu to accomplish this. Refer to "Send Static Directory File" on page 4-48 for details.

You may distribute and install updates across a single IP network or on different IP networks provided there are routes between the networks.

Note: The length of time needed to add a new software update depends on the size of the software change.

For the following procedure, see Figure 7-16 on page 7-48 for a picture of an IP network in which you have multiple client 6611s and are using a RISC System/6000 as the network installation server.

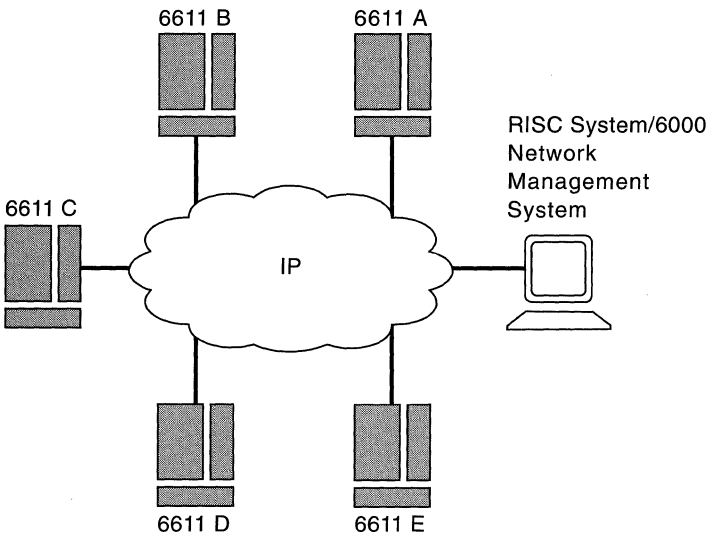


Figure 7-16. Network with Multiple Client 6611s and RISC System/6000 Server

The procedure for performing a remote installation is:

Step 1 The software installation package is sent to you on diskettes or tape. If a workstation is being used, transfer the software files to a directory on the workstation. Refer to "From Diskette to the RISC System/6000 Workstation" on page 7-7 or "From Tape to the RISC System/6000 Workstation" on page 7-7 for details.

The rinstall script will handle this transfer for you if you use the **source** keyword in the required control file.

If a 6611 is being used as the network installation server, refer to "From a Diskette to an IBM 6611" on page 7-5 or "From Tape to an IBM 6611" on page 7-6 for details.

Step 2 Transfer the scripts from the static directory of a 6611 to the workstation, if the workstation is being used. (To use a script, it must be in a directory that is in your path, and the script must have execute permission. Otherwise, no transfer is required.) Refer to "Send Static Directory File" on page 4-48 for details on the menu path to take to send the files via FTP.

Step 3 Create the control file that is to be accessed by this script. (Refer to "Using Control Files as Part of the Installation Process" on page 7-41 for details on using control files.)

If a 6611 is used as the network installation server, the file should be stored in the transfer directory.

Step 4 Execute the rinstall script. You are prompted for the password of the user ID at the workstation from which you execute this script.

Before using rinstall, refer to "Using the .netrc File" on page 7-40 for more information.

If you are using a 6611 as the network installation server, issue the **software rinstall** *control_file_name* command, with the appropriate options. You must also ensure the .netrc file is in the transfer directory of the 6611.

Fast-Path Command(s)

If you are using a RISC System/6000 network installation server, type:

rinstall -v *control_file_name*

If you are using a 6611 network installation server, type:

software rinstall -verbose *control_file_name*

The message output from this script is displayed on the screen of the workstation.

Step 5 (Optional)

Display the status of the installation process on one client 6611.

Fast-Path Command(s)

From either network installation server, type:

rexec *client_address* **software state view**

where *client_address* is the IP address of the 6611. This example checks one client 6611 one time.

Step 6 (Optional)

Start monitoring of all client 6611s listed in the control file.

Fast-Path Command(s)

If you are using a RISC System/6000 network installation server, type:

rimon *control_file_name*

If you are using a 6611 network installation server, type:

software rimon *control_file_name*

This example checks multiple client 6611s repetitively.

Step 7 (As needed)

Stop a pending installation on one or all client 6611s listed in the control file.

Fast-Path Command(s)

If you are using a RISC System/6000 network installation server, type:

rexec *client_address* **software cancel {-force}**
ristop *control_file_name*

If you are using a 6611 network installation server, type:

rexec *client_address* **software cancel {-force}**
software ristop *control_file_name*

client_address is the IP address of the 6611. In this example, the rexec commands cancel installation on one client 6611. The ristop commands cancel installation on all client 6611s.

Step 8 (Optional)

View the `pd_update.log` and `pd_install.log` in the transfer directory of the 6611 if you encounter an error in the installation.

Fast-Path Command(s)

files transfer view *file_name*

MPNP Backup Restore Utility

The MPNP Backup Restore utility allows you to include the 6611 in your disaster recovery procedures. The fast-path environment provides a command you can use to back up a 6611 hard disk. When necessary, you can restore the hard disk using the self-restoring backup tape.

This utility lets you capture, on magnetic tape, an image of the hard disk contents from an operational 6611. This tape can be used to recreate those hard disk contents, either on the original hard disk or a different hard disk of the same model.

This utility consists of:

- Tape backup, in which you copy the hard disk contents to tape. Refer to "Backing Up the Hard Disk" on page 7-51 for details.
- Tape restore, in which you copy the tape contents to a hard disk. Refer to "Restoring the Hard Disk" on page 7-53 for details.

Hard Disk Formatting Operation

The restore program created on the backup tape can perform a format operation on the hard disk. The format operation writes and verifies information on each sector of the hard disk. This establishes a known initial working state for the hard disk. Certain failure modes, like loss of power at critical times, may require that the hard disk be reformatted.

While this formatting step is recommended, it is optional to accommodate certain uses of the tape restore function. For example, a test bed can be restored to a specific software level by using the restore function, but formatting the hard disk is not likely to be useful in this instance. Formatting adds approximately 15 minutes per hard disk to the restore time operation.

Configuration Data

A configuration diskette is required before 6611 operation because the backup tape does not contain configuration data. Exclusion of the configuration data allows a single tape to serve as backup for multiple 6611s of the same model and software service level.

Required Software and Hardware

To use the MPNP Backup Restore utility, certain software and hardware elements must be installed. See Chapter 7 in the *IBM 6611 Network Processor Introduction and Planning Guide* for the required software and hardware.

Creating Backup Tapes

Your enterprise should already have a disaster recovery procedure as insurance against unplanned outages. To include the 6611 in your recovery procedures, create a backup tape after configuring and testing each 6611. Thereafter, make a new backup tape whenever you update the MPNP software on each 6611. You may want to make an additional copy of the backup tape. Keep one copy near the 6611 and another at a remote site.

Note: Because the backup operation does not copy the configuration information that can be unique to each 6611, you should also retain a copy of the configuration diskette for each 6611. To expedite your backup operation, you need only make a backup tape for each model of 6611 with a level of MPNP used in your establishment's network. For example, if you have 10 Model 120s, 10 Model 140s, and five Model 170s, you would need to make three backup tapes.

Backing Up the Hard Disk

The backup operation is initiated from an operational 6611. To back up the 6611 hard disk:

1. Remove the terminator from the connector on the SCSI adapter.

   Note: When installing the hardware RPQ (see the *IBM 6611 Network Processor Introduction and Planning Guide* for the appropriate number), the service representative plugs the SCSI cable into the 6611 and then attaches the other end to your tape drive. This should be attached to the tape drive before the 6611 is powered on.

2. If not already attached, plug the cable into the connector on the SCSI adapter. If you are not sure of the location of the SCSI adapter, see the *IBM 6611 Network Processor Maintenance Information* manual.

3. Tighten the screws to secure the cable to the connector to the SCSI adapter.

   Note: There are no screws on the Model 120 SCSI adapter cable.

4. Plug the other end of the cable into the connector on the tape drive.

   Warning: Follow the procedures for attaching the tape drive to the 6611. All supported IBM tape drives require you to shut down the 6611 and power it off before connecting the tape drive. For specific connection instructions, see the installation or setup instructions provided with your tape drive.

5. Using the setup information supplied with your tape drive, set the SCSI Address Switch on the tape drive to 3.

6. Power on **(I)** the 6611 in Normal Mode.

7. Power on **(I)** the tape drive.

8. Ensure that the tape is *not* write-protected, then insert the tape into the tape drive.

9. Log in using a controlling user ID.

10. Ensure there are a minimum of 8000 1K blocks of free space in the transfer directory:

    a. Select **Operations** from the System Manager main menu.

    b. Select **fdo** from the next menu.

c. Select **Delete Transfer Directory Files** from the next menu. The header of the selector screen displays the free space in the transfer directory:

```
# Free space in transfer directory: 40708 1K blocks
# File Name                              Date/Time          Size(bytes)
# ---------------------------------    -------------    --------------
```

d. If the number of 1K blocks is less than 8000, use **F9 (Esc+9)** to select the files to delete. You may want to delete large, unnecessary files (such as dumps or traces) before continuing, to minimize the backup process.

e. Press **Enter** to register your selection.

f. A COMMAND STATUS screen displays a message after the file or files have been deleted.

g. Press **F10 (Esc+0)** to return to the System Manager main menu.

11. Press **F3 (Esc+3)** from the System Manager main menu to get to the fast-path command line.

12. Type **system backup** and press **Enter**.

13. These messages will display.

```
Are you sure you want to back up the system?
All data on the backup tape will be destroyed.
Enter "y" to continue, anything else to stop.
```

14. When you type **y** and press **Enter**, the backup begins with these messages:

```
Configuring tape drive ...
Setting tape block size ...
Writing system backup tape ...
```

Note: If you are using a tape media that requires more than one tape to back up the contents of the hard disk, messages prompting you to remove full tapes and insert empty tapes display on the screen. Refer to "Using Multiple Backup Tapes" on page 7-55 for more information.

15. After approximately 5 to 10 minutes, this message displays:

```
0301-164 bosboot:  Boot image is xxxx 512 blocks
```

The backup operation continues. Various informational and progress messages display during the approximately 15 to 60 minutes needed for the backup operation to complete (depending on the type of tape drive used). When finished, the tape rewinds and this message displays:

```
System backup is complete.
```

16. Remove the tape from the tape drive.

17. Shut down and power off the 6611.

18. If you are not going to leave the tape drive permanently connected to the 6611, power off the tape drive, then unplug the cable from the SCSI adapter and reinstall the terminator.

19. Label the backup tape. The backup tape label should include (at a minimum):

    6611 name
    Configuration name
    MPNP Release and PTF level (for example, MPNP 1.1.1.2 + PTF NP00287)
    Creation date

Tape drive model used
Tape number (if multiple tapes were used)

You may want to include more information (for example, the 6611 location) as appropriate for your enterprise. Remember, the more information you include on the tape label, the easier it will be to use if it becomes necessary to restore the hard disk.

20. Store backup tapes in a safe place. You may also wish to store a matching configuration diskette with the backup tape. Your disaster recovery procedures should already describe where and how to store backup tapes. You may want to keep one copy near the 6611 and another at your remote storage site.

Restoring the Hard Disk

The restore operation is initiated from a nonoperational 6611 by booting the tape image obtained from a previous backup operation. The only requirement is that the 6611 hardware is functional. Because the backup tape image contains the actual program used for the restore operation, the contents of the 6611 hard disk can be anything, including items such as nonoperational code or previous versions.

The restore operation support is limited. The target (hard disk) for the restore must be the same type (the same 6611 model) as the original source used to create the tape with the backup function.

If you or your service representative suspect that the hard disk needs to be replaced, try to restore it using its backup tape. To restore the hard disk:

1. Shut down and power **Off (O)** the 6611.
2. Remove the terminator from the connector on the SCSI adapter.
3. Attach the tape drive to the SCSI adapter, using the appropriate cable. See Chapter 7 in the *IBM 6611 Network Processor Introduction and Planning Guide* for the required software and hardware.
4. Power **On (I)** the tape drive.
5. (Optional) Attach and power on **(I)** an ASCII terminal.

   Note: You will need the ASCII terminal if you are restoring the hard disk from more than one tape (1/4 inch only), or you want to bypass the hard disk formatting step. For more information, refer to "Using Multiple Backup Tapes" on page 7-55 and "Hard Disk Formatting Operation" on page 7-50.
6. Insert the backup tape in the tape drive.
7. Verify that the diskette drive is empty.
8. Turn the key mode switch to the Service position.
9. Power on **(I)** the 6611.

   Note: The total restore operation takes approximately 35 to 120 minutes to complete, depending on the type of tape drive used, the 6611 model, and whether the hard disk formatting is performed. The Model 140 will take longer than the other models (approximately 50 to 120 minutes) as there are two hard disks to format as opposed to the single hard disk on the Models 120 and 170.

If an ASCII terminal is attached to the 6611, these messages display when the restore operation begins:

```
INIT: EXECUTING /sbin/rc.boot 2
6611 Installation

 Bypass hard disk format operation?
 Enter yes to bypass hard disk format or press RETURN to continue.
```

Note: You have 15 seconds to respond to this prompt. If there is no response within 15 seconds, the default (perform formatting) is taken. This 15 second timer allows for a restore operation without an ASCII terminal attached, while still allowing you to bypass the format operation (with a terminal attached).

If you bypass formatting, you will see the following message instead of the formatting progress messages:

```
Hard disk will NOT be formatted. If the restore operation fails,
preform restore again and select hard disk format.
```

If formatting was selected (or you used the default), you will see the following progress messages:

```
Format in progress. Please stand by.
1% complete ...
Format complete.
```

The percentage amount will be incremented as the hard disk is formatted. The Model 140 will display this information twice, once for each hard disk.

When the formatting is completed, the following message will be displayed:

```
Certify in progress. Please stand by.
1% complete ...
Certify complete.
```

Note: The Model 140 does not display the `Certify Complete` message.

The percentage amount will be incremented as the hard disk is certified. The Model 140 will display this information for each hard disk.

When the certification is completed, the following message will be displayed:

```
Retrieving file systems from install media ....
```

Note: After these messages display, the tape drive scans the tape for several minutes (as long as 30 minutes if using a slower tape drive). When scanning completes, informational messages display as the restore operation continues.

10. When the restore operation completes, the tape rewinds, the 6611 shuts down, `c60` appears in the 6611 3-digit display, and this message displays:

    ```
    Halt completed ....
    ```

11. Remove the tape from the tape drive.

12. Turn the key mode switch to the Normal position and power off **(O)** the 6611.
13. If you are not going to leave the tape drive permanently connected to the 6611, power off the tape drive, then unplug the cable from the SCSI adapter and reinstall the terminator.
14. Insert the correct configuration diskette in the diskette drive, then power on **(I)** the 6611.

Note: IBM recommends that you reset the time after restoring the hard drive.

Using Multiple Backup Tapes

If your tape drive cannot store the entire contents of the hard disk (approximately 150–200 MB) on one tape, the program will prompt you to remove one tape and insert another.

Backing Up the Hard Disk Using Multiple Tapes

When the tape is full and the program needs another tape to continue, the tape rewinds and these messages display:

```
There are xxxxx blocks on /dev/rmt0.1.
Insert next tape into tape drive and press Return.
```

The program continues to back up the hard disk to tape and this message displays:

```
Proceeding to device /dev/rmt0.1.
```

When finished, the tape rewinds and this message displays:

```
System backup is complete.
```

Restoring the Hard Disk Using Multiple Tapes

When one tape has been read and another tape is needed for the backup operation to continue, the tape rewinds and this message displays:

```
Insert next tape into tape drive.
Type "go" when ready to proceed (or "quit" to stop):
```

The program will continue to restore the hard disk from tape.

Tape Compatibility

When restoring a hard disk from a backup tape, you should use the same model tape drive that you used to create the backup tape. However, the following information may be helpful.

- The IBM 7207-012 will read backup tapes created on an IBM 7207-001.
- The IBM 7208-011 will read backup tapes created on an IBM 7208-001.

Error Messages

```
---------------------------------------------------------------------
ERROR: System backup failed: no tape drives available

EXPLANATION: A tape drive is not attached or the tape drive is
powered off.
This message appears after "Configuring tape drive ..."

USER RESPONSE: Attach or power on (|) the SCSI tape drive.
```

ERROR: Tape drive is not ready.
Make sure that a tape is inserted in the tape drive
and that the door is closed.
Press Return to continue. Otherwise type "quit" to stop.

EXPLANATION: There is no tape drive attached or the tape drive is
powered off.
This message appears after "Configuring tape drive ..."

USER RESPONSE: Attach or power on (|) the SCSI tape drive.

ERROR: System backup failed: not enough space in transfer directory.

To continue the backup operation delete unnecessary files in the
transfer directory.

EXPLANATION: There are less than 8000 1K blocks of free space in the
transfer directory.

USER RESPONSE: To continue the backup operation,
delete unnecessary files in the transfer directory.
From the System Manager Main Menu, select
"Operations".
Then select "File and Diskette Operations" to delete
unnecessary files.

ERROR: Tape is write protected.

Tape is write protected.
Check the write protect tab on the tape. If the tape is
write protected then unprotect it.
Press return to continue. Otherwise enter "quit" to stop.

EXPLANATION: The backup operation cannot write information on a
write protected tape.

USER RESPONSE: Remove the tape from the tape drive.
Verify you are using the correct tape. If you are using the
correct tape, remove the write protection.

ERROR: System backup failed: could not rewind tape.

EXPLANATION: The tape may have broken, or caught in the mechanism.

USER RESPONSE: Remove the tape and examine.

```
---------------------------------------------------------------------

 ERROR: System backup failed:  no table of contents on tape.

 EXPLANATION: The tape is damaged.

 USER RESPONSE: Retry the operation with a new tape.

---------------------------------------------------------------------

 ERROR: System backup failed:  could not create verification data file.

 EXPLANATION: The tape is corrupted.

 USER RESPONSE: Retry the operation with a new tape.

---------------------------------------------------------------------

 ERROR: System backup failed: system backup tape is damaged.

 EXPLANATION: The tape is damaged.

 USER RESPONSE: Retry the operation with a new tape.

---------------------------------------------------------------------
```

Helpful Hints

If a backup or restore operation fails:

1. Check the cable connections and repeat the procedure.
2. Call your service representative.

Chapter 8. Hardware Maintenance

About This Chapter

This chapter describes how to use the System Manager to gather data about the hardware vital product data (VPD).

Using the System Manager, you can view information about the hardware components of the 6611. You can list all the supported, defined, and installed hardware components. Characteristics about defined devices can be listed. VPD is available for all installed devices.

Supported devices
Devices that are allowed on the 6611 but not necessarily present, configured, or enabled.

Defined devices
Supported devices that exist at different status levels. The status levels are:

Available The device is present, configured, and enabled.

Defined The device is configured, but it is disabled. Defined does not necessarily mean that the device is present. The device may have been moved or removed, and the VPD remains from a previous configuration. Select the **Configuration Change VPD Update** menu item to match the VPD with the actual hardware setup.

Stopped The device is not operating. Either it is not configured or contains an error. Contact an IBM service representative or select **Configuration Change VPD Update** to remove this device.

Installed devices
Devices that are present and defined.

Figure 8-1 shows the Hardware Maintenance menu.

```
IBM 6611                                                        hostname
                          Hardware Maintenance

Move cursor to desired item and press Enter.

  Installed Devices
  Device Characteristics

  Hardware Vital Product Data
  Configuration Change VPD Update

  Serial Number
  Model Number




F1=Help           F2=Redraw screen    F3=Return          F4=SysID
F10=Main Menu                         Esc+L=Turn Log On
```

Figure 8-1. Hardware Maintenance Menu

Refer to the following for information about the individual menu items:

- "Installed Devices" on page 8-4
- "Device Characteristics" on page 8-5
- "Hardware Vital Product Data" on page 8-6
- "Configuration Change VPD Update" on page 8-7

Hardware VPD Format

There is a facility that manages the hardware components of the 6611. Records are maintained in the VPD repository for each supported, defined, and installed hardware component. The record contents are:

Hardware Component
A 2-byte field that uniquely identifies the hardware component.

Component Description
A brief description of the part, for example, Ethernet adapter.

FRU Number
The FRU number is an 8-character ASCII entry that defines the part number used by field service to order a replacement part. It is usually different from the manufacturing part number.

Part number
An 8-character ASCII field that contains the manufacturing part number that identifies the hardware element. This is the number used by manufacturing and development.

Engineering Change (EC) Level
An 8-character ASCII field used by manufacturing and development that specifically identifies the maintenance level of the hardware element.

Manufacturer
The manufacturer descriptor field is a 6-byte ASCII field. Components manufactured by IBM use IBM for the first three characters. The next 3 characters are alphanumeric and are a code assigned to each IBM location, for example, RTP is assigned code 023.

Vendor manufacturers are identified by a 6-digit number assigned by the purchasing department when a contract is established. An abbreviation for the IBM location establishing the contract is concatenated to the purchase order number.

Serial Number
The serial number is specified as an 8-character ASCII field in the range from 00000000 to ZZZZZZZZ. This number is required to allow you to track assets and allows IBM to track components in the field for machine control purposes.

ROM Level and ID
The data portion of this descriptor is in ASCII format and is a minimum of 4 characters. Optionally, a second field of variable length information specifies the ROM ID. This additional information is required if the adapter contains more than one ROM module.

Loadable Microcode Level
The level of microcode that exists in the adapter.

Network Address (Token Ring and Ethernet)
The 6-byte universal address for the network interfaces on the hardware element that support universally assigned network addresses. This includes all the LAN adapters in the 6611. There is one entry for each network interface on the adapter.

Slot Location
An ASCII number from 0 to 7 that indicates the physical slot in which an adapter resides.

Available for Adapter-Specific Use (Z0 L–ZZ L)
Displays various adapter specific information such as the adapter ID. The amount of information varies according to the adapter.

There is a detailed discussion of hardware VPD in the *IBM 6611 Network Processor Maintenance Information*.

Installed Devices

The Installed Devices menu item generates a list of all installed hardware devices along with their location and description.

1. Select **Hardware Maintenance** from the System Manager main menu.
2. Select **Installed Devices** from the next menu.
3. A COMMAND STATUS screen displays the list of installed devices.

Fast-Path Command(s)

hardware list -installed

Figure 8-2 on page 8-5 shows an example of the output.

```
The following resources are installed on the machine.
+/- = Added or deleted from Diagnostic Test List.
*   = NOT supported by Diagnostics.

  Device Name      Location Code     Device Description
  -----------      -------------     ------------------
+ sysplanar0       00-00             CPU Planar
+ fpa0             00-00             Floating Point Processor
* slc0             00-00             Serial Optical Link Chip
+ mem0             00-0D             16 MB Memory Card
+ ioplanar0        00-00             I/O Planar
* bus0             00-00             Micro Channel Bus
* sio0             00-00             Standard I/O Planar
+ fda0             00-00-0D          Standard I/O Diskette Adapter
+ fd0              00-00-0D-00       Diskette Drive
* ppa0             00-00-0P          Standard I/O Parallel Port Adapter
+ sa0              00-00-S1          Standard I/O Serial Port 1
+ tty0             00-00-S1-00       Asynchronous Terminal
+ sa1              00-00-S2          Standard I/O Serial Port 2
+ tty1             00-00-S2-00       Asynchronous Terminal
+ trtya0           00-01             token-ring network 16/4 adapter
+ entya0           00-03             Ethernet adapter
+ entya1           00-04             Ethernet adapter
+ entya2           00-05             Ethernet adapter
+ tltya0           00-06             Serial Adapter
+ scsi0            00-08             SCSI I/O Controller
+ hdisk0           00-08-00-00       355 MB SCSI Disk Drive
* sysunit0         00-00             IBM 6611 Network Processor
* tlty0            00-06-01          Serial Adapter Port
* tlty1            00-06-02          Serial Adapter Port
* trty0            00-01-01          token-ring network 16/4 adapter Port
* enty0            00-03-01          Ethernet adapter Port
* enty1            00-04-01          Ethernet adapter Port
* enty2            00-05-01          Ethernet adapter Port
```

Figure 8-2. Example of Installed Devices Output

Device Characteristics

The Device Characteristics menu item generates information about a configured and defined hardware device.

1. Select **Hardware Maintenance** from the System Manager main menu.
2. Select **Device Characteristics** from the next menu.
3. On the selector screen, select the defined device from a list.
4. Press **Enter** to make your choice.
5. A COMMAND STATUS screen displays the output. Figure 8-3 on page 8-6 displays an example of the device characteristics output obtained for the Ethernet adapter. The device name is listed along with its description, status, and location.

   When displaying device attributes, you may get additional information. The first column shows the attribute description. The second column shows the current attribute's values.

Fast-Path Command(s)

hardware device view *device_name*

Use **hardware device (list)** for the *device_name* parameter.

```
name     description              status       location

enty1    Ethernet adapter Port    Available    00-04-00


description                          value

RECEIVE DATA TRANSFER OFFSET         32
Enable ALTERNATE ETHERNET address    no
ALTERNATE ETHERNET address           0x
```

Figure 8-3. Example of Device Characteristics Output

Hardware Vital Product Data

The VPD of all installed hardware devices (such as adapters) is listed. For some devices, there is very little or no VPD given. For other devices, complete VPD is provided.

To display this information:

1. Select **Hardware Maintenance** from the System Manager main menu.
2. Select **Hardware Vital Product Data** from the next menu.
3. A COMMAND STATUS screen displays the output.

Fast-Path Command(s)

hardware view

When you display the hardware VPD for most items, as shown by the example in Figure 8-4, you receive:

- Hardware component
- Slot location
- Component description

```
Hardware Component   Slot Location       Component Description

  fpa0                 00-00             Floating Point Processor
  bus0                 00-00             Micro Channel Bus
  fd0                  00-00-0D-00       Diskette Drive
```

Figure 8-4. Example of Displaying Hardware VPD (Most Common Format)

When you display the hardware VPD, some hardware components will also display a list of other VPD items, if the information is available. Figure 8-5 on page 8-7 contains an example of this longer type of VPD display for the token-ring network 16/4 adapter and Ethernet adapter.

```
INSTALLED RESOURCE LIST WITH VPD
The following resources are installed on your machine.

  trtya0            00-01              token-ring network 16/4 adapter
  trty0             00-01-00           token-ring network 16/4 adapter port
        Device Specific.(Z0).........{
        Network Address.............08005A13006A
        Part Number.................93F1146
        EC Level....................C40140
        FRU Number..................93F3066
        Serial Number...............000106
        Displayable Message.........6611 Token-Ring Network 16/4 Adapter
        Manufacturer................RAL7868898
        Device Driver Level.........00
        Diagnostic Level............00
        ROS Level and ID............00
        Loadable Microcode Level....00

  entya0            00-03              Ethernet adapter
  enty0             00-03-00           Ethernet adapter port

        Device Specific.(Z0).........z
        Network Address.............08005A13224D
        Part Number.................93F1145
        EC Level....................C40140
        FRU Number..................93F3067
        Serial Number...............000589
        Displayable Message.........Ethernet adapter
        Manufacturer................RAL7868898
        Device Driver Level.........00
        Diagnostic Level............00
        ROS Level and ID............00
        Loadable Microcode Level....00
```

Figure 8-5. Example of Hardware Vital Product Data (Extended Output)

Configuration Change VPD Update

Use this option to update the hardware VPD to match the present configuration.

When hardware devices are added or removed from the 6611, the hardware component information needs to be updated to reflect the change. The 6611 can check for changes in its hardware configuration using the System Manager or the fast-path environment commands.

To use the System Manager to check for configuration changes:

1. Log in using a controlling user ID.
2. Select **Hardware Maintenance** from the System Manager main menu.
3. Select **Configuration Change VPD Update** from the next menu.

Fast-Path Command(s)

hardware config update

If the 6611 finds differences between the existing hardware VPD and the present hardware configuration, a menu is displayed. The menu identifies the items that have different VPD and configuration information. A list of possible scenarios causing the mismatch is provided. Select the one that explains the mismatch.

Figure 8-6 displays an example of this report. In the example, an Ethernet adapter was removed.

```
MISSING RESOURCE                                              801020

The following resource was detected previously, but is not detected now:

- entya 0               00-04                 Ethernet adapter

Has the resource been removed from the screen, moved to another location
or address, or turned off?

  The resource has NOT been removed from the system, moved to
    another location or address, or turned off.
    This selection will determine why the resource was not detected.
  The resource has been removed from the system and should be
    removed from the system configuration.
  The resource has been moved to another location and should be
    removed from the system configuration.
  The resource has been turned off and should be removed from
    the system configuration.
  The resource has been turned off but should remain in the
    system configuration.


F3=Cancel          Esc+7=Page Up          Esc+8=Page Down     Esc+0=Exit
```

Figure 8-6. Example of Configuration Change VPD Update Output

When no changes are found by the Configuration Change VPD Update, the system returns to the Hardware Maintenance menu screen.

Serial Number

To update the serial number of the 6611:

1. Select **Hardware Maintenance** from the System Manager main menu.
2. Select **Serial Number** from the next menu.
3. Select the type of action on the dialog screen:

   view

   Allows you to view the serial number.

   update

   Updates the serial number with the number you type in the Serial number field.
4. A COMMAND STATUS screen displays the output.

Fast-Path Command(s)

hardware serial update *serial_number*

Model Number

To update the model number of the 6611:

1. Select **Hardware Maintenance** from the System Manager main menu.
2. Select **Model Number** from the next menu.
3. Select the type of action on the dialog screen:

   view

   Allows you to view the model number.

   update

   Updates the model number with the number you type in the Model number field.
4. A COMMAND STATUS screen displays the output.

Fast-Path Command(s)

hardware model update *model_number*

Chapter 9. Fast-Path Environment

About This Chapter

This chapter describes the fast-path environment and contains an alphabetical listing of all the fast-path commands.

Fast-Path Commands

There are four types of commands available in the fast-path environment:

- Object-oriented commands
- Help commands
- Remote access commands
- Exit commands: **exit** and **quit**

For more information about help, refer to "Fast-Path Environment Help" on page 9-5. For more information about the remote access commands, refer to "Remote Access Commands" on page 9-104.

Syntax

Figure 9-1 shows the fast-path command syntax, which follows these guidelines:

- An object may or may not have a subobject, option, or parameter.
- An object always has an action.
- Actions follow the subobject.
- Options follow the action.
- Options *always* begin with a hyphen.
- Parameters follow the options.

```
object  subobject   action   options   parameters
```

Figure 9-1. Command Syntax for Object-Oriented Fast-Path Commands

Notation

These guidelines describe how commands are structured:

- Brackets (**[ ]**) surround:
  - Groups of options separated by an |, when only one option in the group can be specified (for example, **[-diskette|-tape]**)
  - Groups of options separated by an &|, when one or more options in the group can be specified (for example, **[(-packet) &| -frame]**)
- Parameters are in italics (*italics*). However, in the online helps parameters are in double quotation marks (" ") instead of italics.
- Parentheses (**( )**) surround any defaults for the subobjects, actions (depending on the subobject), and options.
- Braces (**{ }**) surround options and parameters that are not required.

Abbreviations

At the beginning of each command set, a table lists the abbreviations for the object, subobjects, actions, and options. You can use any combination of the full or abbreviated forms when issuing a fast-path command.

For example, you can view the files in the static directory by issuing this command:

```
files static list
```

or any of these abbreviated equivalent commands:

```
files static l
files st list
files st l
file static list
file static l
file st list
file st l
f static list
f static l
f st list
f st l
```

Output

Most of the fast-path environment commands send their output to the screen. However, some send it directly to the transfer directory. The detailed command help ("Object-Specific Help" on page 9-6) states the file name that contains the output when it is sent directly to the transfer directory. You can view any output file in the transfer directory with the **files transfer view** *file_name* command. The More Facility is invoked when files longer that one screen are viewed from the fast-path environment. For information on using the More Facility, refer to "The More Facility" on page 9-7.

The Fast-Path Log

The fast-path log can gather output from most commands that send output to the screen, such as:

- Route tables
- Statistical output

There can be a separate fast-path log for each user ID. The fast-path log name has the form:

`fp.log.userID`

where `userID` is the user who issued the command with the -log option.

Each of the fast-path logs are monitored when a user enters the fast-path environment. If the file is longer than 512 K bytes, it is renamed to `fp.log.userid.old` and a new log is created when data is directed to the log. The previous `fp.log.userid.old` is overlaid.

Types of output that are excluded from the log include:

- Most traces
- Error report output

- Dumps
- Commands ended by **Ctrl+C** (commands with continuous displays)
- Commands whose output is only one or two lines

To send output to the log, type the **-log** option on the command being issued. Output will go to the log, not to your screen. A time stamp, along with the command issued, will be included in each entry. Entries are appended to the log.

You should delete this file when it is no longer needed. To delete it, enter:

files transfer delete fp.log.userID

Fast-Path Environment Help

There are two kinds of help available in the fast-path environment:

- Global–Offers general information about using the fast-path environment
- Object-specific–Offers three levels of help for each object-oriented command set

Global Help

The fast-path environment global help provides the following information:

- How to use the fast-path environment–which includes information about:
  - The More facility
  - Command syntax
  - Command abbreviations
  - Command output
  - Object-specific help
  - Fast-path log
- How to use the RSH and REXEC environments
- A list of all objects and their abbreviations
- A list of all subobjects and their abbreviations
- A list of all options and their abbreviations

You can access fast-path global help by selecting **Fast Path** on the System Manager help panel, which only displays the help on how to use the fast-path environment, or by typing in one of the following fast-path commands:

- **help fastpath** or **help fp**
- **help remote** or **help rem**
- **help object** or **help obj**
- **help subobj** or **help so**
- **help action** or **help act**
- **help option** or **help opt**

Object-Specific Help

Object-specific help exists at the object, subobject, and action levels. For each of these, you can request help in three levels of detail with the *h* character.

- Level one detail (*h*) shows only the command syntax for the valid commands having the given *object subobject action*.
- Level two detail (*hh*) adds on a brief functional description of the command.

  You can also get level two help for each of the commands having a given object by just entering the object.
- Level three detail (*hhh*) adds help for each of the commands in the group.

  The detailed command help gives the command syntax, the environments in which the command is supported, the user authorization level necessary to issue the command, and detailed information about the parameters. For example, there are some commands that are only valid in the fast-path environment. The detailed help also states when a list can be used to provide valid values for a command parameter.

  If you request level 3 detail for just the object, you get a paragraph describing the set of commands, starting with the object and a list of the valid abbreviations for the object, subobjects, actions, and options used with the set of commands.

To invoke detailed help in the fast-path environment, type the portion of the command on which you request help, with one to three *h*s. For example:

appletalk list h or **at list h**

invokes first-level detailed help for the appletalk list command, resulting in:

```
appletalk (list) -trace_parameters {-log}
```

Specifying:

appletalk list hh or **at list hh**

invokes second-level detailed help, resulting in:

```
appletalk (list) -trace_parameters {-log}
  -  List the AppleTalk protocol trace parameters.
```

Specifying:

appletalk list hhh or **at list hhh**

invokes third-level detailed help, resulting in:

```
APPLETALK LIST

COMMAND SYNTAX:              appletalk (list) -trace_parameters {-log}
        DESCRIPTION:         List the AppleTalk protocol trace parameters .
        PARAMETERS:          None
        AUTHORIZATION:       Controlling and viewing users
        SYSTEM ENVIRONMENT:  RSH, REXEC, and fast-path
```

The More Facility

Fast-path help uses the More facility to view the help text. The More facility displays continuous text one screen at a time, pausing after each screen with an indication of how much of the file has already been read:

```
More--(xx%) [space = page down b = page up q = quit h = help]
```

See Table 9-1 and Table 9-2 for a list of available functions. The Action column lists what you should enter or press to perform the function.

Table 9-1. More Facility Basic Functions

Function	Action	Note
Next page	**Space bar**	1
Next line	**Enter**	2
Forward one screen	**f**	2
Backward one screen	**b**	2
Down 1/2 page	**d**	1
Go to end of file	**g**	
Repeat previous command	**.**	
Display line number	**=**	
Display file name and line number	**:f**	
Redisplay screen	**Ctrl+L**	
Exit this facility	**q**	

Notes:

1. Typing a number before the action allows you to scroll down that number of lines. For example, typing **5<space>** scrolls down five lines. For these actions, a default page size is automatically set. To change the default, type **nz**, where *n* is the desired number of lines per page.
2. Typing a number before this action repeats the function. For example, typing **5b** scrolls backward five screens.

Table 9-2. More Facility Search Functions

Function	Action
Search for a string	**/string**
Find the next occurrence of a string	**n**
Go to where the last search began	**'**

The More facility is also used to view any command output that spans more than one page.

The Retrieve Key

A retrieve key with editing functions exists for use in the fast-path environment. Key functions and user actions are:

Table 9-3. Retrieve Key Functions

Function	Action
Retrieve the last command	Press the up arrow. The cursor is placed at the end of the line
Retrieve the next command	Press the down arrow. The cursor is placed at the end of the line
Move the cursor to the left	Press the left arrow
Move the cursor to the right	Press the right arrow
Append to the displayed command	Type with the cursor at the end of the command
Insert into the displayed command	Type with the cursor at the insert spot
Delete a character	Press **Backspace** with the cursor immediately to the right of the character to be deleted
Overlay a character	Press **Backspace** to delete, and then type the new character

AIX-Like Commands

Table 9-4 on page 9-9 lists the AIX-like commands available in the fast-path environment and the exact fast-path command associated with each AIX-like command. System Manager does not support a full implementation of the AIX commands; only the options and parameters shown in the table are available.

Table 9-4. AIX-Like Commands and Their Fast-Path Command Equivalents

AIX Command	Fast-Path Command
cat *file_name*	files (transfer) view *file_name*
cksum *file_name*	files (transfer) checksum *file_name*
compress *file_name*	files (transfer) compress *file_name*
date	timeofday view
df	files system (view)
diff *file_name file_name*	files (transfer) compare *file_name file_name*
iostat *number_seconds number_samples*	system statistics (view) -input_output *number_seconds number_samples*
ls	files (transfer) list
lscfg	hardware (list) -installed
mv *file_name new_file_name*	files (transfer) rename *file_name new_file_name*
ps	process list -status
rm *file_name*	files (transfer) delete *file_name*
sar *number_seconds number_samples*	system statistics (view) -activity *number_seconds number_samples*
shutdown *number_minutes*	system stop (-restart) (-minutes) *number_minutes*
sum *file_name*	files (transfer) checksum *file_name*
ts	hardware slots (view) -detail
uncompress *file_name*	files (transfer) uncompress *file_name*
vmstat *number_seconds number_samples*	system statistics (view) -virtual_memory *number_seconds number_samples*
who	user (id) view (-logged_in)

Support of Older Command Format

Older versions of most fast-path commands are still supported. For the commands not supported, you will receive an error message. The commands no longer supported (and the current means of invoking their functions, if available) are:

arp_sys_add_perm_nopub This function no longer exists.

arp_sys_add_perm_pub This function no longer exists.

arp_sys_add_temp_nopub This function no longer exists.

arp_sys_add_temp_pub This function no longer exists.

arp_sys_del_host This function no longer exists.

atecho **appletalk echo**

config_err_rpt This function no longer exists.

err_rpt_etype_det **Error Log and Reports** menu item

err_rpt_etype_sum **Error Log and Reports** menu item

err_type_list	**Error Log and Reports** menu item
hw_serial_model	**hardware serial view** or **hardware serial set** **hardware model view** or **hardware model set**
install_verify	This function no longer exists.
stat_sys_lanbr	bridge lanbr view
time_zone_set	**Date and Time** menu item
trace_log_trans	This function no longer exists.
trace_sys_man_trans	This function no longer exists.

Adapter Commands

Use the adapter commands to:

- List the adapter names for the active interfaces
- Dump or trace the peer-capable adapters
- View the registers and memory of the peer-capable adapters

Table 9-5. Abbreviations for Adapter Commands

Type of term	Term and Abbreviations	
Object	adapter	adp, a
Subobject	memory	mem, m
	registers	reg, r
Action	dump	du
	list	l
	trace	tr, t
	view	v
Option	-line	-ln
	-log	-l
	-on	

adapter dump *adapter*

Description: Dump the memory and registers of the adapter. The information is sent to the transfer directory in the files:

```
pd_adapter_name.dram
pd_adapter_name.sram
pd_adapter_name.prom
pd_adapter_name.regs
pd_slot_list
```

where *adapter_name* is the name of the specified adapter.

Parameters: Use the **adapter list** command to list the installed adapters.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

adapter list {-log}

Description: List the installed peer-capable adapters.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

adapter memory (view) {-log} *adapter start_addr num_words*

Description: View the adapter memory starting at the specified address for a specific number of words.

Parameters: Use the **adapter list** command to list the installed adapters.

Specify the starting address of memory and the number of words to display. The starting address is either a hexadecimal number or a symbol name. The number of words can be from 1 to 10000.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

adapter registers (view) {-log} *adapter*

Description: View the adapter registers.

Parameters: Use the **adapter list** command to list the installed adapters.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

adapter trace (-line) (-on) *adapter num_packets*

Description: Start a line trace on the specified adapter. The trace stops after the specified number of packets are captured. The trace information is sent to the transfer directory as the file `pd_adapter_name.linetrace`, where *adapter_name* is the name of the adapter traced.

Parameters: Use the **adapter list** command to list the installed adapters. Specify a number from 1 to 200 for the *num_packets* parameter. Each packet can require up to 150 kilobytes in the transfer directory. The /tmp file system needs to have available space equal to the number of packets times 150; otherwise the line trace will not start. Use the **files system (view)** command to view the available space in the /tmp file system.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

Summary of Adapter Commands

Table 9-6. Summary of Adapter Commands

Command	Function
adapter dump *adapter*	Dump the adapter memory and registers.
adapter list {-log}	List the installed adapters.
adapter memory (view) {-log} *adapter start_addr num_words*	View the adapter memory.
adapter registers (view) {-log} *adapter*	View the adapter registers.
adapter trace (-line) (-on) *adapter num_packets*	Trace the input and output of the adapter.

AppleTalk Commands

Use the AppleTalk commands to:

- Start and stop the AppleTalk protocol trace
- List the trace parameters
- Send an echo to an AppleTalk node
- View the AppleTalk Address Resolution Protocol (AARP) table
- View AppleTalk routes, connections, and protocol statistics
- View filter and zone information.
- Set up AppleTalk for debug collection
- Collect AppleTalk debug information

Table 9-7. Abbreviations for AppleTalk Commands

Type of term	Term and Abbreviations	
Object	appletalk	appl, at
Subobject	arp	a
	connections	connection, con, c
	debug	db
	filters	filter, fil, f
	routes	route, r
	statistics	statistic, stat, s
	zones	zone, z
Action	collect	col, c
	echo	e
	list	l
	set	s
	trace	tr, t
	view	v
Option	-cat	-c
	-interface	-intf, -if, -i
	-log	-l
	-notrcstop	-nts, -no
	-off	
	-on	
	-system	-sys, -s
	-tar	-t
	-trace_parameters	-tp

appletalk arp (view) -interface {-log} *interface*

Description: View the AppleTalk ARP table for a given interface.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for AppleTalk.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

appletalk arp (view) (-system) {-log}

Description: View the AppleTalk ARP table.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

appletalk connections (view) {-log} *interface*

Description: View the AppleTalk interface connections.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for AppleTalk.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

appletalk debug (collect) {-system} {-notrcstop} [(-tar)|-cat] {*output_file*}

Description: Collect AppleTalk debug information. Specify the -system option to collect additional system debug information. Specify the -notrcstop option to keep the AppleTalk trace running while collecting the other debug information.

This command creates several output files in the transfer directory. These output files are combined into one file to facilitate the transfer from the 6611 to a remote host.

Specify the -tar option to archive the individual files to a binary file specified by *output_file*. Transfer the *output_file* to an AIX or UNIX workstation using the binary mode of ftp. Use the **tar -xvf** *output_file* command to restore the individual files. The individual files can be viewed with most workstation editors.

Specify the -cat option to combine the individual files into an ASCII file specified by *output_file*. Transfer the *output_file* to any workstation using the ASCII mode of ftp. The *output_file* can be viewed with most workstation editors.

Parameters: If you do not specify an output file name, the output is placed in the file `pd_hostname.appletalk.debug`, where *hostname* is the host name for this 6611. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the output file name.

If you specify an output file name, the prefix `pd_` is added to it. Specify only alphanumeric characters, periods (.), dashes (–), and underscores (_) in the output file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

appletalk debug set {*trace_parameters*}

Description: Set up AppleTalk to collect debug information. The output is placed in the file `hostname.AT.setup.db`, where *hostname* is the host name of the 6611. When you run the **appletalk debug collect** command, `hostname.AT.setup.db` is combined with the debug collection files and placed in the output file. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the setup file name.

This command starts the AppleTalk trace. The trace output is placed in the file `pd_appletalk.trc`.

Parameters: Use the **appletalk (list) -tp** command to list the valid trace parameters. If you do not specify any trace parameters, the AppleTalk trace is started with the *all* and *errors* parameters.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

appletalk echo {-log} *dest_network_id dest_node_id number_echos*

Description: Issue an echo request to another AppleTalk node.

Parameters: The destination network ID is the unique AppleTalk network ID. The destination node ID is the AppleTalk node ID. Specify 1 to 1000. for the *number_echos* parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

appletalk filters (view) {-log} *interface*

Description: View the AppleTalk interface filters.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for AppleTalk.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

appletalk (list) -trace_parameters {-log}

Description: List the AppleTalk protocol trace parameters.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

appletalk routes (view) -interface {-log} *interface*

Description: View the AppleTalk route table for a given interface.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for AppleTalk.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

appletalk routes (view) (-system) {-log}

Description: View the AppleTalk system route table.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

appletalk statistics (view) (-interface) {-log} *interface*

Description: View the AppleTalk network interface protocol statistics.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for AppleTalk.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

appletalk trace -off

Description: Stop the AppleTalk protocol trace. The trace output is sent to the transfer directory as pd_appletalk.trc.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

appletalk trace (-on) *trace_parameters*

Description: Start the AppleTalk protocol trace.

Parameters: Use the **appletalk list (-trace_parameters)** command to list the valid trace parameters.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

appletalk zones (view) {-log}

Description: View the AppleTalk zone table.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

Summary of AppleTalk Commands

Table 9-8 (Page 1 of 2). Summary of AppleTalk Commands

Command	Function
appletalk arp (view) -interface {-log} *interface*	View the AppleTalk ARP table for a given interface.
appletalk arp (view) (-system) {-log}	View the AppleTalk ARP table.
appletalk connections (view) {-log} *interface*	View the AppleTalk interface connections.
appletalk debug (collect) {-system} {-notrcstop} [(-tar)|-cat] {*output_file*}	Collect the AppleTalk protocol debug information.
appletalk debug set {*trace_parameters*}	Set up the AppleTalk protocol for collecting debug information.

Table 9-8 (Page 2 of 2). Summary of AppleTalk Commands

Command	Function
appletalk echo {-log} *dest_network_id dest_node_id number_echos*	Issue an echo request to another AppleTalk node.
appletalk filters (view) {-log} *interface*	View the AppleTalk interface filters.
appletalk (list) -trace_parameters {-log}	List the AppleTalk protocol trace parameters.
appletalk routes (view) -interface {-log} *interface*	View the AppleTalk route table for a given interface.
appletalk routes (view) (-system) {-log}	View the AppleTalk system route table.
appletalk statistics (view) (-interface) {-log} *interface*	View the AppleTalk network interface protocol statistics.
appletalk trace -off	Stop the AppleTalk protocol trace.
appletalk trace (-on) *trace_parameters*	Start the AppleTalk protocol trace.
appletalk zones (view) {-log}	View the AppleTalk zone table.

APPN Commands

Use the APPN commands to:

- Dump the APPN process
- Start or stop tracing the APPN protocol
- Format the APPN trace report
- List the APPN trace parameters and trace IDs
- Restart the APPN protocol
- Set or view user characteristics of an APPN class of service (COS)
- Set or view the APPN COS mode name
- Transfer an APPN COS file to and from the transfer directory.
- Set up APPN for debug collection
- Collect APPN debug information

Table 9-9. Abbreviations for APPN Commands

Type of term	Term and Abbreviations	
Object	APPN	appn, ap
Subobject	debug	db
Action	collect	col, c
	dump	du
	list	l
	restart	res
	set	s
	trace	tr, t
	transfer	trans, tf
	view	v
Option	-cat	-c
	-COS	-cos, -c
	-format	-for, -f
	-from	-fr, -f
	-log	-l
	-mode_name	-mode, -mod, -mn, -m
	-notrcstop	-nts, -no
	-off	
	-on	
	-restart	-res, -r
	-system	-sys, -s
	-tar	-t
	-to	-t
	-trace_ID	-tid, -ti, -id
	-trace_log	-tl
	-trace_parameters	-tp
	-transmission_group	-tg, -TG
	-user1	-u1
	-user2	-u2
	-user3	-u3

appn debug (collect) {-system} {-notrcstop} [(-tar)|-cat] {*output_file*}

Description: Collect APPN protocol debug information. Specify the -system option to collect additional system debug information. Specify the -notrcstop option to keep the APPN trace running while collecting the other debug information.

This command creates several output files in the transfer directory. These output files are combined into one file to facilitate the transfer from the 6611 to a remote host.

Specify the -tar option to archive the individual files to a binary file specified by *output_file*. Transfer the *output_file* to an AIX or UNIX workstation using the binary mode of ftp. Use the **tar -xvf** *output_file* command to restore the individual files. The individual files can be viewed with most workstation editors.

Specify the -cat option to combine the individual files into an ASCII file specified by *output_file*. Transfer the *output_file* to any workstation using the ASCII mode of ftp. The *output_file* can be viewed with most workstation editors.

Parameters: If you do not specify an output file name, the output is placed in the file `pd_hostname.appn.debug`, where *hostname* is the host name for the 6611. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the output file name. If you specify an output file name, the prefix `pd_` is added to it. Specify only alphanumeric characters, periods (.), dashes (–), and underscores (_) in the output file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

appn debug set {*trace_parameters*} {*trace_IDs*}

Description: Set up APPN to collect debug information. The output is placed in the file `hostname.APPN.setup.db`, where *hostname* is the host name of the 6611. When you run the **appn debug collect** command, `hostname.APPN.setup.db` is combined with the debug collection files and placed in the output file. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the setup file name.

This command starts the APPN trace. The APPN trace is integrated with the system trace. The trace output is placed in the file `hostname.APPN.trcfile`, where *hostname* is the host name of the 6611.

Parameters: Use the **appn (list) -tp** command to list the valid trace parameters. If you do not specify additional trace parameters, the APPN trace is started with the *all* parameter.

Use the **appn (list) -ti** command to list the valid trace IDs. The APPN trace is always started with the global trace IDs 001, 002, 106 10C, 134, and 139, and with the APPN trace IDs 360 and 361. Any additional trace IDs must be specified as three-digit uppercase hexadecimal numbers.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

appn dump

Description: Dump APPN nondisruptively. There can be up to three APPN dumps present at any given time. The dump is placed in the transfer directory as pd_dump.APPN.d#, where # is either 1, 2, or 3.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

appn (list) -trace_ID {-log}

Description: List the system trace trace IDs. The APPN trace is integrated with the system trace. These are the trace IDs for the portion of the trace that is common for all traces based on the system trace.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

appn (list) -trace_parameters {-log}

Description: List the APPN trace parameters. The APPN trace is integrated with the system trace. These are the parameters for the APPN-only section of the trace.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

appn restart

Description: Restart the APPN protocol.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

appn set (-COS) (-mode_name) {-restart} *COS_number mode_name*

Description: Add a mode name to an APPN class of service (COS) file. The mode name is used at session set up to specify session characteristics, including the COS. This configuration change is effective only after APPN is restarted. Specify the -restart option to restart APPN immediately. Use the **appn restart** command to restart APPN at a later time.

Note: To ensure that all 6611 network nodes in an APPN network use the same criteria to make routing decisions, each of the network nodes should have identical COS files. Consequently, any changes to a COS file should be made on each 6611 network node in the network.

Parameters: Specify the number corresponding to the APPN COS:

1–#BATCH
2–#BATCHSC
3–#CONNECT
4–#INTER
5–#INTERSC
6–CPSVCMG

7–SNASVCMG

Specify a string up to 8 characters in length (including special characters) for the *mode_name* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

appn set (-COS) [-user1|-user2|-user3] {-restart} *COS_number TG_row min_user_char max_user_char*

Description: Set the minimum and maximum values for a user-defined transmission group (TG) characteristic within an APPN COS file. Specify either the -user1, -user2, or -user3 option to determine which user-defined characteristic will be modified.

This configuration change is effective only after APPN is restarted. Specify the -restart option to restart APPN immediately. Use the **appn restart** command to restart APPN at a later time.

Note: To ensure that all 6611 network nodes in an APPN network use the same criteria to make routing decisions, each of the network nodes should have identical COS files. Consequently, any changes to a COS file should be made on each 6611 network node in the network.

Parameters: Specify the number corresponding to the APPN COS:

1–#BATCH
2–#BATCHSC
3–#CONNECT
4–#INTER
5–#INTERSC
6–CPSVCMG
7–SNASVCMG

Specify a number between 1 and 8 for the *TG_row* parameter. Specify a number between 0 and 255 for both the *min_user_char* and the *max_user_char* parameters. The *min_user_char* parameter must not be higher than the *max_user_char* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

appn trace -format

Description: Format the APPN trace. The APPN trace is integrated with the system trace. The trace output is placed in the transfer directory as pd_appn.trc.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

appn trace -off

Description: Stop the APPN trace. The APPN trace is integrated with the system trace. The trace log file is in `trcfile`.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

appn trace (-on) {-trace_log} {*trace_log_size*} {*trace_IDs*}

Description: Start the APPN trace. The APPN trace is integrated with the system trace. Use the **appn trace -trace_parameters** command to set trace parameters.

To stop the trace, issue **appn trace -off**. To format the trace, issue **appn trace -format**. The output is placed in `pd_appn.trc`; the trace log file is in `trcfile`.

Parameters: If you specify the -trace_log option, the *trace_log_size* parameter is required, and must precede any trace IDs. The trace log size is between 1 048 576 and 10 485 760 bytes with a default of 1 048 576 bytes.

The trace is always started with the global trace IDs 001, 002, 106, 10C, 134, and 139, with APPN trace IDs 360 and 361. Any additional trace IDs must be represented as three digit uppercase hexadecimal numbers. Use the **appn (list) -trace_ID** command to list the valid APPN trace IDs.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

appn trace -trace_parameters *trace_parameters*

Description: Set the APPN trace options. The APPN trace is integrated with the system trace. These are the parameters for the APPN-only section of the trace.

Parameters: Use the **appn (list) -trace_parameters** command to list the valid trace parameters.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

appn transfer (-COS) [(-to)|-from] *COS_number*

Description: Move a specific COS file between the APPN directory and the transfer directory.

Specify the -to option to move the COS file from the APPN directory to the transfer directory. After the COS file is in the transfer directory, you can export the file to a remote host for editing. As a rule, you should not edit a COS file manually unless you need to change a characteristic in the file that cannot be changed through System Manager. An error introduced into a COS file can negatively impact the routing of traffic in you APPN network.

Specify the -from option to move the COS file from the transfer directory to the APPN directory. APPN automatically restarts when you use the -from option.

Note: To ensure that all 6611 network nodes in an APPN network use the same criteria to make routing decisions, each of the network nodes should have identical COS files. Consequently, any changes to a COS file should be made on each 6611 network node in the network.

Refer to "Transferring Files" on page 4-62 for information about transferring files between the 6611 and a remote host.

Parameters: Specify the number corresponding to the APPN COS:

1–#BATCH
2–#BATCHSC
3–#CONNECT
4–#INTER
5–#INTERSC
6–CPSVCMG
7–SNASVCMG

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

appn view (-COS) {-log} *COS_number*

Description: Display the specified APPN COS file.

Parameters: Specify the number corresponding to the APPN COS:

1–#BATCH
2–#BATCHSC
3–#CONNECT
4–#INTER
5–#INTERSC
6–CPSVCMG
7–SNASVCMG

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

appn view (-COS) -mode_name *COS_number*

Description: Display the mode names in a specific APPN COS file.

Parameters: Specify the number corresponding to the APPN COS:

1–#BATCH
2–#BATCHSC
3–#CONNECT
4–#INTER
5–#INTERSC
6–CPSVCMG
7–SNASVCMG

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

appn view (-COS) -transmission_group *COS_number TG_row*

Description: Display the APPN COS information for a specific TG row.

Parameters: Specify the number corresponding to the APPN COS:

1–#BATCH
2–#BATCHSC
3–#CONNECT
4–#INTER
5–#INTERSC
6–CPSVCMG
7–SNASVCMG

Specify a number between 1 and 8 for the *TG_row* parameter.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

Summary of APPN Commands

Table 9-10. Summary of APPN Commands

Command	Function
appn debug (collect) {-system} {-notrcstop} [(-tar)|-cat] {*output_file*}	Collect the APPN protocol debug information.
appn debug set {*trace_parameters*} {*trace_IDs*}	Set up the APPN protocol for collecting debug information.
appn dump	Dump APPN nondisruptively.
appn (list) -trace_ID {-log}	List the APPN trace IDs.
appn (list) -trace_parameters {-log}	List the APPN trace parameters.
appn restart	Restart the APPN protocol.
appn set (cos) (-mode_name) {-restart} *COS_number mode_name*	Add a mode name to an APPN COS file.
appn set (cos) [-user1|-user2|-user3] *COS_number TG_row min_user_char max_user_char*	Set the minimum and maximum values for a user-defined TG characteristic for a specific TG and COS.
appn trace -format	Format the APPN trace.
appn trace -off	Stop the APPN trace.
appn trace (-on) {-trace_log} {*trace_log_size*} {*trace_IDs*}	Start the APPN trace.
appn trace -trace_parameters *trace_parameters*	Set the APPN trace parameters.
appn transfer (-COS) [(-to)|-from] *COS_number*	Move a COS file between the APPN directory and the transfer directory.
appn view (-COS) {-log} *COS_number*	Display an APPN COS file.
appn view (-COS) -mode_name *COS_number*	Display the mode names in a specific APPN COS file.
appn view (-COS) -transmission_group *COS_number TG_row*	Display APPN COS information for a specific TG row.

Bridge Commands

There are bridge commands for:

- LAN bridging
- Source route bridging
- Transparent bridging
- Translational bridging

Use the bridge commands to:

- Trace source route bridging
- View statistical information for source route, transparent, translational, and LAN bridging
- View the possible interfaces or port indexes for source route, transparent, translational, and LAN bridging
- Collect bridging debugging information
- View the MAC addresses necessary to define a bridge with LAN Network Manager

Table 9-11. Abbreviations for Bridge Commands

Type of term	Term and Abbreviations	
Object	bridge	brdg, br, b
Subobject	debug	db
	LAN_bridge	lanbr, lb
	LAN_network_manager	lnm
	source_route_bridge	srb, s
	transparent_bridge	tb, t
	translational_bridge	tlb
Action	collect	col, c
	list	l
	trace	tr, t
	view	v
Option	-both	-b
	-cat	-c
	-filter	-filters, -fil, -f
	-frame_trace	-ft
	-interface	-intf, -if, -i
	-interface_info	-info, -ii, -i
	-internal_frames	-if
	-LAN_bridge	-lanbr, -lb
	-local	-loc
	-log	-l
	-off	
	-on	
	-port_index	-pi, p
	-receive	-rec, -rcv, -r
	-remote	-rem
	-source_route_bridge	-srb
	-spanning_tree	-spt
	-spanning_tree_frame_relay	-sptfr
	-statistics	-statistic, -stat
	-system	-sys, -s
	-tar	-t
	-transmit	-xmit, -tr, -t
	-transparent_bridge	-tb
	-translational_bridge	-tlb

bridge debug (collect) [(-srb)|-tb|-lb|-tlb] {-system} [(-tar)|-cat] {*output_file*}

Description: Collect bridge debug information for either source route bridge, transparent bridge, LAN bridge, or translational bridge. Specify the -system option to collect additional system debug information.

This command creates several output files in the transfer directory. These output files are combined into one file to facilitate the transfer from the 6611 to a remote host.

Specify the -tar option to archive the individual files to a binary file specified by *output_file*. Transfer the *output_file* to an AIX or UNIX workstation using the binary mode of ftp. Use the **tar -xvf** *output_file* command to restore the individual files. The individual files can be viewed with most workstation editors.

Specify the -cat option to combine the individual files into an ASCII file specified by *output_file*. Transfer the *output_file* to any workstation using the ASCII mode of ftp. The *output_file* can be viewed with most workstation editors.

Parameters: If you do not specify an output file name, the output is placed in the file:

```
pd_hostname.srb.debug
pd_hostname.tb.debug
pd_hostname.lb.debug
pd_hostname.tlb.debug
```

where *hostname* is the host name of this 6611. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the output file name. If you specify an output file name, the prefix `pd_` is added to it. Specify only alphanumeric characters, periods (.), dashes (–), and underscores (_) in the output file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

bridge lb list (-interface)

Description: List the possible LAN bridging interfaces.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge lb (view) -internal_frames *interface number_seconds*

Description: View the internal frames for the LAN bridge protocol for the given serial interface. Press **Ctrl+C** to end the command.

Parameters: Use the **bridge lb list (-interface)** command to list the possible LAN bridging interfaces. Choose only the serial interfaces configured for LAN bridge.

Use the *number_seconds* parameter to specify the time interval between updating the display. Specify a number between 1 and 5 for this parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

bridge lb (view) (-statistics) *interface number_seconds*

Description: View the LAN bridge interface statistics for a given serial interface. Press **Ctrl+C** to end the command.

Parameters: Use the **bridge lb list (-interface)** command to list the possible LAN bridging interfaces. Choose only the serial interfaces configured for LAN bridge.

Use the *number_seconds* parameter to specify the time interval between updating the display. Specify a number between 1 and 5 for this parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

bridge lb (view) (-statistics) -system *interface number_seconds*

Description: View the LAN bridge system statistics for a given serial interface. Press **Ctrl+C** to end the command.

Parameters: Use the **bridge lb list (-interface)** command to list the possible LAN bridging interfaces. Choose only the serial interfaces configured for LAN bridge.

Use the *number_seconds* parameter to specify the time interval between updating the display. Specify a number between 1 and 5 for this parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

bridge lnm (view) [(-local)|-remote]

Description: View the bridge port MAC addresses needed to create a bridge definition on LAN Network Manager.

Specify the -local option when defining a local bridge. The output contains the physical MAC address of the port on the 6611 connected to the token ring, and the DLSw virtual MAC address.

Specify the -remote option when defining a remote bridge. The output contains the physical MAC address of the ring to be managed, and the DLSw virtual MAC address.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge (srb) list (-interface)

Description: List the possible source route bridging interfaces.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge (srb) list -port_index *interface*

Description: List the port indexes of the given serial interface that are configured for source route bridging and frame relay.

Parameters: Use the **bridge (srb) list (-interface)** command to list the possible source route bridging interfaces. Choose only the serial interfaces configured for source route bridging and frame relay.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge (srb) trace -off [(-transmit)|-receive|-both] *interface*

Description: Stop the source route bridging frame trace on the given interface tracing transmitted, received, or transmitted and received frames.

Parameters: Use the **bridge (srb) list (-interface)** command to list the possible source route bridging interfaces. Choose only the interfaces configured for source route bridging.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge (srb) trace (-on) [(-transmit)|-receive|-both] *number_frames interface*

Description: Start the source route bridging frame trace on the given interface tracing the given number of transmitted, received, or transmitted and received frames.

Parameters: You can trace from 1 to 32 frames. The *number_frames* parameter can be any number from 1 to 800. If 32 or less is specified, that number of frames is captured and the trace is stopped. If a number greater than 32 is specified, the last 32 frames are captured.

Use the **bridge (srb) list (-interface)** command to list the possible source route bridging interfaces. Choose only the interfaces configured for source route bridging.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge (srb) trace -spt [(-on)|-off]

Description: Start or stop the source route bridge spanning tree trace.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge (srb) (view) -filter {-log} *interface*

Description: View source route bridge filter information for the given interface.

Parameters: Use the **bridge (srb) list (-interface)** command to list the possible source route bridging interfaces. Choose only the interfaces configured for source route bridging.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge (srb) (view) -frame_trace [(-transmit)|-receive|-both] {-log} *interface*

Description: View the source route bridging frame trace on the given interface tracing transmitted, received, or transmitted and received frames.

Parameters: Use the **bridge (srb) list (-interface)** command to list the possible source route bridging interfaces. Choose only the interfaces configured for source route bridging.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge (srb) (view) -information_info {-log} *interface*

Description: View the source route bridge interface information for the given interface.

Parameters: Use the **bridge (srb) list (-interface)** command to list the possible source route bridging interfaces. Choose only the interfaces configured for source route bridging.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge (srb) (view) (-statistics) *interface number_seconds*

Description: View the source route bridge statistics for the given interface. Press **Ctrl+C** to end the command.

Parameters: Use the **bridge (srb) list (-interface)** command to list the possible source route bridging interfaces. Choose only the interfaces configured for source route bridging.

Use the *number_seconds* parameter to specify the time interval between updating the display. Specify a number between 1 and 5 for this parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

bridge (srb) (view) (-statistics) -spt *interface number_seconds*

Description: View the source route bridge spanning tree statistics for the given interface. Press **Ctrl+C** to end the command.

Parameters: Use the **bridge (srb) list (-interface)** command to list the possible source route bridging interfaces. Choose only the interfaces configured for source route bridging.

Use the *number_seconds* parameter to specify the time interval between updating the display. Specify a number between 1 and 5 for this parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

bridge (srb) (view) (-statistics) -sptfr *port_index number_seconds*

Description: View the source route bridging spanning tree frame relay statistics for the given interface. Press **Ctrl+C** to end the command.

Parameters: Use the **bridge (srb) list -port_index** *interface* command to list the source route bridging port indexes for the given serial interface.

Use the *number_seconds* parameter to specify the time interval between updating the display. Specify a number between 1 and 5 for this parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

bridge tb list (-interface)

Description: List the possible transparent bridging interfaces.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge tb list -port_index *interface*

Description: List the port indexes of the given serial interface that are configured for transparent bridging and frame relay.

Parameters: Use the **bridge tb list (-interface)** command to list the possible transparent bridging interfaces. Choose only the serial interfaces configured for transparent bridging and frame relay.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge tb trace -off *interface*

Description: Stop the transparent bridging frame trace on the specified interface.

Parameters: Use the **bridge tb list (-interface)** command to list the possible transparent bridging interfaces. Choose only the interfaces configured for transparent bridging.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge tb trace (-on) *number_frames interface*

Description: Start the transparent bridging frame trace on the specified interface tracing the given number of frames.

Parameters: You can trace from 1 to 32 frames. The *number_frames* parameter can be any number from 1 to 800. If 32 or less is specified, that number of frames is captured and the trace is stopped. If a number greater than 32 is specified, the last 32 frames are captured.

Use the **bridge tb list (-interface)** command to list the possible transparent bridging interfaces. Choose only the interfaces configured for transparent bridging.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge tb trace -spt [(-on)|-off]

Description: Start or stop the transparent bridge spanning tree trace.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge tb (view) -filter {-log} *interface*

Description: View transparent bridge filter information for the given interface.

Parameters: Use the **bridge tb list (-interface)** command to list the possible transparent bridging interfaces. Choose only the interfaces configured for transparent bridging.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge tb (view) -frame_trace {-log} *interface*

Description: View transparent bridging frame trace on the given interface.

Parameters: Use the **bridge tb list (-interface)** command to list the possible transparent bridging interfaces. Choose only the interfaces configured for transparent bridging.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge tb (view) (-statistics) *interface number_seconds*

Description: View the transparent bridge statistics for the given interface. Press **Ctrl+C** to end the command.

Parameters: Use the **bridge tb list (-interface)** command to list the possible transparent bridging interfaces. Choose only the interfaces configured for transparent bridging.

Use the *number_seconds* parameter to specify the time interval between updating the display. Specify a number between 1 and 5 for this parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

bridge tb (view) (-statistics) -spt *interface number_seconds*

Description: View the transparent bridge spanning tree statistics for the given interface. Press **Ctrl+C** to end the command.

Parameters: Use the **bridge tb list (-interface)** command to list the possible transparent bridging interfaces. Choose only the interfaces configured for transparent bridging.

Use the *number_seconds* parameter to specify the time interval between updating the display. Specify a number between 1 and 5 for this parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

bridge tb (view) (-statistics) -sptfr *port_index number_seconds*

Description: View the transparent bridging spanning tree frame-relay statistics for the given interface. Press **Ctrl+C** to end the command.

Parameters: Use the **bridge tb list -port_index** *interface* command to list the transparent bridging port indexes for the given serial interface.

Use the *number_seconds* parameter to specify the time interval between updating the display. Specify a number between 1 and 5 for this parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

bridge tlb list (-interface)

Description: List the possible translational bridging interfaces.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge tlb list -port_index *interface*

Description: List the port indexes of the given serial interface that are configured for translational bridging and frame relay.

Parameters: Use the **bridge tlb list (-interface)** command to list the possible translational bridging interfaces. Choose only the serial interfaces configured for translational bridging and frame relay.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge tlb trace -spt [(-on)|-off]

Description: Start or stop the translational bridge spanning tree trace.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

bridge tlb (view) (-statistics) -spt *interface number_seconds*

Description: View the translational bridge spanning tree statistics for the given interface. Press **Ctrl+C** to end the command.

Parameters: Use the **bridge tlb list (-interface)** command to list the interfaces configured for translational bridging. Choose only the interfaces configured for translational bridging.

Use the *number_seconds* parameter to specify the time interval between updating the display. Specify a number between 1 and 5 for this parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

bridge tlb (view) (-statistics) -sptfr *port_index number_seconds*

Description: View the translational bridging spanning tree frame-relay statistics for the given interface. Press **Ctrl+C** to end the command.

Parameters: Use the **bridge tlb list -port_index** *interface* command to list the translational bridging port indexes for the given serial interface.

Use the *number_seconds* parameter to specify the time interval between updating the display. Specify a number between 1 and 5 for this parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

Summary of Bridge Commands

Table 9-12 (Page 1 of 2). Summary of Bridge Commands

Command	Function
bridge debug (collect) [(-srb)|-tbl-lbl-tlb] {-system} [(-tar)|-cat] {*output_file*}	Collect bridging debugging information for either source route bridge, transparent bridge, translational bridge, or LAN bridge.
bridge lb list (-interface)	List the possible LAN bridging interfaces.
bridge lb (view) -internal_frames *interface number_seconds*	View the internal frames for the LAN bridge protocol for the given serial interface.
bridge lb (view) (-statistics) *interface number_seconds*	View the LAN bridge interface statistics for a given serial interface.
bridge lb (view) (-statistics) -system *interface number_seconds*	View the LAN bridge system statistics for a given serial interface.
bridge lnm (view) [(-local)|-remote]	View the bridge port MAC addresses needed to create a bridge definition in LAN Network Manager.
bridge (srb) list (-interface)	List the possible source route bridging interfaces.
bridge (srb) list -port_index *interface*	List the port indexes of the given serial interface that are configured for source route bridging and frame relay.
bridge (srb) trace -off [(-transmit)|-receive|-both] *interface*	Stop the source route bridging frame trace on the given interface tracing transmitted, received, or transmitted and received frames.
bridge (srb) trace (-on) [(-transmit)|-receive|-both] *number_frames interface*	Start the source route bridging frame trace on the given interface tracing the given number of transmitted, received, or transmitted and received frames.
bridge (srb) trace -spt [(-on)|-off]	Start or stop the source route bridge spanning tree trace.
bridge (srb) (view) -filter {-log} *interface*	View the source route bridging filter information for the given interface.
bridge (srb) (view) -frame_trace [(-transmit)|-receive|-both] {-log} *interface*	View the source route bridging frame trace on the given interface tracing transmitted, received, or transmitted and received frames.

Table 9-12 (Page 2 of 2). Summary of Bridge Commands

Command	Function
bridge (srb) (view) -mib {-log} *interface*	View the source route bridging MIB information for the given interface.
bridge (srb) (view) (-statistics) *interface number_seconds*	View the source route bridge statistics for the given interface.
bridge (srb) (view) (-statistics) -spt *interface number_seconds*	View the source route bridging spanning tree statistics for the given interface.
bridge (srb) (view) (-statistics) -sptfr *port_index number_seconds*	View the source route bridging spanning tree frame relay statistics for the given interface.
bridge tb list (-interface)	List the possible transparent bridging interfaces.
bridge tb list -port_index *interface*	List the port indexes of the given serial interface that are configured for transparent bridging and frame relay.
bridge tb trace -off *interface*	Stop the transparent bridging frame trace on the specified interface.
bridge tb trace (-on) *number_frames interface*	Start the transparent bridging frame trace on the specified interface.
bridge tb trace -spt [(-on)|-off]	Start or stop the transparent bridge spanning tree trace.
bridge tb (view) -filter {-log} *interface*	View the transparent bridging filter information for the given interface.
bridge tb (view) -frame_trace {-log} *interface*	View the transparent bridging frame trace on the given interface.
bridge tb (view) (-statistics) *interface number_seconds*	View the transparent bridge statistics for the given interface.
bridge tb (view) (-statistics) -spt *interface number_seconds*	View the transparent bridge spanning tree statistics for the given interface.
bridge tb (view) (-statistics) -sptfr *port_index number_seconds*	View the transparent bridging spanning tree frame relay statistics for the given interface.
bridge tlb list (-interface)	List the possible translational bridging interfaces.
bridge tlb list -port_index *interface*	List the port indexes of the given serial interface that are configured for translational bridging and frame relay.
bridge tlb trace -spt [(-on)|-off]	Start or stop the translational bridge spanning tree trace.
bridge tlb (view) (-statistics) -spt *interface number_seconds*	View the translational bridge spanning tree statistics for the given interface.
bridge tlb (view) (-statistics) -sptfr *port_index number_seconds*	View the translational bridging spanning tree frame relay statistics for the given interface.

Config Commands

Use the configuration (config) commands to:

- Install a new configuration from the transfer directory
- Send the current configuration to the transfer directory
- Apply, commit, or reject configurations created from the System Manager or the fast-path environment
- Reinstate saved configurations and list the saved configurations from the System Manager or the fast-path environment
- View a configuration report, the state of the configuration, and the configuration script

Table 9-13. Abbreviations for Config Commands

Type of term	Term and Abbreviations	
Object	config	cfg, c
Subobject	script	scr
	state	st
Action	appiy	app, a
	commit	com, c
	install	in, i
	list	l
	reinstate	rein
	reject	rej
	send	s
	view	v
Option	-applied	-app, -a
	-both	-b
	-cfgfile	-cf, -c
	-detail	-det, -d
	-log	-l
	-summary	sum, -s
	-unapplied	-una, -u

config apply

Description: Apply configuration changes. They can later be rejected.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

config commit [-applied|-both]

Description: Commit configuration changes. They cannot be rejected later. If you select **-both**, all unapplied and applied configuration changes made with your user ID are committed. If you select **-applied**, only applied configuration changes made with your user ID are committed.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

config install *cfgfile_name*

Description: Install the configuration file in the transfer directory.

Parameters: Specify the configuration file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

config list (-cfgfile) {-log}

Description: List the saved configuration files. The last ten configurations are saved.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

config reinstate *cfgfile_number*

Description: Reinstate a saved configuration file. The last ten configurations are saved. A new saved configuration file is created anytime a configuration change is made from the System Manager or the fast-path environment and the change is either applied or committed. If the latest configuration change made from this user ID is unapplied, the change is rejected before the configuration file is reinstated. If the latest configuration change made from this user ID is applied, the change is committed before the configuration file is reinstated.

Parameters: Use the **config list -cfgfile** command to list the saved configurations. Use only the number of the configuration file.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

config reject [-unappliedl-both]

Description: Reject the uncommitted configuration changes. If you select **-both**, all applied and unapplied configuration changes made with your user ID are rejected. If you select **-unapplied**, only unapplied configuration changes made with your user ID are rejected.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

config script (view)

Description: View the configuration script. The output is sent to the transfer directory as config.script.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

config send

Description: Send the current configuration on the 6611 to the transfer directory as `config`.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

config state (view) {-log}

Description: View the configuration name and state. The 6611 host name, serial number, and model number are also displayed, as well as a description of the adapters in each of the slots.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

config (view) [-detaill-summary] {-log}

Description: View the detailed or summary configuration report. The output is sent to the transfer directory as either `config.report.detail` or `config.report.summary`.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

Summary of Config Commands

Table 9-14. Summary of Config Commands

Command	Function
config apply	Apply configuration changes.
config commit [-appliedl-both]	Commit configuration changes.
config install *cfgfile_name*	Install configuration file in transfer directory.
config list (-cfgfile) {-log}	List saved configuration files.
config reinstate *cfgfile_number*	Reinstate saved configuration file.
config reject [-unappliedl-both]	Reject uncommitted configuration changes.
config script (view)	View the configuration script.
config send	Send the current configuration on the 6611 to the transfer directory.
config state (view) {-log}	View the configuration name and state.
config (view) [-detaill-summary] {-log}	View the detailed or summary configuration report.

DECnet Commands

Use the DECnet (decnet) commands to:

- Start and stop the DECnet trace
- Change the output destination of the trace
- Set the trace parameters, the trace mask, and time stamp mask
- List the trace mask settings
- View DECnet routes, connections, and protocol statistics
- View filter and routing information
- Set up DECnet for debug collection
- Collect DECnet debug information

Table 9-15. Abbreviations for DECnet Commands

Type of term	Term and Abbreviations	
Object	decnet	dec
Subobject	connections	connection, con, c
	debug	db
	filters	filter, fil, f
	routes	route, r
	statistics	statistic, stat, s
Action	collect	col, c
	list	l
	set	s
	trace	tr, t
	view	v
Option	-adjacencies	-adj
	-area_cost	-ac
	-area_hop	-ah
	-area_minimum_cost	-amc
	-area_minimum_hop	-amh
	-area_output_adj	-aoa
	-area_reach	-ar
	-cat	-c
	-circuit	-cir
	-cost	-c
	-decnet	-dec, -d
	-executor	-exec, -ex
	-hop	-h
	-interface	-intf, -if, -i
	-log	-l
	-minimum_cost	-mc
	-minimum_hop	-mh
	-notrcstop	-nts, -no
	-off	
	-on	
	-output_adj	-oa
	-reach	-r
	-route_info	-ri
	-system	-sys, -s
	-tar	-t
	-timestamp_mask	-tsm
	-trace_log	-tl
	-trace_mask	-tm

decnet connections (view) {-log} *interface*

Description: View the DECnet interface connections.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for DECnet.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet debug (collect) {-system} {-notrcstop} [(-tar)|-cat] {*output_file*}

Description: Collect DECnet debug information. Specify the -system option to collect additional system debug information. Specify the -notrcstop option to keep the DECnet trace running while collecting the other debug information.

This command creates several output files in the transfer directory. These output files are combined into one file to facilitate the transfer from the 6611 to a remote host.

Specify the -tar option to archive the individual files to a binary file specified by *output_file*. Transfer the *output_file* to an AIX or UNIX workstation using the binary mode of ftp. Use the **tar -xvf** *output_file* command to restore the individual files. The individual files can be viewed with most workstation editors.

Specify the -cat option to combine the individual files into an ASCII file specified by *output_file*. Transfer the *output_file* to any workstation using the ASCII mode of ftp. The *output_file* can be viewed with most workstation editors.

Parameters: If you do not specify an output file name, the output is placed in the file `pd_hostname.decnet.debug`, where *hostname* is the host name of this 6611. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the output file name. If you specify an output file name, the prefix `pd_` is added to it. Specify only alphanumeric characters, periods (.), dashes (–), and underscores (_) in the output file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

decnet debug set {*trace_level*} {*trace_mask*}

Description: Set up DECnet to collecting debug information. The output is placed in the file `hostname.DEC.setup.db`, where *hostname* is the host name of the 6611. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the setup file name. When you run the **decnet debug collect** command, `hostname.DEC.setup.db` is combined with the debug collection files and placed in the output file.

This command starts the DECnet trace. The trace output is placed in the file `pd_dnarouted.log`.

Parameters: You can specify a trace level from 1 to 15. If you do not specify a trace level, the DECnet trace is started with a level of 15.

You can specify an eight digit hexadecimal trace mask. If you do not specify a trace mask, the DECnet trace is started with a trace mask of `X'FFFFFFFF'`. Use the **decnet (list) -tm** to list the valid trace mask settings.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

decnet filters (view) {-log} *interface*

Description: View the DECnet interface filters.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for DECnet.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet (list) -trace_mask {-log}

Description: List the DECnet trace mask settings.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) -interface {-log} *interface*

Description: View the DECnet route table for a given interface.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for DECnet.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) -route_info -adjacencies {-log} *start_entry number_entries*

Description: View the DECnet adjacency vector.

Parameters: The *start_entry* parameter must be in the range from 0 to 1023. The *number_entries* parameter must be in the range from 1 to 283. Each of these parameters is optional. The defaults are:

- *start_entry* = 0
- *number_entries* = 283

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) -route_info -area_cost {-log} *start_entry number_entries*

Description: View the DECnet area cost matrix.

Parameters: The *start_entry* parameter must be in the range from 0 to 63. The *number_entries* parameter must be in the range from 1 to 64. Each of these parameters is optional. The defaults are:

- *start_entry* = 0
- *number_entries* = 64

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) -route_info -area_hop {-log} *start_entry number_entries*

Description: View the DECnet area hop matrix.

Parameters: The *start_entry* parameter must be in the range from 0 to 63. The *number_entries* parameter must be in the range from 1 to 64. Each of these parameters is optional. The defaults are:

- *start_entry* = 0
- *number_entries* = 64

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) -route_info -area_minimum_cost {-log} *start_entry number_entries*

Description: View the DECnet area minimum cost vector.

Parameters: The *start_entry* parameter must be in the range from 0 to 63. The *number_entries* parameter must be in the range from 1 to 64. Each of these parameters is optional. The defaults are:

- *start_entry* = 0
- *number_entries* = 64

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) -route_info -area_minimum_hop {-log} *start_entry number_entries*

Description: View the DECnet area minimum hop vector.

Parameters: The *start_entry* parameter must be in the range from 0 to 63. The *number_entries* parameter must be in the range from 1 to 64. Each of these parameters is optional. The defaults are:

- *start_entry* = 0
- *number_entries* = 64

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) -route_info -area_output_adj {-log} *start_entry number_entries*

Description: View the DECnet area output adjacency vector.

Parameters: The *start_entry* parameter must be in the range from 0 to 63. The *number_entries* parameter must be in the range from 1 to 64. Each of these parameters is optional. The defaults are:

- *start_entry* = 0

- *number_entries* = 64

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) -route_info -area_reach {-log} *start_entry number_entries*

Description: View the DECnet area reach vector.

Parameters: The *start_entry* parameter must be in the range from 0 to 63. The *number_entries* parameter must be in the range from 1 to 64. Each of these parameters is optional. The defaults are:

- *start_entry* = 0
- *number_entries* = 64

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) -route_info -circuit {-log} *start_entry number_entries*

Description: View the DECnet circuit vector.

Parameters: The *start_entry* parameter must be in the range from 1 to 14. The *number_entries* parameter must be in the range from 1 to 14. Each of these parameters is optional. The defaults are:

- *start_entry* = 1
- *number_entries* = 14

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) -route_info -cost {-log} *start_entry number_entries start_column number_columns*

Description: View the DECnet cost matrix.

Parameters: The *start_entry* parameter must be in the range from 0 to 1023. The *number_entries* parameter must be in the range from 1 to 1024. The start_column parameter must be in the range from 0 to 46. The number_columns parameter must be in the range from 1 to 47. Each of these parameters is optional. The defaults are:

- *start_entry* = 0
- *number_entries* = 1024
- start_column = 0
- number_columns = 47

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) -route_info (-executor) {-log}

Description: View the DECnet executor data structure.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) -route_info -hop {-log} *start_entry number_entries start_column number_columns*

Description: View the DECnet hop matrix.

Parameters: The *start_entry* parameter must be in the range from 0 to 1023. The *number_entries* parameter must be in the range from 1 to 1024. The start_column parameter must be in the range from 0 to 46. The number_columns parameter must be in the range from 1 to 47. Each of these parameters is optional. The defaults are:

- *start_entry* = 0
- *number_entries* = 1024
- start_column = 0
- number_columns = 47

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) -route_info -minimum_cost {-log} *start_entry number_entries*

Description: View the DECnet minimum cost vector.

Parameters: The *start_entry* parameter must be in the range from 0 to 1023. The *number_entries* parameter must be in the range from 1 to 1024. Each of these parameters is optional. The defaults are:

- *start_entry* = 0
- *number_entries* = 1024

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) -route_info -minimum_hop {-log} *start_entry number_entries*

Description: View the DECnet minimum hop vector.

Parameters: The *start_entry* parameter must be in the range from 0 to 1023. The num_entries parameter must be in the range from 1 to 1024. Each of these parameters is optional. The defaults are:

- *start_entry* = 0
- *number_entries* = 1024

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) -route_info -output_adj {-log} *start_entry number_entries*

Description: View the DECnet output adjacency vector.

Parameters: The *start_entry* parameter must be in the range from 0 to 1023. The *number_entries* parameter must be in the range from 1 to 1024. Each of these parameters is optional. The defaults are:

- *start_entry* = 0
- *number_entries* = 1024

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) -route_info -reach {-log} *start_entry number_entries*

Description: View the DECnet reach vector.

Parameters: The *start_entry* parameter must be in the range from 0 to 1023. The *number_entries* parameter must be in the range from 1 to 1024. Each of these parameters is optional. The defaults are:

- *start_entry* = 0
- *number_entries* = 1024

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet routes (view) (-system) {-log}

Description: View the DECnet system route table.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet statistics (view) (-interface) {-log} *interface*

Description: View the DECnet network interface protocol statistics.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for DECnet.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet trace -off

Description: Stop the DECnet routing protocol trace. The debug level is set to 0.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet trace (-on) *trace_level*

Description: Start the DECnet routing protocol trace.

Parameters: Set the debug level of DECnet tracing to a number between 0 and 15. A tracing level of 0 traces only error conditions and essentially turns off the trace. Everything is traced with a debug level of 15.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet trace -timestamp_mask *timestamp_mask*

Description: Set the DECnet trace time stamp mask. The *timestamp_mask* parameter is a 32 bit number with each bit corresponding to a particular action to trace. If the bit is on, a time stamp is recorded with each trace entry when it is traced.

Parameters: Use the **decnet (list) -timestamp_mask** to list the valid timestamp masks. The *timestamp_mask* parameter is specified in hexadecimal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet trace -trace_log [-system|(-decnet)]

Description: Set the DECnet trace output to either the system log or the DECnet log. The change does not take effect until after the DECnet routing process is restarted.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

decnet trace -trace_mask *trace_mask*

Description: Set DECnet trace mask. The trace_mask is a 32 bit number with each bit corresponding to a particular action to trace. If the bit is on and the debug level of the action is less than or equal to the current debug level, the action is traced.

Parameters: Use the **decnet (list) -trace_mask** command to list the valid trace masks. The trace_mask is specified in hexadecimal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

Summary of DECnet Commands

Table 9-16 (Page 1 of 2). Summary of DECnet Commands

Command	Function
decnet connections (view) {-log} *interface*	View the DECnet interface connections.
decnet debug (collect) {-system} {-notrcstop} [(-tar)|-cat] {*output_file*}	Collect the DECnet protocol debug information.

Table 9-16 (Page 2 of 2). Summary of DECnet Commands

Command	Function
decnet debug set {*trace_level*} {*trace_mask*}	Set up the DECnet protocol for collecting debug information.
decnet filters (view) {-log} *interface*	View the DECnet interface filters.
decnet (list) -trace_mask {-log}	List DECnet trace mask settings.
decnet routes (view) -interface {-log} *interface*	View the DECnet route table for a given interface.
decnet routes (view) -route_info -adjacencies {-log} *start_entry number_entries*	View the DECnet adjacency vector.
decnet routes (view) -route_info -area_cost {-log} *start_entry number_entries*	View the DECnet area cost matrix.
decnet routes (view) -route_info -area_hop {-log} *start_entry number_entries*	View the DECnet area hop matrix.
decnet routes (view) -route_info -area_minimum_cost {-log} *start_entry number_entries*	View the DECnet area minimum cost vector.
decnet routes (view) -route_info -area_minimum_hop {-log} *start_entry number_entries*	View the DECnet area minimum hop vector.
decnet routes (view) -route_info -area_output_adj {-log} *start_entry number_entries*	View the DECnet area output adjacency vector.
decnet routes (view) -route_info -area_reach {-log} *start_entry number_entries*	View the DECnet area reach vector.
decnet routes (view) -route_info -circuit {-log} *start_entry number_entries*	View the DECnet circuit vector.
decnet routes (view) -route_info -cost {-log} *start_entry number_entries start_column number_columns*	View the DECnet cost matrix.
decnet routes (view) -route_info (-executor) {-log}	View the DECnet executor data structure.
decnet routes (view) -route_info -hop {-log} *start_entry number_entries start_column number_columns*	View the DECnet hop matrix.
decnet routes (view) -route_info -minimum_cost {-log} *start_entry number_entries*	View the DECnet minimum cost vector.
decnet routes (view) -route_info -minimum_hop {-log} *start_entry number_entries*	View the DECnet minimum hop vector.
decnet routes (view) -route_info -output_adj {-log} *start_entry number_entries*	View the DECnet output adjacency vector.
decnet routes (view) -route_info -reach {-log} *start_entry number_entries*	View the DECnet reach vector.
decnet routes (view) (-system) {-log}	View the DECnet system route table.
decnet statistics (view) (-interface) {-log} *interface*	View the DECnet network interface protocol statistics.
decnet trace -off	Stop DECnet routing protocol trace.
decnet trace (-on) *trace_level*	Start DECnet routing protocol trace.
decnet trace -timestamp_mask *timestamp_mask*	Set DECnet trace time stamp mask.
decnet trace -trace_log [-system|(-decnet)]	Set the DECnet trace output to either the system log or the DECnet
decnet trace -trace_mask *trace_mask*	Set DECnet trace mask.

Diskette Commands

Use the diskette commands to:

- Format a DOS diskette
- Format a UNIX diskette

Table 9-17. Abbreviations for Diskette Commands

Type of term	Term and Abbreviations	
Object	diskette	disk
Subobject	DOS UNIX	dos, d unix, u
Action	format	for, f
Option	-high -low	-hi, -h -lo, -l

diskette dos format (-high)

Description: Format a high density DOS diskette.

Parameters: None

Authorization: Controlling and viewing users

System Environment: Fast-path only

diskette dos format -low

Description: Format a low density DOS diskette.

Parameters: None

Authorization: Controlling and viewing users

System Environment: Fast-path only

diskette (unix) format (-high)

Description: Format a high density UNIX diskette.

Parameters: None

Authorization: Controlling and viewing users

System Environment: Fast-path only

diskette (unix) format -low

Description: Format a low density UNIX diskette.

Parameters: None

Authorization: Controlling and viewing users

System Environment: Fast-path only

Summary of Diskette Commands

Table 9-18. Summary of Diskette Commands

Command	Function
diskette dos format (-high)	Format a high density DOS diskette.
diskette dos format -low	Format a low density DOS diskette.
diskette (unix) format (-high)	Format a high density UNIX diskette.
diskette (unix) format -low	Format a low density UNIX diskette.

DLSw Commands

Use the data link switching (DLSw) commands to:

- Dump DLSw
- List DLSw trace IDs, semaphore numbers, message queue numbers, and general database members
- Start or stop tracing DLSw
- Format DLSw trace reports
- Start, stop, or restart the DLSw protocol
- View DLSw partners
- View some DLSw specific debug information
- Set up DLSw for debug collection
- Collect DLSw debug information
- Set or view the DLSw circuit pacing value
- Set or view the NetBIOS negative cache option
- Set or view the TCP delay option

Table 9-19. Abbreviations for DLSw Commands

Type of term	Term and Abbreviations	
Object	DLSw	dlsw, dls, d
Subobject	debug	db
	partners	partner, part, p
Action	collect	col, c
	dump	du
	list	l
	restart	res
	set	s
	start	begin, b
	stop	end, e
	trace	tr, t
	view	v
Option	-cat	-c
	-circuit_pacing	-cp
	-conversation_database	-con, -cd, -c
	-format	-for, -f
	-general_database	-gen, -gd, -g
	-log	-l
	-message_buffer	-msgb, -mb
	-message_queue	-msgq, -mq
	-negative_cache	-nc
	-notrcstop	-nts, -no
	-off	
	-on	
	-tar	-t
	-tcp_delay	-td
	-semaphore	-sem
	-summary	-sum
	-system	-sys, -s
	-trace_ID	-ti, -tid, -id
	-trace_log	-tl
	-trace_parameters	-tp

dlsw debug (collect) {-system} {-notrcstop} [(-tar)|-cat] {*output_file*}

Description: Collect DLSw debug information. Specify the -system option to collect additional system debug information. Specify the -notrcstop option to keep the DLSw trace running while while collecting other debug information.

This command creates several output files in the transfer directory. These output files are combined into one file to facilitate the transfer from the 6611 to a remote host.

Specify the -tar option to archive the individual files to a binary file specified by *output_file*. Transfer the *output_file* to an AIX or UNIX workstation using the binary mode of ftp. Use the **tar -xvf** *output_file* command to restore the individual files. The individual files can be viewed with most workstation editors.

Specify the -cat option to combine the individual files into an ASCII file specified by *output_file*. Transfer the *output_file* to any workstation using the ASCII mode of ftp. The *output_file* can be viewed with most workstation editors.

Parameters: If you do not specify an output file name, the output is placed in the transfer directory with the file name `pd_hostname.dls.debug`, where *hostname* is the host name of this 6611. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the output file name. If you specify an output file name, the prefix `pd_` is added to it. Specify only alphanumeric characters, periods (.), dashes (–), and underscores (_) in the output file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

dlsw debug set {*trace_IDs*}

Description: Set up DLSw for collecting debug information. The output is placed in the file `hostname.DLSW.setup.db`, where *hostname* is the host name of the 6611. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the setup file name. When you run the **dlsw debug collect** command, `hostname.DLSW.setup.db` is combined with the debug collection files and placed in the output file.

This command also starts the DLSw trace. The DLSw trace is integrated with the system trace. The trace output is placed in the file `hostname.DLSW.trcfile`, where *hostname* is the host name of the 6611.

Parameters: The DLSw trace is started with the default trace IDs 001, 002, 106, 10C, 134, 139, and 362. Any additional trace IDs must be specified as three digit uppercase hexadecimal numbers. Use the **dlsw (list) -ti** command to list the valid trace IDs. Use the **dlsw (list) -tp** command to list the subset of valid trace IDs that are specific to DLSw.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

dlsw debug (view) -conversation_database {-log}

Description: View the DLSw conversation database.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

dlsw debug (view) -general_database {-log} *gen_db_num*

Description: View the specified object from the DLSw general database.

Parameters: Use the **dlsw (list) -general_database** command to list the valid general database numbers. Specify only the number.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

dlsw debug (view) -general_database (-summary) {-log}

Description: View a summary of the information in the DLSw general database.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

dlsw debug (view) -message_buffer {-log}

Description: View the DLSw message buffers.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

dlsw debug (view) -message_queue {-log} *msg_que_num*

Description: View the specified DLSw message queue.

Parameters: Use the **dlsw (list) -message_queue** command to list the valid message queue numbers. Specify only the number.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

dlsw debug (view) -semaphore {-log} *semaphore_num*

Description: View the specified DLSw semaphore.

Parameters: Use the **dlsw (list) -semaphore** command to list the valid semaphore numbers. Specify only the number.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

dlsw dump

Description: Dump DLSw nondisruptively. The dump is placed in pd_dls.dump in the transfer directory.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

dlsw (list) -general_database {-log}

Description: List the valid DLSw general database numbers.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

dlsw (list) -message_queue {-log}

Description: List the valid DLSw message queue numbers.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

dlsw (list) -semaphore {-log}

Description: List the valid DLSw semaphore numbers.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

dlsw (list) -trace_ID {-log}

Description: List the valid DLSw trace IDs.

The DLSw trace is integrated with the system trace. These are the trace IDs that are common for all traces based on the system trace.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

dlsw (list) -trace_parameters {-log}

Description: List the subset of trace IDs specific to DLSw.

The DLSw trace is integrated with the system trace. These are the system trace IDs that are specific to DLSw.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

dlsw partners (view) {-log}

Description: View the DLSw partners.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

dlsw restart

Description: Restart the DLSw protocol.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

dlsw set -circuit_pacing *pacing_value*

Description: Set the DLSw circuit pacing value. This value limits the number of packets from a single circuit that DLSw will queue before sending a busy signal to the sender.

Circuit pacing is useful when applications that do not use fixed end-to-end pacing transfer large files across a relatively slow WAN. If DLSw circuit pacing is not used, the bulk data may build up on the transmit queue, interfering with interactive traffic. If you specify a relatively small pacing value, bulk data will be intermixed with other DLSw traffic.

Parameters: Specify a number between 2 and 49 for the *pacing_value* parameter. Specify a zero (0) for the *pacing_value* parameter to discontinue DLSw circuit pacing.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

dlsw set -negative_cache [(-on)|-off]

Description: Set the DLSw NetBIOS negative caching either on or off.

DLSw creates an entry in cache memory at the beginning of each NetBIOS session. If no frames are received from a destination node for a period of time, known as the destination cache timeout, DLSw purges the entry from cache memory, ending the NetBIOS session. (You can set the destination cache timeout with the Configuration Program.) If DLSw negative cache is turned on, DLSw will not set up a new NetBIOS session with that destination for a period of time equal to the destination cache timeout. If DLSw negative cache is turned off, DLSw will begin a new NetBIOS session as soon as the destination resumes active communications.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

dlsw set -tcp_delay [(-on)|-off]

Description: Set the DLSw TCP delay either on or off.

If you set the TCP delay parameter to **on**, the 6611 will delay transmitting one or more DLSw frames until TCP can send multiple frames as a single TCP segment, increasing the link utilization in heavy traffic conditions. If you set the TCP delay parameter to **off**, the 6611 will transmit all DLSw frames immediately, lowering the effective link utilization.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

dlsw start

Description: Start the DLSw protocol.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

dlsw stop

Description: Stop the DLSw protocol.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

dlsw trace -format

Description: Format the DLSw trace. The DLSw trace is integrated with the system trace. The trace output is placed in the transfer directory as `pd_dls_trc`.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

dlsw trace -off

Description: Stop the DLSw trace. The DLSw trace is integrated with the system trace.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

dlsw trace (-on) {-trace_log} {*trace_log_size*} {*trace_IDs*}

Description: Start the DLSw trace. The DLSw trace is integrated with the system trace.

To stop the trace, use the **dlsw trace -off** command. To format the trace, use the **dlsw trace -format** command. The output is placed in the transfer directory as pd_dls_trc.

Parameters: If you specify the -trace_log option, the trace_log_size parameter must be specified and must precede the trace_IDs. The trace_log_size is between 1048576 and 10485760 bytes with a default of 1048576 bytes.

The trace is started with the global trace IDs of 001, 002, 106, 10C, 134, and 139, and with the DLSw trace ID 362. Any additional trace IDs must be specified as three digit uppercase hexadecimal numbers. Use the **dlsw (list) -trace_ID** command to list the valid trace IDs. Use the **dlsw (list) -trace_parameters** command to list the subset of trace IDs specifically related to DLSw.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

dlsw view -circuit_pacing

Description: Display the DLSw circuit pacing value.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

dlsw view -negative_cache

Description: Display the setting for DLSw negative caching.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

dlsw view -tcp_delay

Description: Display the setting for DLSw TCP delay.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

Summary of DLSw Commands

Table 9-20. Summary of DLSw Commands

Command	Function
dlsw debug (collect) {-system} {-notrcstop} [(-tar)|-cat] *output_file*	Collect the DLSw protocol debug information.
dlsw debug set {*trace_IDs*}	Set up the DLSw protocol for collecting debug information.
dlsw debug (view) -conversation_database {-log}	View the DLSw conversation database.
dlsw debug (view) -general_database {-log} *gen_db_num*	View the specified object from the DLSw general database.
dlsw debug (view) -general_database (-summary) {-log}	View a summary of the information in the DLSw general database.
dlsw debug (view) -message_buffer {-log}	View the DLSw message buffers.
dlsw debug (view) -message_queue {-log} *msg_que_num*	View the specified DLSw message queue.
dlsw debug (view) -semaphore {-log} *semaphore_num*	View the specified DLSw semaphore.
dlsw dump	Dump DLSw nondisruptively.
dlsw (list) -general_database {-log}	List the valid DLSw general database numbers.
dlsw (list) -message_queue {-log}	List the valid DLSw message queue numbers.
dlsw (list) -semaphore {-log}	List the valid DLSw semaphore numbers.
dlsw (list) -trace_ID {-log}	List the system trace IDs.
dlsw (list) -trace_parameters {-log}	List the DLSw trace IDs.
dlsw partners (view) {-log}	View the DLSw partners.
dlsw restart	Restart the DLSw protocol.
dlsw set -circuit_pacing *pacing_value*	Set the DLSw circuit pacing value.
dlsw set -negative_cache [(-on)|-off]	Turn NetBIOS negative caching on or off.
dlsw set -tcp_delay [(-on)|-off]	Turn TCP delay on or off.
dlsw start	Start the DLSw protocol.
dlsw stop	Stop the DLSw protocol.
dlsw trace -format	Format the DLSw trace.
dlsw trace -off	Stop the DLSw trace.
dlsw trace (-on) {-trace_log} {*trace_log_size*} {*trace_IDs*}	Start the DLSw trace.
dlsw view -circuit_pacing	View the DLSw circuit pacing value.
dlsw view -negative_cache	View the setting of the NetBIOS negative cache option.
dlsw view -tcp_delay	View the setting of the TCP delay option.

Errorlog (Error) Commands

Use the error commands to:

- Clear the error log
- Generate a customized error report
- List the valid error IDs, hardware and software resources, and sequence numbers
- Transfer the error log to the transfer directory

Table 9-21. Abbreviations for Errorlog Commands

Type of term	Term and Abbreviations	
Object	errorlog	error, err, e
Action	clear	clr, c
	list	l
	report	rep, rpt, r
	transfer	trans, tf, t
Option	-continuous	-con, -c
	-detail	-det, -d
	-error_ID	-eid, -ei, -id, -e
	-error_log	-el
	-hardware	-hw
	-hw_resource	-hwrsc, -hr
	-log	-l
	-operator	-op
	-sequence_number	-seq, -sn
	-software	-sw
	-summary	-sum, -s
	-sw_resource	-swrsc, -sr

error clear {*number_of_days*}

Description: Delete all entries from the error log that are older than the number of days specified with the *number_of_days* parameter.

Parameters: Specify a whole number greater than zero for the *number_of_days* parameter. If you specify zero or do not specify the *number_of_days* parameter, the entire error log is cleared.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

error clear -error_ID *error_ID* {*number_of_days*}

Description: Delete entries with a specific error ID from the error log.

If you do not specify the *number_of_days* parameter, all entries with a specific error ID are deleted from the error log. If you specify the *number_of_days* parameter, only the entries with a specific error ID that are older than the specific number of days are deleted from the error log.

Parameters: Use the **error list -error_ID** command to list the valid error IDs. Specify a positive, whole number greater than zero for the *number_of_days* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

error clear -hardware {*number_of_days*}

Description: Delete hardware entries from the error log.

If you do not specify the *number_of_days* parameter, all hardware entries are deleted from the error log. If you specify the *number_of_days* parameter, only the hardware entries that are older than the specific number of days are deleted from the error log.

Parameters: Specify a positive, whole number greater than zero for the *number_of_days* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

error clear -hw_resource *hw_resource* {*number_of_days*}

Description: Delete hardware entries pertaining to a hardware resource specified with the *hw_resource* parameter.

If you do not specify the *number_of_days* parameter, all hardware entries pertaining to a specific hardware resource are deleted from the error log. If you specify the *number_of_days* parameter, only the hardware entries pertaining to a specific hardware resource that are older than the specific number of days are deleted from the error log.

Parameters: Use the **error list -hw_resource** command to list the hardware resources currently in the error report. Specify a positive, whole number greater than zero for the *number_of_days* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

error clear -operator {*number_of_days*}

Description: Delete operator entries in from the error log.

If you do not specify the *number_of_days* parameter, all operator entries are deleted from the error log. If you specify the *number_of_days* parameter, only the operator entries that are older than the specific number of days are deleted from the error log.

Parameters: Specify a positive, whole number greater than zero for the *number_of_days* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

error clear -software {*number_of_days*}

Description: Delete software entries from the error log.

If you do not specify the *number_of_days* parameter, all software entries are deleted from the error log. If you specify the *number_of_days* parameter, only the software entries that are older than the specific number of days are deleted from the error log.

Parameters: Specify a positive, whole number greater than zero for the *number_of_days* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

error clear -sw_resource *sw_resource* {*number_of_days*}

Description: Delete software entries pertaining to a software resource specified with the *sw_resource* parameter.

If you do not specify the *number_of_days* parameter, all software entries pertaining to a specific software resource are deleted from the error log. If you specify the *number_of_days* parameter, only the software entries pertaining to a specific software resource that are older than the specific number of days are deleted from the error log.

Parameters: Use the **error list -sw_resource** command to list the software resources currently in the error report. Specify a positive, whole number greater than zero for the *number_of_days* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

error list (-error_ID) {-log}

Description: List the error IDs in the error report.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

error list -hw_resource {-log}

Description: List the hardware resources names in the error report.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

error list -sequence_number {-log}

Description: List the sequence numbers in the error report.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

error list -sw_resource {-log}

Description: List the software resource names in the error report.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

error (report) -continuous

Description: Generate a continuous summary report of all errors. Lines are displayed immediately on the screen as errors are logged. Press **Ctrl+C** to end the display.

Parameters: None

Authorization: Controlling and viewing users

System Environment: Fast-path only

error (report) [-detaill-summary] {*start_date*} {*end_date*}

Description: Generate a summary or detailed error report for all errors. The output is sent to the transfer directory as pd_error.report.

Parameters: If a start date is specified, error records with earlier time stamps are excluded from the report. If an end date is specified, error records with later time stamps are excluded from the report. If dates are not specified, error records are not excluded from the report. The start date and end date format is MMDDhhmmYY.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

error (report) -error_ID [-detaill-summary] *error_ID* {*start_date*} {*end_date*}

Description: Generate a summary or detailed error report for errors with the given error ID. The output is sent to the transfer directory as pd_error.report.

Parameters: If a start date is specified, error records with earlier time stamps are excluded from the report. If an end date is specified, error records with later time stamps are excluded from the report. If dates are not specified, error records are not excluded from the report. The start date and end date format is MMDDhhmmYY.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

error (report) -hardware [-detaill-summary] {*start_date*} {*end_date*}

Description: Generate a summary or detailed error report for all hardware errors. The output is sent to the transfer directory as pd_error.report.

Parameters: If a start date is specified, error records with earlier time stamps are excluded from the report. If an end date is specified, error records with later time stamps are excluded from the report. If no dates are specified, no error records are excluded from the report. The start date and end date format is MMDDhhmmYY.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

error (report) -hw_resource [-detaill-summary] *hw_resource* **{***start_date***} {***end_date***}**

Description: Generate a summary or detailed error report for hardware errors for the specified resource. The output is sent the transfer directory as pd_error.report.

Parameters: If a start date is specified, error records with earlier time stamps are excluded from the report. If an end date is specified, error records with later time stamps are excluded from the report. If no dates are specified, no error records are excluded from the report. The start date and end date format is MMDDhhmmYY.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

error (report) -operator [-detaill-summary] {*start_date***} {***end_date***}**

Description: Generate a summary or detailed error report for all operator errors. The output is sent to the transfer directory as pd_error.report.

Parameters: If a start date is specified, error records with earlier time stamps are excluded from the report. If an end date is specified, error records with later time stamps are excluded from the report. If no dates are specified, no error records are excluded from the report. The start date and end date format is MMDDhhmmYY.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

error (report) -sequence_number {-log} *sequence_number*

Description: Generate an error report for a given sequence number.

Parameters: Use the **error list -seq** command for the sequence_number parameter.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

error (report) -software [-detaill-summary] {*start_date***} {***end_date***}**

Description: Generate a summary or detailed error report for all software errors. The output is sent to the transfer directory as pd_error.report.

Parameters: If a start date is specified, error records with earlier time stamps are excluded from the report. If an end date is specified, error records with later time stamps are excluded from the report. If no dates are specified, no error records are excluded from the report. The start date and end date format is MMDDhhmmYY.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

error (report) -sw_resource [-detaill-summary] *sw_resource* {*start_date*} {*end_date*}

Description: Generate a summary or detailed error report for software errors for the specified resource. The output is sent to the transfer directory as pd_error.report.

Parameters: If a start date is specified, error records with earlier time stamps are excluded from the report. If an end date is specified, error records with later time stamps are excluded from the report. If no dates are specified, no error records are excluded from the report. The start date and end date format is MMDDhhmmYY.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

error transfer (-error_log)

Description: Transfer a copy of the error log to the transfer directory. The error log is placed in the transfer directory as pd_error.log.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

Summary of Error Commands

Table 9-22 (Page 1 of 2). Summary of Error Commands

Command	Function
error clear {*number_of_days*}	Delete all entries from the error log older than the given number of days.
error clear -error_ID *error_ID* {*number_of_days*}	Delete entries with specified error IDs from the error log.
error clear -hardware {*number_of_days*}	Delete hardware entries from the error log.
error clear -hw_resource *hw_resource* {*number_of_days*}	Delete hardware entries for the specified hardware resource from the error log.
error clear -operator {*number_of_days*}	Delete operator entries from the error log.
error clear -software {*number_of_days*}	Delete software entries from the error log.
error clear -sw_resource *sw_resource* {*number_of_days*}	Delete software entries for the specified software resource from the error log.
error list (-error_ID) {-log}	List the error IDs in the error report.
error list -hw_resource {-log}	List the hardware resources names in the error report.

Table 9-22 (Page 2 of 2). Summary of Error Commands

Command	Function
error list -sequence_number {-log}	List the sequence numbers in the error report.
error list -sw_resource {-log}	List the software resource names in the error report.
error (report) -continuous	Generate a continuous summary report of all errors.
error (report) [-detaill-summary] {*start_date*} {*end_date*}	Generate a summary or detailed error report for all errors.
error (report) -error_ID [-detaill-summary] *error_ID* {*start_date*} {*end_date*}	Generate a summary or detailed error report for errors with the given error ID.
error (report) -hardware [-detaill-summary] {*start_date*} {*end_date*}	Generate a summary or detailed error report for all hardware errors.
error (report) -hw_resource [-detaill-summary] *hw_resource* {*start_date*} {*end_date*}	Generate a summary or detailed error report for hardware errors for the specified resource.
error (report) -operator [-detaill-summary] {*start_date*} {*end_date*}	Generate a summary or detailed error report for all operator errors.
error (report) -sequence_number {-log} *sequence_number*	Generate an error report for a given sequence number.
error (report) -software [-detaill-summary] {*start_date*} }*end_date*}	Generate a summary or detailed error report for all software errors.
error (report) -sw_resource [-detaill-summary] *sw_resource* {*start_date*} {*end_date*}	Generate a summary or detailed error report for software errors for the specified resource.
error transfer (-error_log)	Transfer a copy of the error log to the transfer directory.

Files Commands

Use the files commands to:

- List the files in the transfer or static directory
- View a file in the transfer or static directory
- Send a file from the transfer or static directory to a remote node or place it on a diskette
- Issue a checksum against a file in the transfer or static directory to be assured that it was transferred correctly to the remote node
- Receive a file into the transfer directory from a remote node or from a diskette
- Delete, rename, compare, compress, and uncompress files in the transfer directory
- Scan a file or all files in the transfer directory for a certain pattern
- List files on a diskette
- View the space used by the various file systems
- Execute a special file, supplied by IBM service, in the transfer directory

Table 9-23. Abbreviations for Files Commands

Type of term	Term and Abbreviations	
Object	files	file, f
Subobject	diskette	disk, d
	static	st
	system	systems, sys, s
	transfer	trans, t
Action	checksum	chk, cs, sum
	compare	comp, com
	compress	c
	delete	del, d
	exec	ex, e
	list	l
	receive	rec, rcv, r
	rename	ren
	scan	sc
	send	s
	uncompress	unc, u
	view	v
Option	-all	
	-append	-app, -a
	-create	-cre, -c
	-DOS	-dos, -d
	-ftp	-f
	-modem	-mod, -m
	-UNIX	-unix, -u

files diskette (list) -dos {-log}

Description: List files on a DOS diskette.

Parameters: None

Authorization: Controlling and viewing users

System Environment: Fast-path only

files diskette (list) -unix {-log}

Description: List files on a UNIX diskette.

Parameters: None

Authorization: Controlling and viewing users

System Environment: Fast-path only

files static checksum {-log} *file_name*

Description: Issue a checksum to a file in the static directory.

Parameters: Use the **files static (list)** command to list the files in the static directory.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

files static (list) {-log}

Description: List all files in the static directory.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

files static send -dos *file_name DOS_file_name*

Description: Send a static directory file to a DOS diskette.

Parameters: Use the **files static (list)** command to list the files in the static directory.

Specify a file name on the DOS diskette for the DOS file name parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

files static send (-ftp) *host_name*

Description: Send a static directory file to a remote host using FTP. This is an interactive session. You are prompted for the user ID and password at the remote host and the static directory file name.

Parameters: The host IP address can be used in place of the destination host name, if the name is not known. Use the **files static (list)** command to list the files in the static directory.

Authorization: Controlling and viewing users

System Environment: Fast-path only

files static send -modem *file_name*

Description: Send a static directory file to a remote host over a modem.

Parameters: Use the **files static (list)** command to list the files in the static directory.

Authorization: Controlling and viewing users

System Environment: Fast-path only

files static send -unix (-append) *file_name*

Description: Send a static directory file to an existing UNIX diskette.

Parameters: Use the **files static (list)** command to list the files in the static directory.

Authorization: Controlling and viewing users

System Environment: Fast-path only

files static send -unix -create *file_name*

Description: Send a static directory file to a new UNIX diskette.

Parameters: Use the **files static (list)** command to list the files in the static directory.

Authorization: Controlling and viewing users

System Environment: Fast-path only

files static view *file_name*

Description: View a file in the static directory.

Parameters: Use the **files static (list)** command to list the files in the static directory.

Authorization: Controlling and viewing users

System Environment: Fast-path only

files system (view) {-log}

Description: View the used and available space on the 6611 file systems.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

files (transfer) checksum {-log} *file_name*

Description: Issue a checksum to a file in the transfer directory.

Parameters: Use the **files (transfer) list** command to list the files in the transfer directory.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

files (transfer) compare {-log} *file_name file_name*

Description: Compare two transfer directory files.

Parameters: Use the **files (transfer) list** command to list the files in the transfer directory.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

files (transfer) compress *file_name*

Description: Compress a file in the transfer directory. The compressed file is stored in the transfer directory as `file_name.Z`.

Parameters: Use the **files (transfer) list** command to list the files in the transfer directory. Only those files without the .Z extension can be compressed.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

files (transfer) delete *file_name*

Description: Delete a file from the transfer directory.

Parameters: Use the **files (transfer) list** command to list the files in the transfer directory.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

files (transfer) delete -all

Description: Delete files from the transfer directory. See Table 4-4 on page 4-64 for a list of the files that will be removed.

Note: Deleting these files in the transfer directory may result in the loss of needed problem determination output.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

files (transfer) exec *file_name* {*program_parameters*}

Description: Execute a special file in the transfer directory.

Parameters: The *file_name* must be a special file given to you by IBM service.

The *program_parameters* are determined by the requirements of the special file.

Note: This function cannot be used on user-written files.

Authorization: Controlling users only

System Environment: Fast-path only

files (transfer) list {-log}

Description: List all files in the transfer directory.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

files (transfer) receive -dos *DOS_file_name new_file_name*

Description: Receive a file from a DOS diskette.

Parameters: Use the **files diskette (list) -dos** command to list the files on the DOS diskette.

Specify the file name to receive the DOS diskette file.

Authorization: Controlling and viewing users

System Environment: Fast-path only

files (transfer) receive (-ftp) *host_name*

Description: Receive a file from a remote host using FTP. This is an interactive session. You are prompted for the user ID, password, and file name at the remote host.

Parameters: The host's IP address can be used in place of the host name, if the name is not known.

Authorization: Controlling and viewing users

System Environment: Fast-path only

files (transfer) receive -modem *file_name*

Description: Receive a file to a remote host over a modem.

Parameters: The file specified must be in the local directory of the remote host.

Authorization: Controlling and viewing users

System Environment: Fast-path only

files (transfer) receive -unix *file_name*

Description: Receive a file from a UNIX diskette.

Parameters: Use the **files diskette (list) -unix** command to list the files on the UNIX diskette.

Authorization: Controlling and viewing users

System Environment: Fast-path only

files (transfer) receive -unix -all

Description: Receive all files on a UNIX diskette.

Parameters: None

Authorization: Controlling and viewing users

System Environment: Fast-path only

files (transfer) rename *file_name new_file_name*

Description: Rename a file in the transfer directory.

Parameters: Use the **files (transfer) list** command to list the files in the transfer directory.

Specify the new file name for the file.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

files (transfer) scan -all {-log} *pattern*

Description: Scan all files in the transfer directory for a given pattern and display the lines containing the pattern.

Parameters: Specify the search pattern. The pattern can be any search string.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

files (transfer) scan {-log} *pattern file_names*

Description: Scan specific files in the transfer directory for a given pattern and display the lines containing the pattern.

Parameters: Use the **files (transfer) list** command to list the files in the transfer directory.

Specify the search pattern. The pattern can be any search string.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

files (transfer) send -dos *file_name DOS_file_name*

Description: Send a (transfer) directory file to a DOS diskette.

Parameters: Use the **files (transfer) list** command to list the files in the transfer directory.

Specify a file name on the DOS diskette for the DOS file name parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

files (transfer) send (-ftp) *host_name*

Description: Send a transfer directory file to a remote host using FTP. This is an interactive session. You are prompted for the user ID and password at the remote host and the transfer directory file name.

Parameters: The host's IP address can be used in place of the host name, if the name is not known. Use the **files (transfer) list** command to list the files in the transfer directory.

Authorization: Controlling and viewing users

System Environment: Fast-path only

files (transfer) send -modem *file_name*

Description: Send a transfer directory file to a remote host over a modem.

Parameters: Use the **files (transfer) list** command to list the files in the transfer directory.

Authorization: Controlling and viewing users

System Environment: Fast-path only

files (transfer) send -unix (-append) *file_name*

Description: Send a transfer directory file to an existing UNIX diskette.

Parameters: Use the **files (transfer) list** command to list the files in the transfer directory.

Authorization: Controlling and viewing users

System Environment: Fast-path only

files (transfer) send -unix -create *file_name*

Description: Send a transfer directory file to a new UNIX diskette.

Parameters: Use the **files (transfer) list** command to list the files in the transfer directory.

Authorization: Controlling and viewing users

System Environment: Fast-path only

files (transfer) uncompress *file_name*

Description: Uncompress a file in the transfer directory.

Parameters: Use the **files (transfer) list** command to list the files in the transfer directory. Only those files with the .Z extension can be uncompressed.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

files (transfer) view *file_name*

Description: View a file in the transfer directory.

Parameters: Use the **files (transfer) list** command to list the files in the transfer directory.

Authorization: Controlling and viewing users

System Environment: Fast-path only

Summary of Files Commands

Table 9-24 (Page 1 of 2). Summary of Files Commands

Command	Function
files diskette (list) -dos {-log}	List files on a DOS diskette.
files diskette (list) -unix {-log}	List files on a UNIX diskette.
files static checksum {-log} *file_name*	Issue a checksum to a file in the static directory.
files static (list) {-log}	List all files in the static directory.
files static send -dos *file_name DOS_file_name*	Send a static directory file to a DOS diskette.
files static send (-ftp) *host_name*	Send a static directory file to a remote host using ftp.
files static send -modem *file_name*	Send a static directory file to a remote host over a modem.
files static send -unix (-append) *file_name*	Send a static directory file to an existing UNIX diskette.
files static send -unix -create *file_name*	Send a static directory file to a new UNIX diskette.
files static view *file_name*	View a file in the static directory.
files system (view) {-log}	View the used and available space on the 6611 filesystems.
files (transfer) checksum {-log} *file_name*	Issue a checksum to a file in the transfer directory.
files (transfer) compare {-log} *file_name file_name*	Compare two files in the transfer directory.
files (transfer) compress *file_name*	Compress a file in the transfer directory.
files (transfer) delete *file_name*	Delete a file from the transfer directory.
files (transfer) delete -all	Delete files from the transfer directory.
files (transfer) exec *file_name {program_parameters}*	Execute a special file in the transfer directory.
files (transfer) list {-log}	List all files in the transfer directory.
files (transfer) receive -dos *DOS_file_name new_file_name*	Receive a file from a DOS diskette.
files (transfer) receive (-ftp) *host_name*	Receive a file from a remote host using ftp.
files (transfer) receive -modem *file_name*	Receive a file to a remote host over a modem.
files (transfer) receive -unix *file_name*	Receive a file from a UNIX diskette.
files (transfer) receive -unix -all	Receive all files on a UNIX diskette.
files (transfer) rename *file_name new_file_name*	Rename a file in the transfer directory.
files (transfer) scan -all {-log} *pattern*	Scan all files in the transfer directory for a given pattern and echo the lines containing it.
files (transfer) scan {-log} *pattern file_names*	Scan specific files in the transfer directory for a given pattern and echo the lines containing it.
files (transfer) send -dos *file_name DOS_file_name*	Send a (transfer) directory file to a DOS diskette.

Table 9-24 (Page 2 of 2). Summary of Files Commands

Command	Function
files (transfer) send (-ftp) *host_name*	Send a transfer directory file to a remote host using ftp.
files (transfer) send -modem *file_name*	Send a transfer directory file to a remote host over a modem.
files (transfer) send -unix (-append) *file_name*	Send a transfer directory file to an existing UNIX diskette.
files (transfer) send -unix -create *file_name*	Send a transfer directory file to a new UNIX diskette.
files (transfer) uncompress *file_name*	Uncompress a file in the transfer directory.
files (transfer) view *file_name*	View a file in the transfer directory.

Framerelay Command

Use the frame relay command to collect frame-relay debug information.

Table 9-25. Abbreviations for Framerelay Command

Type of term	Term and Abbreviations	
Object	framerelay	fr
Subobject	debug	db
Action	collect	col, c
Option	-cat	-c
	-system	-sys, -s
	-tar	-t

framerelay debug (collect) {-system} [(-tar)|-cat] {interface} {*output_file*}

Description: Collect frame-relay debug information for a specific serial adapter interface or for all serial interfaces configured for frame relay. Specify the -system option to collect additional system debug information.

This command creates several output files in the transfer directory. These output files are combined into one file to facilitate the transfer from the 6611 to a remote host.

Specify the -tar option to archive the individual files to a binary file specified by *output_file*. Transfer the *output_file* to an AIX or UNIX workstation using the binary mode of ftp. Use the **tar -xvf** *output_file* command to restore the individual files. The individual files can be viewed with most workstation editors.

Specify the -cat option to combine the individual files into an ASCII file specified by *output_file*. Transfer the *output_file* to any workstation using the ASCII mode of ftp. The *output_file* can be viewed with most workstation editors.

Parameters: Use the **interface list** command to list the active interfaces. Choose only those interfaces configured for frame relay. If you do not specify an output file name, the output is placed in the file `pd_hostname.fr.intf.debug` (where `hostname` is the host name for this 6611 and `intf` is the interface name), or in the file `pd_hostname.fr.debug` for all frame relay interfaces. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the output file name. If you specify an output file name, the prefix `pd_` is added to it. Specify only alphanumeric characters, periods (.), dashes (–), and underscores (_) in the output file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

Summary of Framerelay Command

Table 9-26. Summary of Framerelay Command

Command	Function
framerelay debug (collect) {-system} [(-tar)|-cat] {interface} {*output_file*}	Collect frame-relay debug information.

Hardware Commands

Use the hardware commands to:

- List the supported, defined, and installed devices
- List the devices that are testable (those that have hardware diagnostics)
- Update the hardware vital product data (VPD) after configuration changes
- View hardware vital product data
- List the devices for which detailed characteristics can be viewed
- View the detailed characteristics of a defined device
- Test a specified hardware device
- View the type of adapter in a slot
- View or update the serial or model number.

Table 9-27. Abbreviations for Hardware Commands

Type of term	Term and Abbreviations	
Object	hardware	hw
Subobject	config	cfg, c
	device	dev, d
	model	mod, m
	serial	ser, s
	slots	slot, sl
Action	list	l
	test	t
	update	upd, u
	view	v
Option	-defined	-def, -d
	-detail	-det, -d
	-installed	-in, -i
	-log	-l
	-supported	-sup, -s
	-testable	-test, -t

hardware config (update)

Description: Update hardware VPD after configuration changes.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

hardware device (list) {-log}

Description: List the devices for which detailed characteristics can be viewed.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

hardware device test *device_name*

Description: Run a test with the specified hardware device.

Parameters: Use the **hardware (list) -testable** command to list the devices supported by the Hardware Diagnostics Facility.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

hardware device view {-log} *device_name*

Description: View the detailed characteristics of a defined device.

Parameters: Use the **hardware device (list)** command to list the devices for which detailed characteristics can be viewed.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

hardware (list) -defined {-log}

Description: List the defined devices.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

hardware (list) -installed {-log}

Description: List the installed devices.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

hardware (list) -supported {-log}

Description: List the supported devices.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

hardware (list) -testable {-log}

Description: List the devices for which diagnostics can be run.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

hardware model update *model_number*

Description: Update the hardware VPD with new model number.

Parameters: Specify 120, 125, 140, 145, 170, or 175 for the *model_number* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

hardware model (view)

Description: View model number from hardware VPD.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

hardware serial update *serial_number*

Description: Update hardware VPD with new serial number.

Parameters: The serial_number parameter has the format XX-NNNNNNN, where XX is any two-character uppercase alphanumeric string and NNNNNNN is any seven-character alphanumeric string.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

hardware serial (view)

Description: View serial number from hardware VPD.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

hardware slots {view} {-detail} {-log}

Description: View the type of adapters in each slot of the 6611. Specify the -detail option to get the in depth hardware information.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

hardware view {-log}

Description: View hardware VPD.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

Summary of Hardware Commands

Table 9-28. Summary of Hardware Commands

Command	Function
hardware config (update)	Update the hardware VPD after configuration changes.
hardware device (list) {-log}	List the devices for which detailed characteristics can be viewed.
hardware device test *device_name*	Run a test with the specified hardware device.
hardware device view {-log} *device_name*	View the detailed characteristics of a defined device.
hardware (list) -defined {-log}	List the defined devices.
hardware (list) -installed {-log}	List the installed devices.
hardware (list) -supported {-log}	List the supported devices.
hardware (list) -testable {-log}	List the devices for which diagnostics can be run.
hardware model update *model_number*	Update the hardware VPD with new model number.
hardware model (view)	View the model number from the hardware VPD.
hardware serial update *serial_number*	Update the hardware VPD with a new serial number.
hardware serial (view)	View the serial number from the hardware VPD.
hardware slots (view) {-detail} {-log}	View the type of adapter in each slot of the 6611
hardware view {-log}	View the hardware VPD.

Hostname Commands

Use the host name commands to:

- View the host name for this 6611 and change the name
- View the list of IP addresses that have been mapped to host names
- Add and delete entries from the mapping

Table 9-29. Abbreviations for Hostname Commands

Type of term	Term and Abbreviations	
Object	hostname	host, hn, h
Subobject	map	m
Action	add	a
	delete	del, d
	set	s
	view	v
Option	-log	-l

hostname map add *host_name IP_address*

Description: Add a host name and IP address pair to the mapping. You must issue the **config apply** or **config commit** command for the new host name and IP address to become part of the mapping.

Parameters: Specify up to 31 alphanumeric characters, periods (.), dashes (–), or underscores (_) for the *host_name* parameter. Specify a dotted decimal IP address for the *IP_address* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

hostname map delete *host_name*

Description: Delete a host name and IP address pair from the mapping. You must issue the **config apply** or **config commit** command for the new host name and IP address to be removed from the mapping.

Parameters: Use the **hostname map view** command to list the configured host names.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

hostname map (view) {-log}

Description: View the mapping of host names to their IP addresses.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

hostname set *host_name domain_name*

Description: Set the host name and domain name of the 6611. You must issue the **config apply** or **config commit** command for the new host name and domain name to be part of the working configuration.

Parameters: Specify up to 31 alphanumeric characters, periods (.), dashes (–), or underscores (_) for the *host_name* parameter. Specify up to 63 alphanumeric characters, periods (.), dashes (–), or underscores (_) for the *domain_name* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

hostname view

Description: View the host name and domain name of the 6611.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

Summary of Hostname Commands

Table 9-30. Summary of Hostname Commands

Command	Function
hostname map add *host_name IP_address*	Add a host name and IP address pair to the mapping.
hostname map delete *host_name*	Delete a host name and IP address pair from the mapping.
hostname map (view) {-log}	View the mapping of host names to their IP addresses.
hostname set *host_name domain_name*	Set the host name and domain name of the 6611.
hostname view	View the host name and domain name of the 6611.

Interface Commands

Use the interface commands to:

- List the interface names and adapter names for the active interfaces
- View the interface status, interface packet traffic statistics, and interface utilization statistics
- Collect interface debug information

Table 9-31. Abbreviations for Interface Commands

Type of term	Term and Abbreviations	
Object	interface	intf, i
Subobject	debug	db
	state	st
	statistics	statistic, stat, s
Action	collect	col, c
	list	l
	reinsert	rins, ri
	view	v
Option	-cat	-c
	-log	-l
	-system	-sys, -s
	-tar	-t
	-traffic	-trf
	-utilization	-util, -u

interface debug (collect) {*interface*} {-system} [(-tar)|-cat] {*output_file*}

Description: Collect debug information for a specified peer-capable adapter interface or for all peer-capable adapter interfaces. Specify the -system option to collect additional system debug information.

This command creates several output files in the transfer directory. These output files are combined into one file to facilitate the transfer from the 6611 to a remote host.

Specify the -tar option to archive the individual files to a binary file specified by *output_file*. Transfer the *output_file* to an AIX or UNIX workstation using the binary mode of ftp. Use the **tar -xvf** *output_file* command to restore the individual files. The individual files can be viewed with most workstation editors.

Specify the -cat option to combine the individual files into an ASCII file specified by *output_file*. Transfer the *output_file* to any workstation using the ASCII mode of ftp. The *output_file* can be viewed with most workstation editors.

Parameters: Use the **interface list** command to list the active adapter interfaces.

If you do not specify an output file name, the output is placed in the file `pd_hostname.intf.debug`, where *hostname* is the host name for this 6611 and *intf* is either the adapter interface name as specified with the *interface* parameter, or the word *interface* when running this command for all adapter interfaces. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the output file name. If you specify an output file name, the prefix `pd_` is added to it. Specify only alphanumeric characters, periods (.), dashes (–), and underscores (_) in the output file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path only

interface list {-log}

Description: List the interface names for the active interfaces.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

interface reinsert *interface*

Description: Reinsert a token-ring interface to the LAN.

Parameters: Use the **interface list** command to list the active interfaces. Specify only token-ring interfaces.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

interface state (view) *interface*

Description: View the state of the interface and some protocol information for some of the protocols configured for that interface.

Parameters: Use the **interface list** command to list the active interfaces. All interfaces are valid except for the mpq# interfaces.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

interface statistics (view) (-traffic) *interface number_seconds*

Description: View the interface packet traffic statistics. Press **Ctrl+C** to end the command.

Parameters: Use the **interface list** command to list the active interfaces. Only the te#, tk#, and to# interfaces are valid.

Specify a number between 1 and 5 for the *number_seconds* parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

interface statistics (view) -utilization *number_seconds* {*xt0_speed*} {*xt1_speed*} {*xt2_speed*} {*xt3_speed*}

Description: View the interface utilization statistics. The statistics are continually updated. Press **Ctrl+C** to end the command.

Parameters: Specify a number between 15 and 60 for the *number_seconds* parameter.

The *xt#_speed* parameters specify the line speeds of the configured X.25 adapters. Use the **hardware (list) -installed** command to list the configured devices. X.25 adapters will be listed as **ampx#**, where the # will match the # in the *xt#_speed* parameter. The number of xt#_speed parameters must equal the number of configured X.25 interfaces.

Authorization: Controlling users only

System Environment: Fast-path only

Summary of Interface Commands

Table 9-32. Summary of Interface Commands

Command	Function
interface debug (collect) {*interface*} {-system} [(-tar)|-cat] {*output_file*}	Collect debug information for a specified peer-capable adapter interface.
interface list {-log}	List the interface names for the active interfaces.
interface reinsert *interface*	Reinsert a token-ring interface on a LAN.
interface state (view) *interface*	View the state of the interface and some protocol information for some of the protocols configured for that interface.
interface statistics (view) (-traffic) *interface number_seconds*	View the interface packet traffic statistics.
interface statistics (view) -utilization *number_seconds* {*xt0_speed*} {*xt1_speed*} {& xt2.} {*xt3_speed*}	View the interface utilization statistics.

IP Commands

Use the IP commands to:

- Start and stop the IP trace
- List the trace parameters
- Send an echo or trace a route to an IP node
- Add and delete entries to the IP ARP table
- View the entries of the IP ARP table
- View IP routes, connections, and protocol statistics
- View filter and OSPF routing information
- Dump the IP routing protocol process
- Set up IP for debug collection
- Collect IP debug information

Table 9-33. Abbreviations for IP Commands

Type of term	Term and Abbreviations	
Object	IP	ip
Subobject	arp	a
	connections	connection, con, c
	debug	db
	filters	filter, fil, f
	OSPF	ospf, o
	routes	route, r
	statistics	statistic, stat, s
Action	add	a
	collect	col, c
	delete	d
	dump	du
	echo	e
	list	l
	set	s
	trace	tr
	view	v
Option	-all	
	-cat	-c
	-continuous	-cont, -c
	-general_info	-general, -gen, -gi, -g
	-host_name	-hn
	-hw_address	-hwa, -ha
	-information	-info
	-interface	-intf, -if, -i
	-log	-l
	-lsdb	-ls
	-neighbors	-neighbor, -nbr, -n
	-nopublish	-nop
	-notrcstop	-nts, -no
	-off	
	-on	
	-permanent	-perm
	-publish	-pub
	-route	-routes, -r
	-system	-sys, -s
	-tar	-t
	-temporary	-temp, -tmp
	-trace_log	-tl
	-trace_parameters	-tp

ip arp add [(-permanent)|-temporary] [(-nopublish)|-publish] *host_name hw_address interface*

Description: Add either a permanent or temporary IP ARP table entry to a given interface and publish it, if necessary.

Parameters: The host IP address can be used in place of the host name, if known.

The hardware address parameter is in the form:

```
xx:xx:xx:xx:xx:xx
```

where *xx* is any hexadecimal number from 00 to FF.

Use the **ip arp list (-interface)** command to list the possible IP ARP interfaces.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

ip arp delete -all *interface*

Description: Delete all IP ARP table entries on a given peer-capable interface.

Parameters: Use the **ip arp list (-interface)** to list the possible IP ARP interfaces.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

ip arp delete (-host_name) *host_name interface*

Description: Delete an IP ARP table entry from a given peer-capable interface using the host name.

Parameters: The host's IP address can be used in place of the host name, if known.

Use the **ip arp list (-interface)** command to list the possible IP ARP interfaces. Use the **ip arp (view)** *interface* command to view the entries that can be deleted.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

ip arp delete -hw_address *hw_address interface*

Description: Delete an IP ARP table entry from a given peer-capable interface using the hardware address.

Parameters: The hardware address parameter is in the form:

```
xx:xx:xx:xx:xx:xx
```

where *xx* is any hexadecimal number from 00 to FF.

Use the **ip arp list (-interface)** command to list the possible IP ARP interfaces. Use the **ip arp (view)** *interface* command to view the entries that can be deleted.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

ip arp list (-interface)

Description: List the possible IP ARP interfaces.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ip arp (view) {-log} *interface*

Description: View the IP ARP table entries on a given peer-capable interface.

Parameters: Use the **ip arp list (-interface)** command to list the possible IP ARP interfaces.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ip connections (view) -information {-log}

Description: View the IP interface connection information.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ip connections (view) {-log} *interface*

Description: View the IP interface connections.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for IP.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ip debug (collect) {-system} {-notrcstop} [(-tar)|-cat] {*output_file*}

Description: Collect IP debug information. Specify the -system option to collect additional system debug information. Specify the -notrcstop option to keep the IP trace running while collecting other debug information.

This command creates several output files in the transfer directory. These output files are combined into one file to facilitate the transfer from the 6611 to a remote host.

Specify the -tar option to archive the individual files to a binary file specified by *output_file*. Transfer the *output_file* to an AIX or UNIX workstation using the binary mode of ftp. Use the **tar -xvf** *output_file* command to restore the individual files. The individual files can be viewed with most workstation editors.

Specify the -cat option to combine the individual files into an ASCII file specified by *output_file*. Transfer the *output_file* to any workstation using the ASCII mode of ftp. The *output_file* can be viewed with most workstation editors.

Parameters: If you do not specify an output file name, the output is placed in the file `pd_hostname.ip.debug`, where *hostname* is the host name for this 6611. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the output file name. If you specify an output file name, the prefix `pd_` is added to it. Specify only alphanumeric characters, periods (.), dashes (–), and underscores (_) in the output file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

ip debug set {*trace_log_size*} {*number_trace_files*} {*trace_parameters*}

Description: Set up IP for collecting debug information. The output is placed in the file `hostname.IP.setup.db`, where *hostname* is the host name of the 6611. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the setup file name. When you run the **ip debug collect** command, `hostname.IP.setup.db` is combined with the debug collection files and placed in the output file.

The command also starts the IP trace. The trace output is placed in the file `pd_ip.trc`.

Parameters: You can select the location of the trace data, the size of the trace files and how many trace files to keep. If you DO NOT specify either the trace log size or the number of trace files, the trace output is appended to the existing trace file which is allowed to grow indefinitely. If you specify either the trace log size or the number of trace files, a new trace file is started. If the maximum number of IP trace files do not exist, the newly created file is given the name, `pd_ip.trc.#`, where # is one higher than the largest existing # at the end of an IP trace file name. If the maximum number of IP trace files do exist, the `pd_ip.trc` file is cleared and used for the current trace file. If you do not specify a trace log size, it will default to 1M. If you specify a trace log size, it must be represented in either kilobytes (K) or megabytes (M). The value of the trace log size must be at least 10K and no larger than 10M. If you do not specify the number of trace files to keep, it will default to two files. If you specify the number of trace files to keep, it must be between two and ten. If you specify a value of zero for the number of trace files to keep, a single trace file is allowed to grow indefinitely. Use the **ip (list) -tp** command to list the valid IP trace parameters. If you do not specify any trace parameters, the trace is started with the **all** parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path only

ip dump

Description: Dump the IP routing protocol. The output is sent to the transfer directory as pd_ip.dump.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

ip echo -continuous *dest_host_name* {*packet_size*} {*interval*}

Description: Issue continuous echo requests to another IP node. Press **Ctrl+C** to end the command.

Parameters: Either the IP address or host name can be specified for the *dest_host_name* parameter.

Specify 1 and 100 bytes for the *packet_size* parameter. The default is 64.

Specify 1 and 120 seconds for the *interval* parameter. The default is 2. You must specify a packet size if you want to specify an interval.

Authorization: Controlling and viewing users

System Environment: Fast-path only

ip echo {-log} *dest_host_name* {*packet_size*} {*number_echos*}

Description: Issue an echo request to another IP node.

Parameters: Either the IP address or host name can be specified for the *dest_host_name* parameter. Specify 1 and 100 bytes for the *packet_size* parameter; the default is 64. Specify 1 and 1 000 for the *number_echos* parameter; the default is 3. You must specify a packet size if you want to specify the number of echoes.

Authorization: Controlling and viewing users

System Environment: Fast-path only

ip filters (view) {-log} *interface*

Description: View the IP interface filters.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for IP.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ip (list) -trace_parameters {-log}

Description: List the IP protocol trace parameters.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ip ospf (view) {-log} [(-neighbors)|-interface|-lsdb|-general_info]

Description: View the specified OSPF routing information for this 6611 (loopback IP address). You can view OSPF neighbors, interface status, the link state database, and some general OSPF information.

Parameters: None

Authorization: Controlling and viewing users

System Environment: Fast-path only

ip ospf (view) {-log} [(-neighbors)|-interface|-lsdb|-general_info] *IP_address*

Description: View the specified OSPF routing information for the specified IP address. You can view OSPF neighbors, interface status, the link state database, and some general OSPF information.

Parameters: Specify a dotted decimal address for the *IP_address* parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

ip routes trace {-log} *dest_host_name* {*packet_size*} {*num_queries*} {*maximum_hops*} {*source_host_name*}

Description: Trace a route to another IP node.

Parameters: Each of the parameters can be defaulted, except the destination host name. The IP address can be used in place of the destination or source host name. The packet size is in bytes from 40 to 2048 with a default of 40. The number of queries is from 1 to 1000 with a default of 3. The maximum number of hops is from 2 to 100, with a default of 30. The source host name or IP address must be defined in this 6611.

Authorization: Controlling and viewing users

System Environment: Fast-path only

ip routes (view) -interface {-log} *interface*

Description: View the IP route table for a given interface.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for IP.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ip routes (view) (-system) {-log}

Description: View the system IP route table.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ip statistics (view) (-interface) {-log} *interface*

Description: View the IP network interface protocol statistics.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for IP.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ip statistics (view) -route {-log}

Description: View the IP route statistics.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ip statistics (view) -system {-log}

Description: View the TCP/IP system network protocol statistics.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ip trace -off

Description: Stop the IP protocol trace. The output is sent to the transfer directory as pd_ip.trc.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

ip trace (-on) {-trace_log} {-number_files} {*trace_log_size*} {*number_trace_files*} {*trace_parameters*}

Description: Start the IP protocol trace. You can select the location of the trace data and you can optionally select the size of the trace files and how many trace files to keep. You can also select what type of data to collect from a large number of trace parameters. The trace output can be either appended to the existing IP trace file or a new set of trace files can be started with the *trace_log_size* parameter.

Parameters: If you specify the -trace_log and -number_files options, you must also specify the corresponding trace parameters. If neither option is specified, the trace output is appended to the existing trace file, which is allowed to grow indefinitely. If either option is specified, a new trace file is started.

If the maximum number of trace files does not exist, a new trace file is created and named `pd_ip.trc.#`, where the number sign, #, is one higher than the largest existing trace file number. If the maximum number of trace files does exist, the `pd_ip.trc` file is cleared and used for the current trace file. The maximum number of IP trace files is specified with the -number_files option and the *number_trace_files* parameter. The default and minimum for the parameter is two; the maximum is 10. If a value of zero is given for the *number_trace_files* parameter, the *trace_log_size* parameter is ignored and a single trace file is allowed to grow indefinitely. The size of the trace files is given with the -trace_log option and the *trace_log_size* parameter. The size can be specified in either kilobytes (K) or megabytes (M). The default size is 1M; the range is from 10K to 10M.

The type of data to trace is specified with the *trace_parameters*.

The *trace_parameters* are the last parameters entered. Use the **ip (list) (-trace_parameters)** command to list the valid trace parameters. The default for the *trace_parameters* is *all*.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

Summary of IP Commands

Table 9-34 (Page 1 of 2). Summary of IP Commands

Command	Function
ip arp add [(-permanent)|-temporary] [(-nopublish)|-publish] *host_name hw_address interface*	Add either a permanent or temporary IP ARP table entry to a given interface and either publish it or not.
ip arp delete -all *interface*	Delete all IP ARP table entries on a given peer-capable interface.
ip arp delete (-host_name) *host_name interface*	Delete an IP ARP table entry from a given peer-capable interface using the host name.
ip arp delete -hw_address *hw_address interface*	Delete an IP ARP table entry from a given peer-capable interface using the hardware address.
ip arp list (-interface)	List the possible IP ARP interfaces.
ip arp (view) {-log} *interface*	View the IP ARP table entries on a given peer-capable interface.
ip connections (view) -information {-log}	View the IP interface connection information.
ip connections (view) {-log} *interface*	View the IP interface connections.
ip debug (collect) {-system} {-notrcstop} [(-tar)|-cat] {*output_file*}	Collect the IP protocol debug information.
ip debug set {*trace_log_size*} {*number_trace_files*} {*trace_parameters*}	Set up the IP protocol for collecting debug information.
ip dump	Dump the IP routing protocol.
ip echo -continuous *dest_host_name* {*packet_size*} {*interval*}	Issue an echo request to another IP node.
ip echo {-log} *dest_host_name* {*packet_size*} {*number_echos*}	Issue an echo request to another IP node.
ip filters (view) {-log} *interface*	View the IP interface filters.
ip (list) -trace_parameters {-log}	List the IP protocol trace parameters.
ip ospf (view) {-log} [(-neighbors)|-interface|-lsdb| -general_info]	View the specified OSPF routing information for this 6611 (loopback IP address).
ip ospf (view) {-log} [(-neighbors)|-interface|-lsdb| -general_info] *IP_address*	View the specified OSPF routing information for the specified IP address.
ip routes trace {-log} *dest_host_name* {*packet_size*} {*num_queries*} {*maximum_hops*} {*source_host_name*}	Trace a route to another IP node.
ip routes (view) -interface {-log} *interface*	View the IP route table for a given interface.
ip routes (view) (-system) {-log}	View the system IP route table.
ip statistics (view) (-interface) {-log} *interface*	View the IP network interface protocol statistics.
ip statistics (view) -route {-log}	View the IP route statistics.
ip statistics (view) -system {-log}	View the TCP/IP system network protocol statistics.

Table 9-34 (Page 2 of 2). Summary of IP Commands

Command	Function
ip trace -off	Stop the IP protocol trace.
ip trace (-on) {-trace_log} {-number_files} {*trace_log_size*} {*number_trace_files*} {*trace_parameters*}	Start the IP protocol trace.

IPX Commands

Use the IPX commands to:

- Start and stop the IPX protocol trace
- Dump the IPX protocol
- View IPX routes, connections, and protocol statistics
- View filter information
- Collect IPX debugging information

Table 9-35. Abbreviations for IPX Commands

Type of term	Term and Abbreviations	
Object	IPX	ipx
Subobject	connections	connection, con, c
	debug	db
	filters	filter, fil, f
	routes	route, r
	statistics	statistic, stat, s
Action	collect	col, c
	dump	du
	trace	tr, t
	view	v
Option	-cat	-c
	-flood	-fl, -f
	-IBM	-ibm
	-interface	-intf, -if, -i
	-log	-l
	-off	
	-on	
	-system	-sys, -s
	-tar	-t

ipx connections (view) {-log} *interface*

Description: View the IPX interface connections.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for IPX.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ipx debug (collect) {-system} [(-tar)|-cat] {*output_file*}

Description: Collect IPX debug information. Specify the -system option to collect additional system debug information.

This command creates several output files in the transfer directory. These output files are combined into one file to facilitate the transfer from the 6611 to a remote host.

Specify the -tar option to archive the individual files to a binary file specified by *output_file*. Transfer the *output_file* to an AIX or UNIX workstation using the binary mode of ftp. Use the **tar -xvf** *output_file* command to restore the individual files. The individual files can be viewed with most workstation editors.

Specify the -cat option to combine the individual files into an ASCII file specified by *output_file*. Transfer the *output_file* to any workstation using the ASCII mode of ftp. The *output_file* can be viewed with most workstation editors.

Parameters: If you do not specify an output file name, the output is placed in the file `pd_hostname.ipx.debug`, where *hostname* is the host name for this 6611. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the output file name. If you specify an output file name, the prefix `pd_` is added to it. Specify only alphanumeric characters, periods (.), dashes (–), and underscores (_) in the output file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path only

ipx dump

Description: Dump the IPX protocol. The dump is placed in the transfer directory with the file name `pd_ipxd.tables`.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

ipx echo (-IBM) {-flood} *dest_net_num dest_host_num* {*packet_size*} {*num_echoes*}

Description: Issue an echo request to another IPX node. If you specify the -flood option, the 6611 will send all the echo requests to the destination host immediately; otherwise the echo requests will be sent at the rate of one per second.

Parameters: Specify a four-byte hexadecimal number (1 to FFFFFFFE) for the *dest_net_num* parameter. Specify a six-byte hexadecimal number for the *dest_host_num* parameter. The *dest_host_num* parameter is the MAC address of the interface that connects to the destination host. Specify 1 to 100 bytes for the *packet_size* parameter; the default is 64. Specify 1 to 1000 for the *num_echoes* parameter; the default is 3. You must specify a packet size, if you want to specify the number of echoes.

System Environment Fast-path only

ipx filters (view) {-log} *interface*

Description: View the IPX interface filters.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for IPX.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ipx filters (view) {-log} -RIP

Description: View the IPX Routing Information Protocol (RIP) filters.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ipx filters (view) {-log} -SAP

Description: View the IPX Service Advertisement Protocol (SAP) filters.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ipx routes (view) -interface {-log} *interface*

Description: View the IPX route table for a given interface.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for IPX.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ipx routes (view) (-system) {-log}

Description: View the system IPX route table.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ipx statistics (view) (-interface) {-log} *interface*

Description: View the IPX network interface protocol statistics.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for IPX.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ipx statistics (view) -system {-log}

Description: View the IPX system network protocol statistics.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ipx trace -off

Description: Stop the IPX routing protocol trace. The trace output is in the transfer directory with the file names `pd_ipxd.SAP` and `pd_ipxd.RIP`.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

ipx trace (-on)

Description: Start the IPX routing protocol trace. The trace output is in the transfer directory with the file names `pd_ipxd.SAP` and `pd_ipxd.RIP`.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

Summary of IPX Commands

Table 9-36. Summary of IPX Commands

Command	Function
ipx connections (view) {-log} *interface*	View the IPX interface connections.
ipx debug (collect) {-system} [(-tar)|-cat] {*output_file*}	Collect the IPX protocol debug information.
ipx dump	Dump the IPX protocol.
ipx echo (-IBM) {-flood} *dest_net_num dest_host_num* {*packet_size*} {*num_echoes*}	Issue an echo request to an IPX host.
ipx filters (view) {-log} *interface*	View the IPX interface filters.
ipx filters (view) {-log} -RIP	View the IPX RIP filters.
ipx filters (view) {-log} -SAP	View the IPX SAP filters.
ipx routes (view) -interface {-log} *interface*	View the IPX route table for a given interface.
ipx routes (view) (-system) {-log}	View the system IPX route table.
ipx statistics (view) (-interface) {-log} *interface*	View the IPX network interface protocol statistics.
ipx statistics (view) -system {-log}	View the IPX system network protocol statistics.
ipx trace -off	Stop the IPX protocol trace.
ipx trace (-on)	Start the IPX protocol trace.

LED Commands

Use the LED commands to view the current LED display on the operator panel and the explanation of any given 3-digit LED code.

Table 9-37. Abbreviations for LED Commands

Type of term	Term and Abbreviations	
Object	LED	led, l, panel, code
Action	view	v
Option	-log	-l

LED view {-log}

Description: View the setting of the 3-digit LED display on the operator panel and give its explanation.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

LED view {-log} *LED_code*

Description: View the explanation of a given 3-digit LED code.

Parameters: A valid code for the 3-digit display.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

Summary of LED Commands

Table 9-38. Summary of LED Commands

Command	Function
LED view {-log}	View the setting of the 3-digit display on the operator's panel.
LED view {-log} *LED_code*	View the explanation of the given 3-digit LED code.

Nameserver Commands

Use the name server commands to:

- Start and stop using remote name service
- List the IP addresses of the configured remote name servers
- Add and delete remote name servers from the list

Table 9-39. Abbreviations for Nameserver Commands

Type of term	Term and Abbreviations	
Object	nameserver	name, ns
Action	add	a
	delete	del, d
	list	l
	start	begin, b
	stop	end, e
Option	-log	-l

nameserver add *IP_address*

Description: Add a host to the list of remote host name servers. You must issue the **config apply** or **config commit** command for the name server to be part of the working configuration.

Parameters: Specify the IP address of the host to be added.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

nameserver delete *IP_address*

Description: Delete a host from the list of remote host name servers. You must issue the **config apply** or **config commit** command for this name server to be removed from the working configuration.

Parameters: Specify the IP address of the host to be deleted.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

nameserver list {-log}

Description: List the IP addresses of all host name servers.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

nameserver start

Description: Allow this 6611 to use remote host name service. You must issue the **config apply** or **config commit** command for this 6611 to begin using the remote host name service.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

nameserver stop

Description: Stop this 6611 from using remote host name service. You must issue the **config apply** or **config commit** command for this 6611 to stop using the remote host name service.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

Summary of Nameserver Commands

Table 9-40. Summary of Nameserver Commands

Command	Function
nameserver add *IP_address*	Add a host to the list of remote host name servers.
nameserver delete *IP_address*	Delete a host from the list of remote host name servers.
nameserver list {-log}	List the IP addresses of all host name servers.
nameserver start	Allow this 6611 to use remote host name service.
nameserver stop	Stop this 6611 from using remote host name service.

PPP Command

Use the Point-to-Point Protocol (PPP) command to collect PPP debug information.

Table 9-41. Abbreviations for PPP Command

Type of term	Term and Abbreviations	
Object	PPP	ppp
Subobject	debug	db
Action	collect	col, c
Option	-cat	-c
	-system	-sys, -s
	-tar	-t

ppp debug (collect) {-system} [(-tar)|-cat] {*interface*} {*output_file*}

Description: Collect PPP debug information for a specific serial adapter interface or for all serial interfaces configured for PPP. Specify the -system option to collect additional system debug information.

This command creates several output files in the transfer directory. These output files are combined into one file to facilitate the transfer from the 6611 to a remote host.

Specify the -tar option to archive the individual files to a binary file specified by *output_file*. Transfer the *output_file* to an AIX or UNIX workstation using the binary mode of ftp. Use the **tar -xvf** *output_file* command to restore the individual files. The individual files can be viewed with most workstation editors.

Specify the -cat option to combine the individual files into an ASCII file specified by *output_file*. Transfer the *output_file* to any workstation using the ASCII mode of ftp. The *output_file* can be viewed with most workstation editors.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for PPP. If you do not specify an output file name, the output is placed in the file `pd_hostname.ppp.intf.debug`, where *hostname* is the host name for this 6611 and *intf* is the interface name, or in the file `pd_hostname.ppp.debug` for all PPP interfaces. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the output file name. If you specify an output file name, the prefix `pd_` is added to it. Specify only alphanumeric characters, periods (.), dashes (–), and underscores (_) in the output file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path only

Summary of PPP Command

Table 9-42. Summary of the PPP Command

Command	Function
ppp debug (collect) {-system} [(-tar)|-cat] {*interface*} {*output_file*}	Collect PPP protocol debug information.

Process Commands

Use the process commands to:

- List the active processes, the command issued to start the process, detailed information about the process, the status of the active processes, and process details sorted by protocol
- Dump any active process disruptively
- View the process table information

Table 9-43. Abbreviations for Process Commands

Type of term	Term and Abbreviations	
Object	process	proc, pro, p
Subobject	table	tab, t
Action	dump	du
	list	l
	view	v
Option	-commands	-command, -cmds, -cmd, -c
	-detail	-det, -d
	-log	-l
	-protocol	-proto, -pro, -p
	-status	-stat, -st, -s

process dump *processID*

Description: Take a disruptive core dump of the given active process. The dump is placed in the transfer directory as pd_dump.process.nnnn., where *process* is the process name and *nnnn* is the error log sequence number.

Parameters: Use the **process list** command to get the process ID parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

process list

Description: List the active processes alphabetically by process name.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

process list -commands {-log}

Description: List the commands issued to start the active processes in ascending numerical order by process ID.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

process list -detail {-log}

Description: List detailed information about the active processes alphabetically by process name.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

process list -protocol {-log}

Description: List detailed information about the active processes. The processes are listed by protocol.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

process list -status {-log}

Description: List the status of the active processes in ascending numerical order by process ID.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

process table view

Description: View the process table information.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

Summary of Process Commands

Table 9-44. Summary of Process Commands

Command	Function
process dump *processID*	Take a disruptive core dump of the given active process.
process list	List the active processes.
process list -commands {-log}	List the command issued to start the active processes.
process list -detail {-log}	List detailed information about the active processes.
process list -protocol {-log}	List detailed information about the active processes by protocol.
process list -status {-log}	List the status of the active processes.
process table view	View the process table information.

Remote Access Commands

Use the remote access commands to initiate communication with a remote host. The supported remote access commands are:

- **ftp**
- **ping**
- **rlogin**
- **telnet**

Note: The ping command deviates from the command structure of the fast-path commands in that parameters follow some of the options.

ftp *dest_host_name*

Description: Issue FTP to send or receive a file to or from a remote IP station. This is an interactive session. You are prompted for the user ID and password at the remote host. Only files in the transfer or static directories can be sent to a remote host. Files being received from a remote host are placed in the transfer directory. To send a file to a remote host that exists in the transfer directory, issue **put filename**. If it exists in the static directory, issue **lcd /tmp/hold/static** and then **put filename**. The file is placed in the home directory of the user ID at the *dest_host_name*. To receive a file from a remote host, change directories to the one containing the file you want to receive and issue **get filename**. The files are sent or received as ascii files, unless you specify them to be transferred as a binary file. Specify **bin** prior to issuing the get or put command.

Note: This command deviates from the object-orientated command structure in that:

- Parameters and options are intermixed
- Some options do not start with a dash

Parameters: Specify an IP address or host name for the *dest_host_name* parameter. An IP address is a dotted decimal number of the form *xxx.xxx.xxx.xxx*, where *xxx* can be any number from 1 to 255.

Authorization: Controlling and viewing users

System Environment: Fast-path only

ftp -c *user_id password* **put** *filename* **{asciilbin}** *dest_host_name*

Description: Issue a non-interactive FTP to send a file to a remote IP station. This type of FTP is only supported on the 6611. The file to be sent must be in the transfer directory. The file is placed in the home directory for the specified user at the remote IP station. Specify the type of file transfer as either ascii or bin.

Note: This command deviates from the object-orientated command structure in that:

- Parameters and options are intermixed
- Some options do not start with a dash

Parameters: Specify the user ID and password of a user at the remote IP station with the *user_id* and *password* parameters. Specify the IP address or host name with the *dest_host_name* parameter. The IP address is a dotted decimal number of the form *xxx.xxx.xxx.xxx*, where *xxx* can be any number from 1 to 255 Specify the file name to be sent with the *filename* parameter.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast-path.

ftp -c *user_id password* **get** *filename* **{asciilbin}** *dest_host_name*

Description: Issue a non-interactive FTP to receive a file from a remote IP station. This type of FTP is only supported on the 6611. The file to be received must be in the home directory for the specified user at the remote IP station. The file being received is placed in the transfer directory. Specify the type of file transfer as either ascii or bin.

Note: This command deviates from the object-orientated command structure in that:

- Parameters and options are intermixed
- Some options do not start with a dash

Parameters: Specify the user ID and password of a user at the remote IP station with the *user_id* and *password* parameters. Specify the IP address or host name with the *dest_host_name* parameter. The IP address is a dotted decimal number of the form *xxx.xxx.xxx.xxx*, where *xxx* can be any number from 1 to 255 Specify the file name to receive with the *filename* parameter.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast-path

ping {-d} {-n} {-q} {-r} {-v} {-R}

{-fl-i *seconds***} {-l** *number_echos***} {-s** *packet_size***}**

{-c *number_echos***} {-p** *pattern***}** *dest_host_name*

{packet_size} *{number_echos}*

Description: Test if you can reach another IP node from this 6611. The **ping** command sends an Internet Control Message Protocol (ICMP) echo_request to obtain an ICMP echo_response from a remote host. If the remote host is operational and on the network, it responds to the echo.

All the options are optional. The default is to continuously send echo requests to the destination host name (*dest_host_name*) until an interrupt is received by pressing **Ctrl+C**. The options are:

-d	Starts socket-level debugging
-n	Specifies numeric output only. No attempt is made to look up symbolic names for host addresses.
-q	Specifies quiet output. Nothing is displayed except the summary lines at startup time and when finished.
-r	Bypasses the routing tables and sends directly to a host on an attached network. If the host is not on a directly-connected network, the ping command generates an error message. Use the -r option to ping a local host through an interface that no longer has a route through it.

The IP header is only large enough for nine such routes. Be aware that many hosts ignore this option.

-v Requests verbose output, which lists ICMP packets that are received in addition to echo responses.

-R Specifies that the record_route option be included in the echo_request packet and display the route buffer on returned packets.

-f Specifies that echo_requests be flooded onto the destination host as fast as the responses are received, or 100 times per second, whichever is faster. For every echo_request sent, a . (period) is printed. For every echo_reply received, a backspace is printed. This provides a rapid display of how many packets are being dropped. Only the root user may use this option.

Note: This option can stress a network and should be used with caution. Do not ping the broadcast address unnecessarily. The -f option cannot be specified with the -i *seconds* wait option.

-i *seconds* Waits the number of seconds specified between the sending of each packet. The default is to wait for one second between each packet. This option cannot be specified with the -f option.

-l *number_echos*
Floods the number of echoes specified before falling into a normal mode of one per second.

-s *packet_size* Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data. This option may also be specified as a parameter without the -s if it follows the *dest_host_name* parameter.

-c *number_echos*
Specifies the number of echo requests to be sent and received. This option may also be specified as a parameter without the -c if it follows the *packet_size* parameter, which can follow the *dest_host_name* parameter.

If this option is not specified, you must press **Ctrl+C** to end the pinging.

-p *pattern* Specifies hexadecimal pad bytes to fill out the packet you send. This is useful for diagnosing data-dependent problems in a network.

Parameters: The host's IP address can be used in place of the destination host name. This parameter is required.

Note: The ping command deviates from the fast-path command structure in that parameters follow some of the options.

These parameters have the following recommended ranges:

-i *seconds* Integer value of 2 through 5

-l *number_echos*
Integer value of 3 through 100

-l *number_echos*
Integer value of 3 through 1000

-s *packet_size* Integer value of 0 through 100

-p *pattern* Hexadecimal value of 1 through 16 bytes

Authorization: Controlling and viewing users

System Environment: Fast-path only

rlogin *dest_host_name userID*

Description: Log in to another 6611. This initiates an interactive session. You are prompted for the password of the given user ID.

Parameters: The host's IP address can be used in place of the destination host name.

Authorization: Controlling and viewing users

System Environment: Fast-path only

telnet *dest_host_name*

Description: Log in to another IP node. This initiates an interactive session. You are prompted for a user ID and password at the remote host.

Parameters: The host's IP address can be used in place of the destination host name.

Authorization: Controlling and viewing users

System Environment: Fast-path only

Summary of the Remote Access Commands

Table 9-45. Summary of Remote Access Commands

Command	Function
ftp *dest_host_name*	Send or receive a file to or from a remote IP station.
ftp -c *user_id password* put *filename* {asciilbin} *dest_host_name*	Issue a non-interactive FTP to send a file to a remote IP station.
ftp -c *user_id password* get *filename* {asciilbin} *dest_host_name*	Issue a non-interactive FTP to receive a file from a remote IP station.
ping {-d} {-n} {-q} {-r} {-v} {-R} {-fl-i *seconds*} {-l *number_echos*} {-s *packet_size*} {-c *number_echos*} {-p *pattern*} *dest_host_name* {*packet_size*} {*number_echos*}	Test if you can reach another IP node from this 6611.
rlogin *dest_host_name userID*	Log in to another 6611.
telnet *dest_host_name*	Log in to another IP node.

Serialport Commands

Use the serial port commands to:

- Set the baud rate for the S1 or S2 serial ports
- Set up a modem connected to either the S1 or S2 serial ports by sending AT commands

Table 9-46. Abbreviations for Serialport Commands

Type of term	Term and Abbreviations	
Object	serialport	sp
Subobject	baud modem	b mod, m
Action	set	s
Option	-s1 -s2	

serialport (baud) (set) [(-s1)|-s2] *baud_rate*

Description: Set the baud rate on the S1 or S2 EIA 232 serial port. Do not issue this command if you are logged in over the serial port. You must issue the **config apply** or **config commit** command for the new baud rate to become part of the working configuration.

Parameters: The valid baud rates are 1200, 2400, 9600, 19200, and 38400.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

serialport modem (set) [(-s1)|-s2] *AT_command(s)*

Description: Set up the modem on the S1 or S2 EIA 232 serial port by sending it AT command(s). Do not issue this command if you are logged in over the serial port.

Parameters: Specify the AT commands that you want to send to the modem.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

Summary of Serialport Commands

Table 9-47. Summary of Serialport Commands

Command	Function
serialport (baud) (set) [(-s1)|-s2] *baud_rate*	Set the baud rate on S1 or S2 EIA 232 serial port.
serialport modem (set) [(-s1)|-s2] *AT_command(s)*	Set up the modem on the S1 or S2 EIA 232 serial port by sending it AT command(s).

SNMP Commands

Use the SNMP commands to:

- View the SNMP activity log
- List SNMP trace parameters
- Trace the SNMP processes
- Collect SNMP debug information

Table 9-48. Abbreviations for SNMP Commands

Type of term	Term and Abbreviations	
Object	SNMP	snmp
Subobject	debug	db
Action	collect	col, c
	list	l
	trace	tr, t
	view	v
Option	-activity_log	-act, -al, -a
	-cat	-c
	-log	-l
	-off	
	-on	
	-process	-proc, -pro, -p
	-system	-sys, -s
	-tar	-t

snmp debug (collect) {-system} [(-tar)|-cat] {*output_file*}

Description: Collect SNMP debug information. Specify the -system option to collect additional system debug information.

This command creates several output files in the transfer directory. These output files are combined into one file to facilitate the transfer from the 6611 to a remote host.

Specify the -tar option to archive the individual files to a binary file specified by *output_file*. Transfer the *output_file* to an AIX or UNIX workstation using the binary mode of ftp. Use the **tar -xvf** *output_file* command to restore the individual files. The individual files can be viewed with most workstation editors.

Specify the -cat option to combine the individual files into an ASCII file specified by *output_file*. Transfer the *output_file* to any workstation using the ASCII mode of ftp. The *output_file* can be viewed with most workstation editors.

Parameters: If you do not specify an output file name, the output is placed in the file `pd_hostname.snmp.debug`, where *hostname* is the host name for this 6611. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the output file name. If you specify an output file name, the prefix `pd_` is added to it. Specify only alphanumeric characters, periods (.), dashes (–), and underscores (_) in the output file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path only

snmp list (-process)

Description: List the SNMP process names used as parameters for the SNMP trace.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

snmp trace -off *process*

Description: Stop the SNMP trace on a specified process.

The trace output is gathered in the transfer directory in one of these files:

- pd_snmpd.log
- pd_cfgd.log
- pd_dlsd.log
- pd_pppd.log
- pd_r66d.log
- pd_rs960d.log
- pd_r960d.log
- pd_tld.log
- pd_trapd.log

Parameters: Use the **snmp list (-process)** command for the SNMP process name parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

snmp trace (-on) *process*

Description: Start the SNMP trace on a specified process.

Parameters: Use the **snmp list (-process)** command for the SNMP process name parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

snmp (view) -activity_log {-log}

Description: View the SNMP process activity log.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

Summary of SNMP Commands

Table 9-49. Summary of SNMP Commands

Command	Function
snmp debug (collect) {-system} [(-tar)|-cat] {*output_file*}	Collect SNMP debug information.
snmp list (-process)	List SNMP process names used as parameters for the SNMP trace.
snmp trace -off *process*	Stop the SNMP trace on a specified process.
snmp trace (-on) *process*	Start the SNMP trace on a specified process.
snmp (view) -activity_log {-log}	View the SNMP process activity log.

Software Commands

Use the software commands to:

- View the updates, history, product identification, and dependents
- Cancel a pending installation
- Start or stop remote installations of software updates
- Apply, commit, and reject software updates
- List software updates
- View the descriptions of the problems fixed by a software update
- List the software that exists in the transfer directory or on a diskette or tape
- Transfer installation files from a remote host
- Transfer (receive) the software from the diskette or tape to the transfer directory
- Clean up after a software installation failure
- Lock the software before selling the 6611 to a third party

Table 9-50. Abbreviations for Software Commands

Type of term	Term and Abbreviations	
Object	software	sw
Subobject	state	st
	updates	update, upd, u
Action	apply	app, a
	cancel	can
	cleanup	clnp, clup
	commit	com, c
	list	l
	lock	
	precheck	pre
	receive	rcv, rec, r
	reinstate	rein
	reject	rej
	remove	rem
	rimon	
	rinstall	rinst
	ristop	
	view	v
Option	-all	
	-commit	-com
	-com_prev	-cp
	-dependents	-dep, -d
	-diskette	-disk
	-files	-file, -f
	-fixes	-fix
	-force	
	-ftp	
	-history	-his, -h
	-log	-l
	-nocommit	-noc, -n
	-noprecheck	-nop
	-output	-out
	-prerequisites	-pre, -p
	-product_ID	-pid, -pi, -id
	-quiet	-q
	-rej_dptf	-rd
	-remote	-rem
	-tape	
	-time	
	-transfer	-trans, -tr
	-updates	-update, -upd, -u
	-verbose	-v

software cancel {-force}

Description: Cancel a pending installation of a software update.

If you do not specify the -force option and an installation phase is in progress, the installation **will not** be cancelled. If you specify the -force option, and an installation phase is in progress, the installation **will** be cancelled anyway.

Using the -force option is not recommended, and could lead to unpredictable results. If you use the -force option, you should restart the 6611 afterwards.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

software cleanup

Description: Remove all incomplete pieces of software after a failed install.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

software (list) [-diskette|-tape|-transfer] {-log}

Description: List all the software on a diskette or tape, or in the transfer directory.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

software lock

Description: Lock the Multiprotocol Network Program, when selling the 6611 to a third party.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

software receive [(-diskette)|-tape] -all

Description: Import all the software from diskette or tape to the transfer directory.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

software receive [(-diskette)|-tape] *software_name*

Description: Import the given software from diskette or tape to the transfer directory.

Parameters: The software must be either an mpnp.obj or mpnp.data software update. Use the **software (list) [-diskette|-tape]** command to see the list of software on the requested medium.

The *software_name* parameter can be:

- mpnp (the same as specifying all)
- mpnp.obj vv.rr.mmmm.ffff.ppppppp
- mpnp.data vv.rr.mmmm.ffff.ppppppp

Where:

- *vv* is the version number
- *rr* is the release number
- *mmmm* is the modification level
- *ffff* is the fix level

- *ppppppp* is the fix ID

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

software receive -ftp *host_name userID passwd software_files*

Description: Transfer the given software files from a remote host to the transfer directory using the noninteractive version of FTP.

Parameters: Specify the host name or IP address of the remote host with the *host_name* parameter. Specify the user ID and its associated password on the remote host with the *userID* and *passwd* parameters, respectively. Specify the software files to be transferred with the *software_files* parameter. The software files must reside in the home directory of the user identified with the *userID* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

software rimon *control_file_name*

Description: Start monitoring of all client 6611s listed in the remote installation control file. Press **Ctrl+C** to stop the rimon script.

Parameters: The *control_file_name* contains the instructions for the network installation process. It is an ASCII file that must reside in the transfer directory of the 6611. See "Using Control Files as Part of the Installation Process" on page 7-41 for more information on the writing and use of control files.

Authorization: Controlling and viewing users

Note: The user must know the controlling password for the client 6611 to perform the function. Specify any client 6611 password in the .netrc file. See "Using the .netrc File" on page 7-40 for more information.

System Environment: RSH, REXEC, and fast-path

software rinstall {-quiet} {-verbose} *control_file_name*

Description: Start the remote installation (from a single control point) of a software update on the multiple client 6611s specified in the control file.

The -quiet option specifies that the command is not interactive. It results in no prompting for needed information during the installation process. If you specify -quiet, and needed information is unavailable, the installation process is stopped.

The -verbose option specifies there will be full progress reporting throughout the installation procedure.

Parameters: The *control_file_name* in the transfer directory contains the instructions for the network installation process. It is an ASCII file that must reside in the transfer directory of the 6611. See "Using Control Files as Part of the Installation Process" on page 7-41 for more information on the writing and use of control files.

Authorization: Controlling and viewing users

Note: The user must know the controlling password for the client 6611 to perform the function. Specify any client 6611 password in the .netrc file. See "Using the .netrc File" on page 7-40 for more information.

System Environment: RSH, REXEC, and fast-path

software ristop *control_file_name*

Description: Stop a pending remote installation of a software update on one or multiple client 6611s involved in the installation process.

Parameters: The *control_file_name* in the transfer directory containing the instructions for the network installation process. It is an ASCII file that must reside in the transfer directory of the 6611. See "Using Control Files as Part of the Installation Process" on page 7-41 for more information on the writing and use of control files.

Authorization: Controlling and viewing users

Note: The user must know the controlling password for the client 6611 to perform the function.

System Environment: RSH, REXEC, and fast-path

software state view {-output}

Description: Display the installation state of the 6611.

Use the -output option to display the output log of the last installation phase.

See "Installation States and Phases" on page 7-41 for descriptions of the different installation phases.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

software update apply (-transfer) {-commit} {-com_prev} {-rej_dptf} {-all} {-time} {*time*} {*update_name*}

Description: Apply the software updates from the transfer directory.

Use the -commit option to immediately commit the software updates that are now being applied with this command.

Use the -com_prev option to automatically commit the PTFs that were applied, but not yet committed, before issuing this command.

Use the -rej_dptf option to automatically reject any applied development PTFs before installation. This option is ignored if you are applying only development PTFs.

Use the -time option to start the apply process at a later time. When you use the -time option, you must also use the *time* parameter.

Parameters: The *time* parameter is only used if the -time option is specified. The time to apply the update may be specified as an absolute value (whose format is MMDDhhmm{.ss}) or as a relative value (+mm) of minutes from the time at which all 6611s are prechecked.

When you do not specify the -all option, you can specify the *update_name* of the update to install. The *update_name* parameter can be:

- mpnp (the same as all)
- mpnp.obj (all updates for mpnp.obj)
- mpnp.data (all updates for mpnp.data)
- mpnp vv.rr.mmmm.ffff.ppppppp
- mpnp.obj vv.rr.mmmm.ffff.ppppppp
- mpnp.data vv.rr.mmmm.ffff.ppppppp
- mpnp ppppppp
- mpnp.obj ppppppp
- mpnp.data ppppppp

Where:

- *vv* is the version number
- *rr* is the release number
- *mmmm* is the modification level
- *ffff* is the fix level
- *ppppppp* is the fix ID

Specify the **software (list) -transfer** command to see the list of software in the transfer directory.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

software update apply (-transfer) -noprecheck {-commit} {-time} {*time*}

Description: Apply software update or updates from the transfer directory without running the update precheck.

(This is software that was previously specified with the **software update precheck** command.)

The -noprecheck option signals that no prechecking be performed. The -transfer option specifies the transfer directory as the location of the software update.

Use the -commit option to immediately commit the software updates that are now being applied with this command.

Use the -all option to apply all the updates on the medium specified.

Use the -time option to start the apply process at a later time. When you use the -time option, you must also use the *time* parameter.

Parameters: The *time* parameter is only used if the -time option is specified. The time to apply the update may be specified as an absolute value (whose format is MMDDhhmm{.ss}) or as a relative value (+mm) in minutes from the time at which all client 6611s are prechecked.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

software update commit *update_name*

Description: Commit the given software update that has been applied.

Parameters: Use the **software update list -nocommit** command to list the uncommitted updates. The *update_name* parameter can be specified as:

- mpnp.obj vv.rr.mmmm.ffff.ppppppp
- mpnp.data vv.rr.mmmm.ffff.ppppppp

Where:

- *vv* is the version number
- *rr* is the release number
- *mmmm* is the modification level
- *ffff* is the fix level
- *ppppppp* is the fix ID

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

software update commit -all

Description: Commit all the software updates that have been applied.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

software update list {-log}

Description: List the installed software updates.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

software update list -nocommit {-log}

Description: List software updates that have been applied, but not committed.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

software update precheck {-com_prev} {-rej_dptf} {*update_name***}**

Description: Performs the precheck function for software updates in the transfer directory.

Use the -com_prev option to automatically commit the PTFs that were applied, but not yet committed, before issuing this command.

Use the -rej_dptf option to automatically reject any applied development PTFs before installation. This option is ignored if you are prechecking only development PTFs.

Parameters: The updates to precheck are defaulted to all, unless you specify an update name.

The *update_name* parameter can be:

- mpnp (the same as all)
- mpnp.obj (all updates for mpnp.obj)
- mpnp.data (all updates for mpnp.data)
- mpnp vv.rr.mmmm.ffff.ppppppp
- mpnp.obj vv.rr.mmmm.ffff.ppppppp
- mpnp.data vv.rr.mmmm.ffff.ppppppp
- mpnp ppppppp
- mpnp.obj ppppppp
- mpnp.data ppppppp

Where:

- *vv* is the version number
- *rr* is the release number
- *mmmm* is the modification level
- *ffff* is the fix level
- *ppppppp* is the fix ID

Use the **software (list) -transfer** command to list the software in the transfer directory.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

software update reject *update_name*

Description: Reject the given software update that has been applied, but not committed.

Parameters: Use the **software update list -nocommit** command to list the uncommitted updates. Specify the *update_name* parameter as either:

- mpnp.obj vv.rr.mmmm.ffff.ppppppp
- mpnp.data vv.rr.mmmm.ffff.ppppppp

Where:

- *vv* is the version number
- *rr* is the release number
- *mmmm* is the modification level
- *ffff* is the fix level
- *ppppppp* is the fix ID

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

software update (view) (-fixes) -all {-log}

Description: View the problems fixed by all the software updates in the transfer directory.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

software update (view) (-fixes) {-log} *update_name*

Description: View the problems fixed by the given software update in the transfer directory.

Parameters: Use the **software (list) -transfer** command to list the software in the transfer directory.

Specify the *update_name* parameter as either:

- mpnp.obj vv.rr.mmmm.ffff.ppppppp
- mpnp.data vv.rr.mmmm.ffff.ppppppp

Where:

- *vv* is the version number
- *rr* is the release number
- *mmmm* is the modification level
- *ffff* is the fix level
- *ppppppp* is the fix ID

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

software view -dependents {-log}

Description: View the list of software updates dependent on previously installed software updates.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

software view -files {-log}

Description: View the list of files included with the Multiprotocol Network Program.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

software view -history {-log}

Description: View the entire installation history for the Multiprotocol Network Program. The installation history consists of all installation actions taken since the current release was installed on the 6611.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

software view -prerequisites {-log}

Description: View the list of software updates that are prerequisites to other software updates.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

software (view) -product_ID {-log}

Description: View the product information for the Multiprotocol Network Program.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

software view (-updates) {-log}

Description: View the list of software updates for the level of Multiprotocol Network Program currently installed on the 6611.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

Summary of Software Commands

Table 9-51 (Page 1 of 2). Summary of Software Commands

Command	Function
software cancel {-force}	Cancel a pending installation of a software update.
software cleanup	Remove all incomplete pieces of software after a failed installation.
software (list) [-diskettel-tapel-transfer] {-log}	List all the software on the diskette or tape, or in the transfer directory.
software lock	Locks the Multiprotocol Network Program, when selling the 6611 to a third party.
software receive [(-diskette)l-tape] -all	Import all the software from diskette or tape to the transfer directory.
software receive [(-diskette)l-tape] *software_name*	Import the software from diskette or tape to the transfer directory.
software receive -ftp *host_name userID passwd software_files*	Transfers the given software from a remote host to the transfer directory using the noninteractive version of FTP.
software rimon *control_file_name*	Start monitoring the installation status of all client 6611s listed in the remote installation control file.
software rinstall {-quiet} {-verbose} *control_file_name*	Start the remote installation (from a single control point) of a software update on multiple client 6611s. specified in the remote installation control file.
software ristop *control_file_name*	Cancel a pending remote installation of a software update on one or multiple client 6611s involved in the installation process.
software state view {-output}	Displays the installation state of the 6611.

Table 9-51 (Page 2 of 2). Summary of Software Commands

Command	Function
software update apply (-transfer) {-commit} {-com_prev} {-rej_dptf} {-all} {-time} {*time*} {*update_name*}	Apply the software updates from the transfer directory.
software update apply (-transfer) -noprecheck {-commit} {-time} {*time*)	Apply the software updates from the transfer directory without running the update precheck.
software update commit *update_name*	Commit the given software update that has been applied.
software update commit -all	Commit all the software updates that have been applied.
software update list {-log}	List the installed software updates.
software update list -nocommit {-log}	List software updates that have been applied, but not committed.
software update precheck {-com_prev} {-rej_dptf} {*update_name*}	Perform the precheck function for software updates in the transfer directory.
software update reject *update_name*	Reject the given software update that has been applied, but not committed.
software update (view) (-fixes) -all {-log}	View the problems fixed by all the software updates in the transfer directory.
software update (view) (-fixes) {-log} *update_name*	View the problems fixed by the given software update in the transfer directory.
software view -dependents {-log}	View the list of software updates dependent on previously installed software.
software view -files {-log}	View the list of files included with the Multiprotocol Network Program.
software view -history {-log}	View the entire installation history of the Multiprotocol Network Program.
software view -prerequisites {-log}	View the list of software updates that are prerequisite to other software updates.
software view -product_ID {-log}	View the product information for the Multiprotocol Network Program.
software view (-updates) {-log}	View the list of all software updates for the Multiprotocol Network Program.

System Commands

Use the system commands to:

- Stop and restart the 6611
- Run the system trace
- Produce a system trace report
- Dump the base operating system
- View information about the dump
- Format the system dump
- Extract error log and trace log entries from the dump
- Transfer the dump from the dump device to the transfer directory
- View the system route tables
- Monitor system protocol and interface statistics
- View many kinds of system statistics and connection information
- Run an interactive program to back up the 6611 on tape
- Collect system debug information

Table 9-52. Abbreviations for System Commands

Type of term	Term and Abbreviations	
Object	system	sys, s
Subobject	connections	connection, con, c
	debug	db
	dump	du, d
	routes	route, r
	statistics	statistic, stat, s
	trace	tr, t
Action	backup	bu, b
	collect	col, c
	dump	du
	extract	ext, ex
	list	l
	monitor	mon, m
	stop	end, e
	trace	tr, t
	transfer	trans
	view	v
Option	-activity	-act, -a
	-all	
	-cat	-c
	-dump_device	-dd
	-error_log	-el
	-format	-for, -f
	-input_output	-io
	-interface	-intf, -if, -i
	-log	-l
	-memory_management	-mm
	-minutes	-min, -m
	-norestart	-nor, -n
	-off	
	-on	
	-paging_space	-ps
	-previous_dump_info	-pdi, -p
	-protocol	-proto, -pro, -p
	-restart	-res, -r
	-socket_info	-sock, -si, -s
	-status	-stat
	-time	-t
	-trace_buffer	-tb
	-trace_ID	-tid, -ti, -id
	-trace_log	-tl
	-trace_mode	-tm
	-traffic	-trf
	-transfer	-trans, -tr
	-virtual_memory	-vm

system backup

Description: Backup the 6611 Multiprotocol Network Program onto a tape. This is an interactive command.

Parameters: None

Authorization: Controlling users only

System Environment: Fast-path only

system connections (view) {-log}

Description: View the system network connections.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

system debug (collect) {-paging_space} [(-tar)|-cat] {*output_file*}

Description: Collect system usage information to assist when solving paging space problems. **Do not use this command unless directed by IBM service personnel.** This command should be used approximately 20 minutes after a system restart if a paging space problem is suspected.

This command creates several output files in the transfer directory. These output files are combined into one file to facilitate the transfer from the 6611 to a remote host.

Specify the -tar option to archive the individual files to a binary file specified by *output_file*. Transfer the *output_file* to an AIX or UNIX workstation using the binary mode of ftp. Use the **tar -xvf** *output_file* command to restore the individual files. The individual files can be viewed with most workstation editors.

Specify the -cat option to combine the individual files into an ASCII file specified by *output_file*. Transfer the *output_file* to any workstation using the ASCII mode of ftp. The *output_file* can be viewed with most workstation editors.

Parameters: If you do not specify an output file name, the output is placed in the file `pd_hostname.pagingspace.debug`, where *hostname* is the host name for this 6611. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the output file name. If you specify an output file name, the prefix `pd_` is added to it. Specify only alphanumeric characters, periods (.), dashes (–), and underscores (_) in the output file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

system debug (collect) [(-tar)|-cat] {*number_days_errlog_clear*} {*output_file*}

Description: Collect system debug information and clear the error log.

This command creates several output files in the transfer directory. These output files are combined into one file to facilitate the transfer from the 6611 to a remote host.

Specify the -tar option to archive the individual files to a binary file specified by *output_file*. Transfer the *output_file* to an AIX or UNIX workstation using the binary mode of ftp. Use the **tar -xvf** *output_file* command to restore the individual files. The individual files can be viewed with most workstation editors.

Specify the -cat option to combine the individual files into an ASCII file specified by *output_file*. Transfer the *output_file* to any workstation using the ASCII mode of ftp. The *output_file* can be viewed with most workstation editors.

Parameters: You can specify the number of days worth of entries to clear from the error log. If you do not use the *number_days_errlog_clear* parameter, the error log will be cleared of all errors occuring more than two days prior to issuing this command.

If you do not specify an output file name, the output is placed in the file `pd_hostname.system.debug`, where *hostname* is the host name for this 6611. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the output file name. If you specify an output file name, the prefix `pd_` is added to it. Specify only alphanumeric characters, periods (.), dashes (–), and underscores (_) in the output file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path only

system dump

Description: Dump the main operating system. This command does not return and the system must be restarted. The dump goes to the dump device.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

system dump extract (-error_log)

Description: Extract error log records from the system dump.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

system dump extract -trace_log

Description: Extract trace log records from the system dump.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

system dump format [(-dump_device)|-transfer]

Description: Format the system dump that is in the either the dump device or the transfer directory and place it in the transfer directory as pd_system.fdump.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

system dump transfer

Description: Transfer the system dump to the transfer directory from the dump device. The system dump is placed in the transfer directory as pd_system.dump.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

system dump (view) -previous_dump_info {-log}

Description: View the information about the previous system dump.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

system routes (view) {-log} (-all)

Description: View the system route table for all protocols.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

system statistics monitor [(-protocol)|-interface] *number_seconds*

Description: Monitor either protocol or interface packet traffic statistics continuously. Specify the -protocol option to monitor protocol statistics. Specify the -interface option to monitor interface statistics. The statistics are periodically updated until you end the command. The period between updates is set with the *number_seconds* parameter. Press **Ctrl+C** to end the command.

Parameters: Specify the number of seconds between updating the statistics with the *number_seconds* parameter. The number of seconds must be between 10 and 300; the default is 10.

Authorization: Controlling users only

System Environment: Fast-path only

system statistics (view) (-activity) {-log} *number_seconds number_samples*

Description: View system activity statistics. Use the *number_seconds* parameter to determine the time period between updating the statistics. Use the *number_samples* parameter to specify how many updates to display.

Parameters: Specify a number between 1 and 5 for the *number_seconds* parameter. Specify a number between 1 and 5 for the *number_samples* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

system statistics (view) -input_output {-log} *number_seconds number_samples*

Description: View statistics for input and output activities. Use the *number_seconds* parameter to determine the time period between updating the statistics. Use the *number_samples* parameter to specify how many updates to display.

Parameters: Specify a number between 1 and 5 for the *number_seconds* parameter. Specify a number between 1 and 5 for the *number_samples* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

system statistics (view) -memory_management {-log}

Description: View the memory management statistics.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

system statistics (view) -paging_space {-log}

Description: View the characteristics of the system paging spaces.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

system statistics (view) -socket_info {-log}

Description: View information about the domain sockets.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

system statistics (view) -traffic *interface number_seconds*

Description: View the packet traffic information for the given interface gathered by the MPNP. Use the *number_seconds* parameter to specify the time interval between updates. Press **Ctrl+C** to end the command.

Parameters: Use the **interface list** command to list the active interfaces. All the interfaces are valid, except for the mpq# interfaces.

Specify a number between 1 and 5 for the *number_seconds* parameter.

Authorization: Controlling and viewing users

System Environment: Fast-path only

system statistics (view) -virtual_memory {-log} *number_seconds number_samples*

Description: View system virtual memory statistics. Use the *number_seconds* parameter to specify the time interval between updating the statistics. Use the *number_samples* parameter to specify how many updates to display.

Parameters: Specify a number between 1 and 5 for the *number_seconds* parameter. Specify a number between 1 and 5 for the *number_samples* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

system stop [(-restart)|-norestart] [(-minutes)|-time] [*number_minutes*|*time*]

Description: Stop the 6611 and Multiprotocol Network Program. Specify the -restart option to perform an automatic reboot. Specify the -norestart option if you want to power off the 6611.

Specify the -minutes option to stop the 6611 in the number of minutes indicated by the *number_minutes* parameter. Specify the -time option to stop the 6611 at the system time indicated by the *time* parameter.

Parameters: Specify a number between 0 and 59 for the *number_minutes* parameter. If you specify 0, the system stop will begin immediately.

Specify a time in the format *hh:mm* for the *time* parameter. *hh* must be between 0 and 23; *mm* must be between 0 and 59.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

system trace -format (-all) *start_time end_time*

Description: Format a system trace for all trace IDs logged during a given time period. The output is sent to the transfer directory as `pd_trace.report`.

Parameters: If a start time is specified, trace records with earlier time stamps are excluded from the report. If an end time is specified, trace records with later time stamps are excluded from the report. If no times are specified, no trace records are excluded from the report. The start time and end time format is MMDDhhmmssYY.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

system trace -format -trace_ID *trace_IDs*

Description: Format a system trace for the given trace IDs. The output is sent to the transfer directory as pd_trace.report.

Parameters: Use the **system trace (list) (-trace_ID)** command to list the valid trace IDs. Specify one or more three digit uppercase hexadecimal numbers for the *trace_IDs* parameter.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

system trace (list) (-trace_ID) {-log}

Description: List the system trace IDs.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

system trace -off

Description: Stop the system trace.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

system trace -on {-trace_mode} {-trace_buffer} {-trace_log}

{*trace_mode*} {*trace_buffer_size*} {*trace_log_size*} {*trace_IDs*}

Description: Start a system trace with the specified trace parameters.

Parameters: The -trace_mode, -trace_buffer, and -trace_log options are optional. If any are specified, then their corresponding parameters must be specified. If both the -trace_buffer and -trace_log options are given, then the trace_buffer_size parameter must *precede* the trace_log_size parameter.

The trace_mode is either:

- c (circular),
- a (alternate), or
- s (single)

with alternate being the default.

The trace_buffer_size is between 8192 and 524 288 bytes with a default of 131 072 bytes. The trace_log_size is between 1 048 576 and 10 485 760 bytes with a default of 1 048 576 bytes. The trace IDs must be at the end of the parameter list after the trace_mode, trace_buffer_size, or trace_log_size parameters, if any are specified.

Use the **system trace list (-trace_ID)** command to list the valid trace IDs. Specify one or more three digit uppercase hexadecimal numbers for the *trace_IDs* parameter. The trace is started for all trace IDs specified and the global trace IDs 001, 002, 106, 10C, 134, and 139.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

system trace -status

Description: Display the status of system and protocol traces.

The output is displayed in three columns. The first column lists the process or protocol name. The second column shows **ON** if the trace is running and **OFF** if the trace is not running. The third column contains the file name of any file in the transfer directory related to the trace.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

Summary of System Commands

Table 9-53 (Page 1 of 2). Summary of System Commands

Command	Function
system backup	Backup the 6611 Multiprotocol Network Program onto a tape.
system connections (view) {-log}	View the system network connections.
system debug (collect) [(-tar)|-cat] {-paging_space} {*output_file*}	Collect system paging space debug information
system debug (collect) [(-tar)|-cat] {*number_days_errlog_clear*} {*output_file*}	Collect system debug information.
system dump	Dump the main operating system.
system dump extract (-error_log)	Extract error log records from the system dump.
system dump extract -trace_log	Extract trace log records from the system dump.
system dump format [(-dump_device)|-transfer]	Format the system dump that is in the either the dump device or the transfer directory and place it in the transfer directory.
system dump transfer	Transfer the system dump to the transfer directory from the dump device.
system dump (view) -previous_dump_info {-log}	View the information about the previous system dump.
system routes (view) {-log} (-all)	View the system route table.
system statistics monitor [(-protocol)|-interface] *number_seconds*	Monitor the protocol and interface packet traffic statistics.
system statistics (view) (-activity) {-log} *number_seconds number_samples*	View system activity.
system statistics (view) -input_output {-log} *number_seconds number_samples*	View the input and output statistics.
system statistics (view) -memory_management {-log}	View the memory management statistics.
system statistics (view) -paging_space {-log}	View the characteristics of the system paging spaces.
system statistics (view) -socket_info {-log}	View information about the domain sockets.
system statistics (view) -traffic *interface number_seconds*	View the packet traffic information for the given interface gathered by the main operating system.
system statistics (view) -virtual_memory {-log} *number_seconds number_samples*	View system virtual memory statistics.

Table 9-53 (Page 2 of 2). Summary of System Commands

Command	Function
system stop [(-restart)|-norestart] [(-minutes)|-time] [*number_minutes|time*]	Stop and optionally restart the system in a given number of minutes or at a certain time.
system trace -format (-all) *start_time end_time*	Format the system trace for all trace IDs logged during a given time period.
system trace -format -trace_ID *trace_IDs*	Format the system trace for the given trace IDs.
system trace (list) (-trace_ID) {-log}	List the system trace IDs.
system trace -off	Stop the system trace.
system trace -on {-trace_mode} {-trace_buffer} {-trace_log} {*trace_mode*} {*trace_buffer_size*} {*trace_log_size*} {*trace_IDs*}	Start a system trace with the specified trace parameters.
system trace -status	Display the status of process and protocol traces.

Terminal Commands

Use the terminal commands to:

- Set an interrupt key
- Set a backspace key

Table 9-54. Abbreviations for Terminal Commands

Type of term	Term and Abbreviations	
Object	terminal	term
Subobject	backspace interrupt	bs, b int, i
Action	set	s

terminal backspace (set) *character*

Description: Set the terminal backspace to the given character. The specified key performs a backspace and erase character function, when pressed.

Parameters: The *character* parameter is any character chosen to be used as the backspace key.

Authorization: Controlling and viewing users

System Environment: Fast-path only

terminal interrupt (set) *character*

Description: Set the terminal interrupt to the given character. Use this key sequence whenever a function specifies that **Ctrl+C** is needed to end an operation.

Parameters: The *character* parameter is any character chosen to be used as the interrupt key.

Authorization: Controlling and viewing users

System Environment: Fast-path only

Summary of Terminal Commands

Table 9-55. Summary of Terminal Commands

Command	Function
terminal backspace (set) *character*	Set the terminal backspace to the given character.
terminal interrupt (set) *character*	Set the terminal interrupt to the given character.

Timeofday Commands

Use the time of day commands to:

- View the current date and time
- Set the current date and time

Table 9-56. Abbreviations for Timeofday Commands

Type of term	Term and Abbreviations	
Object	timeofday	tod, t
Action	set	s
	view	v

timeofday set *date-time*

Description: Set the time and date for the 6611. Log out and log back in to observe the time change.

Parameters: The *date-time* parameter has the format `YYMMDDhhmm.ss`, where:

```
YY is the year (88-99)
MM is the month (1-12)
DD is the day (1-31)
hh is the hour (0-23)
mm is the minute (0-59)
ss is the second (0-59)
```

The .ss is optional.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

timeofday view

Description: View the time and date in the 6611.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

Summary of Timeofday Commands

Table 9-57. Summary of Timeofday Commands

Command	Function
timeofday set *date-time*	Set the time and date for the 6611.
timeofday view	View the time and date in the 6611.

Timeserver Commands

Use the time server commands to:

- Start and stop using remote time service
- List the IP addresses of the configured remote time servers
- Add and delete remote time servers from the list

The time service function has these restrictions:

- It is allowed only over a LAN, not a WAN, connection.
- It does not work across one LAN to another.
- Another 6611 cannot be used as a time server.

Table 9-58. Abbreviations for Timeserver Commands

Type of term	Term and Abbreviations	
Object	timeserver	ts
Action	add	a
	delete	del, d
	list	l
	start	begin, b
	stop	end, e
Option	-log	-l

timeserver add *IP_address*

Description: Add a host to the list of time servers. A time server host must be connected to the 6611 over a LAN, not a WAN, connection. You must issue the **config apply** or **config commit** command for the new host to become part of the working configuration.

Parameters: Specify a dotted decimal address for the *IP_address* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

timeserver delete *IP_address*

Description: Delete a host from the list of time servers. You must issue the **config apply** or **config commit** command for the host to be deleted from the working configuration.

Parameters: Specify a dotted decimal address for the *IP_address* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

timeserver list {-log}

Description: List the IP addresses of all time servers.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

timeserver start

Description: Allow this 6611 to use remote time service. You must issue the **config apply** or **config commit** command before this 6611 will use remote time service.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

timeserver stop

Description: Stop this 6611 from using remote time service. You must issue the **config apply** or **config commit** command before this 6611 will stop using the remote time service.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

Summary of Timeserver Commands

Table 9-59. Summary of Timeserver Commands

Command	Function
timeserver add *IP_address*	Add a host to the list of time servers.
timeserver delete *IP_address*	Delete a host from the list of time servers.
timeserver list {-log}	List the IP addresses of all time servers.
timeserver start	Allow this 6611 to use remote time service.
timeserver stop	Stop this 6611 from using remote time service.

User Commands

Use the user commands to:

- List, add, and delete user IDs
- Change a user's password
- List the current users who are logged on
- Obtain a history of users who have logged on

Table 9-60. Abbreviations for User Commands

Type of term	Term and Abbreviations	
Object	user	users, u
Subobject	id	i
	password	pass, p
Action	add	a
	change	chg, c
	delete	del, d
	list	l
	view	v
Option	-controlling	-ctrl, -c
	-history	-his, -h
	-log	-l
	-logged_in	-li
	-viewing	-view, -v

user (id) add [(-controlling)|-viewing] *userID passwd*

Description: Add a user ID to the list of users and set the password. Specify the -controlling option to add a controlling user ID. Specify the -viewing option to add a viewing user ID.

You must issue the **config apply** or **config commit** command to add the user ID to the working configuration.

Parameters: Specify 1 to 8 lowercase alphanumeric characters for the *userID* parameter. Specify 1 to 8 lowercase alphanumeric characters for the *passwd* parameter.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

user (id) delete *userID*

Description: Delete a user ID from the list of users. You must issue the **config apply** or **config commit** command to delete the user ID from the working configuration.

Parameters: Use the **user (id) list** command to list the configured user IDs.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

user (id) list {-log}

Description: List all the configured users.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

user (id) view -history {-log}

Description: View a history of login and system restart activity. For each log in or restart, this information is displayed:

- User ID
- Terminal
- Host (if Telnet was used)
- Login time
- Session duration

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

user (id) view (-logged_in) {-log}

Description: View the users that are currently logged in. For each user, this information is displayed:

- User ID
- Login terminal
- Time of login
- Host (if Telnet was used)
- Type of user (controlling or viewing)

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

user password change *userID passwd new_passwd*

Description: Change the password for a specific user ID. You must issue the **config apply** or **config commit** command for the password change to become part of the working configuration.

Parameters: Use the **user (id) list** command to list the configured user IDs.

Specify the current password with the *passwd* parameter. Specify 1 to 8 alphanumeric lowercase characters for the *new_passwd* parameter.

Authorization: Controlling users only, unless you are changing your own password.

System Environment: RSH, REXEC, and fast-path

Summary of User Commands

Table 9-61. Summary of User Commands

Command	Function
user (id) add [(-controlling)l-viewing] *userID passwd*	Add a controlling or viewing user.
user (id) delete *userID*	Delete a user.
user (id) list {-log}	List all the configured users.
user (id) view -history {-log}	View a history of login and system restart activity.
user (id) view (-logged_in) {-log}	View the users that are currently logged in.
user password change *userID passwd new_passwd*	Change a user's password.

VINES Commands

Use the VINES commands to:

- Turn the VINES trace on or off
- Send an ICP echo to a VINES node
- View VINES routes, connections, and protocol statistics
- View VINES filter information
- Dump the VINES process
- View VINES ARP table entries for the system and interfaces
- List possible VINES ARP interface names
- View the VINES server name and network address
- Collect VINES debug information

Table 9-62. Abbreviations for VINES Commands

Type of term	Term and Abbreviations	
Object	VINES	vines, vin, vn, v
Subobject	arp	a
	connections	connection, con, c
	debug	db
	filters	filter, fil, f
	id	i
	neighbors	neighbor, nbr, n
	routes	route, r
	statistics	statistic, stat, s
Action	collect	col, c
	delete	del, d
	dump	du
	echo	e
	list	l
	trace	tr, t
	view	v
Option	-all	
	-cat	-c
	-flood	-fl, -f
	-interface	-intf, -if, -i
	-log	-l
	-off	
	-on	
	-RTP	-rtp, -r
	-system	-sys, -s
	-tar	-t

vines arp list (-interface)

Description: List the possible VINES ARP interfaces.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

vines arp (view) (-interface) {-log} *interface*

Description: View the VINES ARP table for a given peer-capable interface.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for VINES.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

vines connections (view) {-log} *interface*

Description: View the VINES interface connections.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for VINES.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

vines debug (collect) {-system} [(-tar)|-cat] {*output_file*}

Description: Collect VINES debug information. Specify the -system option to collect additional system debug information.

This command creates several output files in the transfer directory. These output files are combined into one file to facilitate the transfer from the 6611 to a remote host.

Specify the -tar option to archive the individual files to a binary file specified by *output_file*. Transfer the *output_file* to an AIX or UNIX workstation using the binary mode of ftp. Use the **tar -xvf** *output_file* command to restore the individual files. The individual files can be viewed with most workstation editors.

Specify the -cat option to combine the individual files into an ASCII file specified by *output_file*. Transfer the *output_file* to any workstation using the ASCII mode of ftp. The *output_file* can be viewed with most workstation editors.

Parameters: If you do not specify an output file name, the output will be placed in the file `pd_hostname.vines.debug`, where *hostname* is the host name for this 6611. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the output file name. If you specify an output file name, the prefix `pd_` added to it. Specify only alphanumeric characters, periods (.), dashes (–), and underscores (_) in the output file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path only

vines dump

Description: Dump the VINES routing protocol. The dump is placed in the transfer directory as pd_route_vines.dump.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

vines echo {-flood} {-log} *dest_net_num* **{***packet_size***} {***num_echoes***}**

Description: Issue an ICP echo request to another VINES node.

If the -flood option is not specified, the echo requests will be sent at the rate of one per second. If -flood is specified, the 6611 will send all the echo request to the destination host immediately.

Parameters: Specify a 4-byte hexadecimal number (X'1' to X'FFFFFFFE') for the *dest_net_num* parameter. Specify 1 to 100 bytes for the *packet_size* parameter; the default is 64 bytes. Specify a number between 1 and 1000 for the *num_echoes* parameter; the default is three echoes. You must specify a packet size if you want to specify the number of echoes.

Authorization: Controlling and viewing users

System Environment: Fast-path only

vines filters (view) {-log} *interface*

Description: View the VINES interface filters.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for VINES.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

vines filters (view) (-RTP) {-log}

Description: View the VINES RouTing update Protocol (RTP) filters.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

vines id (view)

Description: View the VINES server name and network address.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

vines neighbors delete *net_number*

Description: Delete an entry from the VINES neighbor table.

Parameters: The *net_number* parameter is a 4-byte hexadecimal number.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

vines neighbors (view) -all {-log}

Description: View the whole VINES neighbor table.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

vines neighbors (view) *interface*

Description: View the VINES neighbor table entries for a given interface.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for VINES.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

vines routes (view) -interface {-log} *interface*

Description: View the VINES route table for a given interface.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for VINES.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

vines routes (view) (-system) {-log}

Description: View the VINES system route table.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

vines statistics (view) (-interface) {-log} *interface*

Description: View the VINES network interface protocol statistics.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for VINES.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

vines statistics (view) (-RTP) {-log}

Description: View the VINES RouTing update Protocol (RTP) statistics.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

vines statistics (view) (-system) {-log}

Description: View the VINES system network protocol statistics.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

vines trace -off

Description: Stop the VINES routing protocol trace. The trace output is in pd_vines.trc in the transfer directory.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

vines trace (-on)

Description: Start the VINES routing protocol trace. The trace output is placed in pd_vines.trc in the transfer directory.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

Summary of VINES Commands

Table 9-63 (Page 1 of 2). Summary of VINES Commands

Command	Function
vines arp list (-interface)	View the possible VINES ARP interfaces.
vines arp (view) (-interface) {-log} *interface*	View the VINES ARP table for a given peer-capable interface.
vines connections (view) {-log} *interface*	View the VINES interface connections.
vines debug (collect) {-system} [(-tar)|-cat] {*output_file*}	Collect VINES debug information.
vines dump	Dump the VINES routing protocol.
vines echo {-flood} {-log} *dest_net_num* {*packet_size*} {*num_echoes*}	Issue an ICP echo request to another VINES node.
vines filters (view) {-log} *interface*	View the VINES interface filters.
vines filters (view) -RTP {-log}	View the VINES RouTing update Protocol (RTP) filters.
vines id (view)	View the VINES server name and network address.
vines neighbors delete *net_number*	Delete an entry from the VINES neighbor table.
vines neighbors (view) -all {-log}	View the whole VINES neighbor table.
vines neighbors (view) *interface*	View the VINES neighbor table entries for a given interface.
vines routes (view) -interface {-log} *interface*	View the VINES route table for a given interface.

Table 9-63 (Page 2 of 2). Summary of VINES Commands

Command	Function
vines routes (view) (-system) {-log}	View the VINES system route table.
vines statistics (view) (-interface) {-log} *interface*	View the VINES network interface protocol statistics.
vines statistics (view) (-RTP) {-log}	View the VINES RouTing update Protocol (RTP) statistics.
vines statistics (view) (-system) {-log}	View the VINES system network protocol statistics.
vines trace -off	Stop the VINES routing protocol trace.
vines trace (-on)	Start the VINES routing protocol trace.

XNS Commands

Use the Xerox Network Systems** (XNS**) commands to:

- Send an echo to an XNS node
- View XNS routes, connections, and protocol statistics
- View XNS filter information
- Collect XNS debug information
- Start and stop the XNS trace

Table 9-64. Abbreviations for XNS Commands

Type of term	Term and Abbreviations	
Object	XNS	xns, x
Subobject	connections	connection, con, c
	debug	db
	filters	filter, fil, f
	routes	route, r
	statistics	statistic, stat, s
Action	collect	col, c
	echo	e
	trace	tr, t
	view	v
Option	-cat	-c
	-flood	-fl, -f
	-interface	-intf, -if, -i
	-log	-l
	-off	
	-on	
	-RIP	-rip, -r
	-system	-sys, -s
	-tar	-t

xns connections (view) {-log} *interface*

Description: View the XNS interface connections.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for XNS.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

xns debug (collect) {-system} [(-tar)|-cat] {*output_file*}

Description: Collect XNS debug information. Specify the -system option to collect additional system debug information.

This command creates several output files in the transfer directory. These output files are combined into one file to facilitate the transfer from the 6611 to a remote host.

Specify the -tar option to archive the individual files to a binary file specified by *output_file*. Transfer the *output_file* to an AIX or UNIX workstation using the binary mode of ftp. Use the **tar -xvf** *output_file* command to restore the individual files. The individual files can be viewed with most workstation editors.

Specify the -cat option to combine the individual files into an ASCII file specified by *output_file*. Transfer the *output_file* to any workstation using the ASCII mode of ftp. The *output_file* can be viewed with most workstation editors.

Parameters: If you do not specify an output file name, the output will placed in the file `pd_hostname.xns.debug`, where *hostname* is the host name for this 6611. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the output file name. If you specify an output file name, the prefix `pd_` added to it. Specify only alphanumeric characters, periods (.), dashes (–), and underscores (_) in the output file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path only

xns echo {-flood} {-log} *dest_net_num dest_host_addr {packet_size} {num_echoes}*

Description: Issue an echo request to another XNS node. If the -flood option is not specified, the echo requests will be sent at the rate of one per second. If -flood is specified, the echo requests will be flooded on the destination host.

Parameters: The *dest_net_num* parameter is a 4-byte hexadecimal number. The *dest_host_addr* parameter is a 6-byte hexadecimal number. Together, the *dest_net_num* and *dest_host_addr* uniquely identify the XNS node to which the echo request is sent.

The packet size is in bytes from 1 to 100. The default is 64 bytes.

The number of echoes is from 1 to 1000. The default is three echoes.

Authorization: Controlling and viewing users

System Environment: Fast-path only

xns filters (view) {-log} *interface*

Description: View the XNS interface filters.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for XNS.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

xns filters (view) -RIP {-log}

Description: View the configured XNS RIP filters.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

xns routes (view) -interface {-log} *interface*

Description: View the XNS route table for a given interface.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for XNS.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

xns routes (view) (-system) {-log}

Description: View the system XNS route table.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

xns statistics (view) (-interface) {-log} *interface*

Description: View the XNS network interface protocol statistics.

Parameters: Use the **interface list** command to list the active interfaces. Choose only the interfaces configured for XNS.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

xns statistics (view) -system {-log}

Description: View the XNS system network protocol statistics.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

xns trace -off

Description: Stop the XNS routing protocol trace. The trace output is placed in the file `pd_XNSrouted.RIP`.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

xns trace -on

Description: Start the XNS routing protocol trace. The trace output is placed in the file `pd_XNSrouted.RIP`.

Parameters: None

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path

Summary of XNS Commands

Table 9-65. Summary of XNS Commands

Command	Function
xns connections (view) {-log} *interface*	View the XNS interface connections.
xns debug (collect) {-system} [(-tar)|-cat] {*output_file*}	Collect XNS debug information.
xns echo {-flood} {-log} *dest_net_num dest_host_addr packet_size num_echoes*	Issue an echo request to another XNS node.
xns filters (view) {-log} *interface*	View the XNS interface filters.
xns filters (view) -RIP {-log}	View the XNS RIP filters.
xns routes (view) -interface {-log} *interface*	View the XNS route table for a given interface.
xns routes (view) (-system) {-log}	View the system XNS route table.
xns statistics (view) (-interface) {-log} *interface*	View the XNS network interface protocol statistics.
xns statistics (view) -system {-log}	View the XNS system network protocol statistics.
xns trace -off	Stop the XNS routing protocol trace.
xns trace -on	Start the XNS routing protocol trace.

X.25 Commands

Use the X.25 commands to:

- Send test data to an X.25 node using the X.25 talk function
- Manage and monitor the X.25 nodes on your network
- Collect X.25 debugging information

Table 9-66. Abbreviations for X.25 Commands

Type of term	Term and Abbreviations	
Object	X25	x25
Subobject	debug	db
Action	collect list monitor	col, c l mon, m
Option	-adapter -cat -frame -packet -system -tar	-adp, -a -c -fr, -f -pack, -p -sys, -s -t

x25 debug (collect) {-system} [(-tar)|-cat] {*output_file*}

Description: Collect X.25 debug information. Specify the -system option to to collect additional system debug information.

This command creates several output files in the transfer directory. These output files are combined into one file to facilitate the transfer from the 6611 to a remote host.

Specify the -tar option to archive the individual files to a binary file specified by *output_file*. Transfer the *output_file* to an AIX or UNIX workstation using the binary mode of ftp. Use the **tar -xvf** *output_file* command to restore the individual files. The individual files can be viewed with most workstation editors.

Specify the -cat option to combine the individual files into an ASCII file specified by *output_file*. Transfer the *output_file* to any workstation using the ASCII mode of ftp. The *output_file* can be viewed with most workstation editors.

Parameters: If you do not specify an output file name, the output is placed in the file `pd_hostname.x25.debug`, where *hostname* is the host name for this 6611. If the *hostname* contains a colon (:), it will be replaced with a dash (–) in the output file name. If you specify an output file name, the prefix `pd_` is added to it. Specify only alphanumeric characters, periods (.), dashes (–), and underscores (_) in the output file name.

Authorization: Controlling users only

System Environment: RSH, REXEC, and fast-path only

x25 list (-adapter)

Description: List the X.25 adapter names.

Parameters: None

Authorization: Controlling and viewing users

System Environment: RSH, REXEC, and fast-path

x25 monitor [(-packet) &| -frame] *adapter*

Description: Monitor HDLC frame and packet activity on an X.25 adapter. The trace runs continuously until you choose to stop it. Press **Ctrl+C** to end the monitor. The monitor output will be placed in the file `pd_x25mon.trc`.

Parameters: Use the **x25 list (-adapter)** command to list the installed X.25 adapters.

Authorization: Controlling users only

System Environment: Fast-path only

Summary of X.25 Commands

Table 9-67. Summary of X.25 Commands

Command	Function
x25 debug (collect) {-system} [(-tar)|-cat] {*output_file*}	Collect X.25 debug information.
x25 list (-adapter)	List the X.25 adapter names.
x25 monitor [(-packet) &| -frame] *adapter*	Monitor the activity on an X.25 adapter.

Appendix A. Viewing and Modifying APPN COS Files

The 6611 enables you to modify the architected COS files provided for APPN routing. These files reside on the 6611 and are used by the APPN network node when calculating a route for an LU-LU session.

Each COS file defines acceptable ranges for node and TG characteristics. When an LU requests a session, it specifies the *mode* to use for the session. The mode specifies the parameters desired for the session, including the COS to be used. When the APPN network node calculates a route for the session, it compares the requested COS against the actual values assigned to intermediate nodes and TGs on paths to the destination node. The comparison determines the desirability of routing the session though specific nodes and node TGs. Each possible path is assigned a weight and the APPN network node selects the best (least-weight) route for the session.

You can view and modify a COS file on the 6611 by using System Manager fast-path commands. You also can transfer a COS file to a remote workstation and edit the file using a standard text editor. This appendix describes each of these options.

To ensure that all 6611 network nodes in an APPN network use the same criteria to make routing decisions, each of the network nodes should have identical COS files. Consequently, any changes to a COS file should be made on each 6611 network node in the network. This can be done manually or by using remote shell (**rsh**) commands to execute the appropriate fast-path commands on each of the 6611 network nodes in your network. See "Using Remote Shell Commands to Execute the Fast-Path Command Options" on page A-10 for more information.

Notes:

1. For a detailed discussion of APPN mode names and COS files, refer to the *IBM Systems Network Architecture Type 2.1 Node Reference*.
2. When configuring APPN on a 6611, you have the option of modifying the TG characteristics that define a connection between the 6611 and an adjacent node. See the *IBM Multiprotocol Network Program Configuration Guide* for more information.

Fast-Path Command Options for APPN COS Files

Using the fast-path commands on the 6611, you can:

- View the contents of an APPN COS file.
- Set the minimum and maximum values for the user-defined TG characteristics within an APPN COS file.
- Add a mode name to an APPN COS file.

To avoid introducing editing errors into a COS file, it is recommended that you use the fast-path commands, when possible, to modify the contents of a file.

Within the fast-path commands, COS names are referred to by number. Table A-1 shows the associated COS number for each COS name.

Note: Each mode name must be mapped to a corresponding COS name. APPN allows one or more mode names to map to the same COS name. The APPN architecture has defined a set of mode names that map to the architected COS names. This mapping is shown is Table A-1.

Table A-1. Architected COS and Mode Names

Mode Name	Corresponding COS Name	Corresponding COS Number Used in Fast-Path Commands
#BATCH	#BATCH	1
#BATCHSC	#BATCHSC	2
None (default)	#CONNECT	3
#INTER	#INTER	4
#INTERSC	#INTERSC	5
CPSVCMG	CPSVCMG	6
SNASVCMG	SNASVCMG	7

For a description of all APPN fast-path commands and command abbreviations, see "Fast-Path Commands."

Viewing the Contents of an APPN COS File

This section describes fast-path commands that enable you to view:

- An entire APPN COS file
- A specific TG row in a COS file
- All mode names in a COS file

The commands can be issued by viewing and controlling users.

- To view an entire COS file, use the fast-path command:

  appn view (-COS) {-log} *COS_number*

  Figure A-1 on page A-5 shows a sample COS file (#INTER).

  Example: The following command displays the contents of the #INTER COS file and stores the contents in the fast-path log.

  appn view -log 4

- To view a specific TG row in a COS file, use the fast-path command:

  appn view (-COS) -transmission_group *COS_number TG_row*

  You can specify a value of 1 to 8 for the *TG_row* parameter.

  Example: The following command displays the contents of TG row 2 in the #INTER COS file.

  appn view -transmission_group 4 2

- To view all mode names in a COS file, use the fast-path command:

  appn view (-COS) -mode_name *COS_number*

  Example: The following command displays the mode names associated with the #INTER COS file.

  appn view -mode_name 4

Modifying User-Defined TG Characteristics

The following fast-path command enables you set the minimum and maximum ranges for the user-defined TG characteristics within an APPN COS file:

appn set (-COS) [-user1|-user2|-user3] {-restart} *COS_number TG_row min_user_char max_user_char*

This command can be issued only by a controlling user. You can specify a value of 0 to 255 for the *min_user_char* and *max_user_char* parameters. The value of the *min_user_char* parameter cannot be greater than the value of the *max_user_char* parameter.

Example: The following command sets the minimum and maximum values for the first user-defined TG characteristic in TG row 2 of the #INTER COS file. The new minimum is 5; the new maximum is 100.

appn set -user1 4 2 5 100

Note: The change is effective when the APPN function on the 6611 is restarted. To restart the APPN function immediately, use the -restart option. To restart the APPN function at a later time, use the **appn restart** command.

Adding a Mode Name

The following fast-path command enables you to add a mode name to an APPN COS file:

appn set (-COS) (-mode_name) {-restart} *COS_number mode_name*

This command can be issued only by a controlling user. The mode name can be a string of up to 8 characters in length, including special characters. In general, this command is used to add a non-architected mode name to a COS file.

Example: The following command adds the mode name QPCSUPP to the #CONNECT COS file.

appn set 3 QPCSUPP

Note: The change is effective when the APPN function on the 6611 is restarted. To restart the APPN function immediately, use the -restart option. To restart the APPN function at a later time, use the **appn restart** command.

Retrieving and Editing an APPN COS File

As an alternative to using the System Manager fast-path commands, you can retrieve an APPN COS file from the 6611 and edit it using a standard text editor. As a rule, you should not edit a COS file manually unless you need to change a characteristic in the file that cannot be changed through the System Manager. An error introduced into a COS file can negatively impact the routing of traffic in your APPN network.

Note: This procedure can be performed only by a controlling user.

To retrieve a COS file from the 6611, do the following:

1. Move the COS file from the APPN directory on the 6611 to the transfer directory using the following fast-path command:

   appn transfer (-to) *COS_number*

2. Send the file to a remote workstation. You can use FTP or the System Manager to send the file. (See "Send Transfer Directory File" on page 4-43 for more information.)

3. Edit the file on the remote workstation. "Editing a COS File" provides guidelines for editing the file.

4. After modifying the file, return it to the 6611's transfer directory.

5. Move the file from the transfer directory to the APPN directory using the following fast-path command:

   appn transfer -from *COS_number*

   The APPN function on the 6611 automatically restarts after the COS file is moved from the transfer directory to the APPN directory.

Editing a COS File

Figure A-1 on page A-5 shows a sample COS file. An architected COS file contains a set of COS entries (including transmission priority and mode name), one to eight rows of node characteristics, and one to eight rows of TG characteristics. Each node and TG row in the file consists of two lines. The top line of the row specifies the minimum values for each of the row characteristics. The bottom line of the row specifies the maximum values for each of the row characteristics. The minimum and maximum values for a COS characteristic represent the range of acceptable values for that characteristic.

Node and TG rows are arranged by weight, with the lowest-weight row appearing first and the highest-weight row appearing last. When actual node or TG values are compared against the contents of a COS file, the values are first compared to the lowest-weight node or TG row in the file, respectively. If the actual values fall within the ranges of acceptable values for the characteristics in the row, the weight associated with the row is assigned to the node or TG. If the actual values do not fall within the ranges of acceptable values for the row, the comparison continues with the next highest-weight row.

```
def_cos:
  cos_name:              #INTER
  store_weights:         YES
  transmission_priority: HIGH
  mode_name:             #INTER

                          (congestion   resistance   weight)
  node_row: 1  (min)           NO           0           5
               (max)           NO          31
  node_row: 2                  NO           0          10
                               NO          63
  node_row: 3                  NO           0          20
                               NO          95
  node_row: 4                  NO           0          40
                               NO         127
  node_row: 5                  NO           0          60
                               NO         159
  node_row: 6                  NO           0          80
                               NO         191
  node_row: 7                  NO           0         120
                               YES        223
  node_row: 8                  NO           0         160
                               YES        255

               (time  byte  security     prop.    capacity  user_defined  weight)
               (cost  cost               delay )
  tg_row:   1    0    0   MINIMAL     MINIMUM      76       0   0   0     30
                 0    0   RAD_GUARDED NEGLIGIBLE   FF     255 255 255
  tg_row:   2    0    0   MINIMAL     MINIMUM      44       0   0   0     60
                 0    0   RAD_GUARDED TERRESTRIAL  FF     255 255 255
  tg_row:   3    0    0   MINIMAL     MINIMUM      44       0   0   0     90
                128  128   RAD_GUARDED TERRESTRIAL  FF     255 255 255
  tg_row:   4    0    0   MINIMAL     MINIMUM      38       0   0   0    120
                 0    0   RAD_GUARDED TERRESTRIAL  FF     255 255 255
  tg_row:   5    0    0   MINIMAL     MINIMUM      38       0   0   0    150
                128  128   RAD_GUARDED PACKET       FF     255 255 255
  tg_row:   6    0    0   MINIMAL     MINIMUM      30       0   0   0    180
                 0    0   RAD_GUARDED PACKET       FF     255 255 255
  tg_row:   7    0    0   MINIMAL     MINIMUM      30       0   0   0    210
                196  196   RAD_GUARDED MAXIMUM      FF     255 255 255
  tg_row:   8    0    0   MINIMAL     MINIMUM      00       0   0   0    240
                255  255   RAD_GUARDED MAXIMUM      FF     255 255 255

edef_cos:
```

Figure A-1. Sample APPN COS File (#INTER)

Node Characteristics

As shown in Figure A-1, each row of node characteristics contains minimum and maximum values for *congestion* and *resistance*, and a weight for the row. The valid values for congestion are **YES** and **NO**, and the following combinations are allowed:

- Both minimum and maximum congestion values are **NO**. In this case, only nodes with no congestion fall within the acceptable range for the row.
- The minimum congestion value is **NO** and the maximum congestion value is **YES**. In this case, all nodes fall within the acceptable range for the row.
- The minimum and maximum congestion values are **YES**. In this case, only congested nodes fall within the acceptable range for the row.

The resistance value must be an integer in the range of 0 to 255. The resistance value indicates the desirability of routing a session through a node. Lower values represent higher levels of desirability. The weight associated with a row must be an integer in the range of 0 to 255. The weights for successive rows cannot decrease.

TG Characteristics

As shown in Figure A-1, each TG row contains minimum and maximum values for the TG characteristics described in Table A-2 on page A-7. Each TG row also contains a weight. The weight associated with a row must be an integer in the range of 0 to 255. The weights for successive rows cannot decrease.

Table A-2. TG Characteristics

Characteristic	Description	Valid Range
Cost per connect time (time cost)	The relative cost of maintaining a connection over a TG	0 to 255 (0 is the minimum cost)
Cost per byte (byte cost)	The relative cost of transmitting a byte over a TG	0 to 255 (0 is the minimum cost)
Security	Architecturally-defined security values	• MINIMAL (nonsecure) • PUBLIC_SWCH (public-switched) • UNDERGROUND (underground cable) • SECURE (secure conduit - not guarded) • PHYS_GUARDED (guarded conduit - protected against physical tapping) • ENCRYPTED (link-level encryption provided) • RAD_GUARDED (guarded conduit - protected against physical and radiation tapping)
Propagation delay (prop. delay)	The length of time it takes for a signal to propagate from one end of a TG to the other end	• MINIMUM • NEGLIGIBLE (less than .48 ms) • TERRESTRIAL (.48 to 49.152 ms) • PACKET (packet-switched - 49.152 to 245.76 ms) • LONG (greater than 245.76 ms) • MAXIMUM
Effective capacity (capacity)	The highest bit transmission rate a TG is allowed to obtain before being considered overloaded.	Table A-3 on page A-8 maps the effective capacity settings (X'00' to X'FF') to link speeds
User-defined	Three additional user-defined characteristics that describes a TG	0 to 255

Table A-3 (Page 1 of 2). Effective Capacity Representations

COS Value	Kbps	COS Value	Kbps	COS Value	Kbps	COS Value	Kbps
X'00'	MINIMUM	X'40'	38.4	X'80'	9830.4	X'C0'	2516582.4
X'01'	0.16875	X'41'	43.2	X'81'	11059.2	X'C1'	2831155.2
X'02'	0.18750	X'42'	48.0	X'82'	12288.0	X'C2'	3145728.0
X'03'	0.20625	X'43'	52.8	X'83'	13516.8	X'C3'	3460300.8
X'04'	0.22500	X'44'	57.6	X'84'	14745.6	X'C4'	37748736
X'05'	0.24375	X'45'	62.4	X'85'	15974.4	X'C5'	4089446.4
X'06'	0.26250	X'46'	67.2	X'86'	17203.2	X'C6'	4404019.2
X'07'	0.28125	X'47'	72.0	X'87'	18432.0	X'C7'	4718592.0
X'08'	0.30000	X'48'	76.8	X'88'	19660.8	X'C8'	5033164.8
X'09'	0.33750	X'49'	86.4	X'89'	22118.4	X'C9'	5662310.4
X'0A'	0.37500	X'4A'	96.0	X'8A'	24576.0	X'CA'	6291456.0
X'0B'	0.41250	X'4B'	105.6	X'8B'	27033.6	X'CB'	6920601.6
X'0C'	0.45000	X'4C'	115.2	X'8C'	29491.2	X'CC'	7549747.2
X'0D'	0.48750	X'4D'	124.8	X'8D'	31948.8	X'CD'	8187892.8
X'0E'	0.52500	X'4E'	134.4	X'8E'	34406.4	X'CE'	8808038.4
X'0F'	0.56250	X'4F'	144.0	X'8F'	36864.0	X'CF'	9437184.0
X'10'	0.60000	X'50'	153.6	X'90'	39321.6	X'D0'	10066329.6
X'11'	0.67500	X'51'	172.8	X'91'	44236.8	X'D1'	11324620.8
X'12'	0.75000	X'52'	192.0	X'92'	49152.0	X'D2'	12582912.0
X'13'	0.82500	X'53'	211.2	X'93'	54067.2	X'D3'	13841203.2
X'14'	0.90000	X'54'	230.4	X'94'	58982.4	X'D4'	15099494.4
X'15'	0.97500	X'55'	249.6	X'95'	63897.6	X'D5'	16357785.6
X'16'	1.05000	X'56'	268.8	X'96'	68812.8	X'D6'	17616076.8
X'17'	1.12500	X'57'	288.0	X'97'	73728.0	X'D7'	18874368.0
X'18'	1.20000	X'58'	307.2	X'98'	78643.2	X'D8'	20132659.2
X'19'	1.35000	X'59'	345.6	X'99'	88473.6	X'D9'	22649241.6
X'1A'	1.50000	X'5A'	384.0	X'9A'	98304.0	X'DA'	25165824.0
X'1B'	1.65000	X'5B'	422.4	X'9B'	108134.4	X'DB'	27682406.4
X'1C'	1.80000	X'5C'	460.8	X'9C'	117964.8	X'DC'	30198988.8
X'1D'	1.95000	X'5D'	499.2	X'9D'	127795.2	X'DD'	32715517.2
X'1E'	2.10000	X'5E'	537.6	X'9E'	137625.6	X'DE'	35232153.6
X'1F'	2.25000	X'5F'	576.0	X'9F'	147456.0	X'DF'	37748736.0
X'20'	2.40000	X'60'	614.4	X'A0'	157286.4	X'E0'	40265318.4
X'21'	2.70000	X'61'	691.2	X'A1'	176947.2	X'E1'	45298483.2
X'22'	3.00000	X'62'	768.0	X'A2'	196608.0	X'E2'	50331648.0
X'23'	3.30000	X'63'	844.8	X'A3'	216268.8	X'E3'	55364812.8
X'24'	3.60000	X'64'	921.6	X'A4'	235929.6	X'E4'	60397977.6
X'25'	3.90000	X'65'	998.4	X'A5'	255590.4	X'E5'	65431142.4
X'26'	4.20000	X'66'	1075.2	X'A6'	275251.2	X'E6'	70464307.2
X'27'	4.50000	X'67'	1152.0	X'A7'	294912.0	X'E7'	75497472.0
X'28'	4.80000	X'68'	1228.8	X'A8'	314572.8	X'E8'	80530636.8
X'29'	5.40000	X'69'	1382.4	X'A9'	353894.4	X'E9'	90596966.4
X'2A'	6.00000	X'6A'	1536.0	X'AA'	393216.0	X'EA'	100663296.0

Table A-3 (Page 2 of 2). Effective Capacity Representations

COS Value	Kbps	COS Value	Kbps	COS Value	Kbps	COS Value	Kbps
X'2B'	6.6	X'6B'	1689.6	X'AB'	432537.6	X'EB'	110729625.6
X'2C'	7.2	X'6C'	1843.2	X'AC'	471859.2	X'EC'	120725955.2
X'2D'	7.8	X'6D'	1996.8	X'AD'	511180.8	X'ED'	130862284.8
X'2E'	8.4	X'6E'	2150.4	X'AE'	550502.4	X'EE'	140928614.4
X'2F'	9.0	X'6F'	2304.0	X'AF'	589824.0	X'EF'	150994944.0
X'30'	9.6	X'70'	2457.6	X'B0'	629145.6	X'F0'	161061273.6
X'31'	10.8	X'71'	2764.8	X'B1'	707788.8	X'F1'	181192932.8
X'32'	12.0	X'72'	3072.0	X'B2'	786432.0	X'F2'	201326592.0
X'33'	13.2	X'73'	3379.2	X'B3'	865075.2	X'F3'	221459251.2
X'34'	14.4	X'74'	3686.4	X'B4'	943718.4	X'F4'	241591910.4
X'35'	15.6	X'75'	3993.6	X'B5'	1022361.6	X'F5'	261724569.6
X'36'	16.8	X'76'	4300.8	X'B6'	1101004.8	X'F6'	281857228.8
X'37'	18.0	X'77'	4608.0	X'B7'	1179648.0	X'F7'	301989888.0
X'38'	19.2	X'78'	4915.2	X'B8'	1258291.2	X'F8'	322122547.2
X'39'	21.6	X'79'	5529.6	X'B9'	1415577.6	X'F9'	362387865.6
X'3A'	24.0	X'7A'	6144.0	X'BA'	1572864.0	X'FA'	402653184.0
X'3B'	26.4	X'7B'	6758.4	X'BB'	1730150.4	X'FB'	422918502.4
X'3C'	28.8	X'7C'	7372.8	X'BC'	1887436.8	X'FC'	483183820.8
X'3D'	31.2	X'7D'	7987.2	X'BD'	2044723.2	X'FD'	523449139.2
X'3E'	33.6	X'7E'	8601.6	X'BE'	2202009.6	X'FE'	563714457.6
X'3F'	36.0	X'7F'	9216.0	X'BF'	2359296.0	X'FF'	MAXIMUM

Verifying the Format of a COS File

Use the following guidelines to verify the format of a COS file that you have edited.

- The file contains a set of *tags* that identify different elements in the file. The last character of each tag must be a : (colon).
- The first tag in the file must be **def_cos:**. The last tag in the file must be **edef_cos:**.
- Each tag in the file, except for **def_cos:** and **edef_cos:**, must be followed by one or more values.
- No line in the file can contain more than one tag (although a tag and its associated values can span more than one line).
- Comments are enclosed in parentheses.
- The file must contain a **cos_name:** tag. This tag cannot be placed among the **node_row:** or **tg_row:** tags. To improve error reporting, it is recommended that the **cos_name:** tag be included as the first tag following the **def_cos:** tag. When APPN finds an error in a COS file tag, it stops processing the COS file and reports the error. If the tag with the error is processed before the **cos_name:** tag, APPN will not know the name of the COS file being processed when it reports the error.
- The file must also contain at least one row of node characteristics and one row of TG characteristics.

Using Remote Shell Commands to Execute the Fast-Path Command Options

Figure A-2 illustrates how remote shell commands can be used to execute a series of APPN fast-path commands on multiple 6611 routers. The general form for an **rsh** command that executes a fast-path command is:

rsh *hostname -l userid passwd fast-path_command*

where:

- *Hostname* is the host name of the 6611 to which the command is sent. An IP address can be used in place of the host name.
- *Userid* is a user ID defined on the 6611 to which the command is sent.
- *Passwd* is the password for the user ID.
- *Fast-path_command* is the fast-path command to be executed.

When the **rsh** commands are included in an executable file, the resulting file can be run from an IP workstation that supports the **rsh** daemon. The file enables you to make changes to COS files on multiple 6611 routers without logging onto a 6611. (See Chapter 3 for more information on using remote shell commands.)

```
:
rsh 8.9.9.1 -l IBM6611C IBM6611C appn set -user1 -restart 4 2 5 100
rsh 8.9.9.1 -l IBM6611C IBM6611C appn set -mode_name -restart 3 QPCSUPP
rsh 9.67.46.129 -l IBM6611C IBM6611C appn set -user1 -restart 4 2 5 100
rsh 9.67.46.129 -l IBM6611C IBM6611C appn set -mode_name -restart 3 QPCSUPP
rsh 6611HQ -l IBM6611C IBM6611C appn set -user1 -restart 4 2 5 100
rsh 6611HQ -l IBM6611C IBM6611C appn set -mode_name -restart 3 QPCSUPP
:
```

Figure A-2. Sample Remote Shell Commands

The fast-path commands shown in Figure A-2:

- Set the range for the first user-defined TG characteristic in TG row 2 of the #INTER COS file to a minimum value of 5 and a maximum value of 100.
- Add the mode name QPCSUPP to the #CONNECT COS file.

Notes:

1. For the purposes of this sample, the default 6611 user ID and password are shown for each router.
2. To execute an **appn set** fast-path command, the user ID contained in the **rsh** command must be a controlling user.

Appendix B. License Program Specification

This appendix contains license information about the IBM Multiprotocol Network Program Version 1 Release 3. The product identifier for this product is 5648-016.

Description

The Multiprotocol Network Program Version 1 Release 3 provides bridging and routing software for the IBM 6611 Network Processor Model 120, Model 125, Model 140, Model 145, Model 170, and Model 175. All models are shipped with the Multiprotocol Network Program installed.

The basic functions of the Multiprotocol Network Program include:

- The ability to route a variety of protocols such as IP, IPX, XNS, AppleTalk, APPN, DECnet, and Banyan VINES
- The ability to bridge packets using source route bridging, transparent bridging, or translational bridging
- The ability to transport Systems Network Architecture (SNA, Advanced Peer to Peer Networking (APPN), and Network Basic Input/Output Systems (NetBIOS) traffic using data link switching (DLSw) in a bridged or routed environment
- A Simple Network Management Protocol (SNMP) network management agent

Included with the Multiprotocol Network Program are two other programs, which complete the software product:

- The IBM Multiprotocol Network Program System Manager is an interactive user interface designed to perform system management and operation tasks. It displays a hierarchy of menus that lead to interactive dialogs. System Manager is installed on all models of the IBM 6611 Network Processor.
- The IBM Multiprotocol Network Program Configuration Program is a graphical user interface designed to configure the IBM 6611 Network Processor. The Configuration Program diskettes are shipped with the 6611. Store the Configuration Program diskettes in the binder for this book. See "Programming Requirements" on page B-2 for the Configuration Program software and hardware requirements.

Specified Operating Environment

Machine Requirements

The Multiprotocol Network Program is designed to operate on all models of the 6611. The minimal machine configuration consists of an 6611 and the communication adapters required to implement the user's configuration.

To run diagnostics after installing or servicing the 6611, it is required that the user make an ASCII terminal such as the IBM 3161 or an equivalent available to IBM service personnel. In normal operating mode, the 6611 and the Multiprotocol Network Program will not use the ASCII terminal.

IBM will provide optional remote service capability for 6611 users. Customers who want to establish this service must provide a modem such as the IBM 5853, or an equivalent, and a communications line.

Programming Requirements

Initial configuration of the Multiprotocol Network Program and subsequent configuration changes can be performed using the IBM Multiprotocol Network Program Configuration Program or the IBM Multiprotocol Network Program System Manager.

You will need one of the following workstations and related equipment and software to run the IBM Multiprotocol Network Program Configuration Program:

- IBM RISC System/6000 POWERstation* equipped with:
  - IBM AIX Version 3.1.5 or later with TCP/IP enabled
  - IBM AIXwindows* Environment/6000
  - 16 MB of memory
  - 3.5-inch diskette drive that can read and write 1.44 MB-formatted diskettes
  - 10 MB of available space of the fixed disk drive
  - Graphics display that supports 640x480 resolution and 16 colors or gray scales
  - Mouse
- An IBM Personal System/2* (PS/2) workstation that has an Intel** 80386** or higher processor or a compatible system which has an Intel 80386 or higher processor. For workstations running Windows**, the following is required:
  - IBM DOS 3.3 or later, MS-DOS** 3.3 or later
  - Microsoft Windows** 3.0 or 3.1
  - 8 MB of memory
  - 3.5-inch diskette drive that can read and write 1.44 MB-formatted diskettes
  - 10 MB of available space on the fixed disk drive
  - Graphics display that supports 640x480 resolution and 16 colors or gray scales
  - Mouse
- For workstations running OS/2*, the following is required:
  - Operating System/2* (OS/2) 2.1
  - 10 MB of memory
  - 3.5-inch diskette drive that can read and write 1.44 MB-formatted diskettes
  - 10 MB of available space on the fixed disk drive
  - Graphics display that supports 640x480 resolution and 16 colors or gray scales
  - Mouse

Licensed Program Materials Availability

Yes. This licensed program is available with some licensed program materials designated as "RESTRICTED MATERIALS OF IBM." The remaining licensed program materials are available and are not designated as "RESTRICTED MATERIALS OF IBM."

Supplemental Terms

Testing Period

None

Installation/Location License

Not applicable. A separate license is required for each machine on which the license program will be used.

Selling to a Third Party

When the 6611 is sold to a third party, the original owner must lock the Multiprotocol Network Program using either the Configuration Program or a fast-path command primitive. The software is locked by the original owner and unlocked by the customer to whom it was sold.

Usage License

Not applicable.

Type/Duration of Program Services

Central Service, including the IBM Support Center, will be available until discontinued by IBM with a minimum of six months written notice.

Warranty

IBM warrants that:

1. IBM has the right to license this program.
2. The IBM program conforms to its specifications.

The warranty period for this program expires when its program services are no longer available. During the warranty period, IBM will provide warranty service, without charge, through Program Services. Program Services are available for a warranty program for at least one year following the program's general availability.

Additional Information

Any other documentation with respect to this licensed program, including any documentation referenced herein, is provided for reference purposes only and does not extend or modify these specifications.

Abbreviations, Glossary, Bibliography, and Index

List of Abbreviations

A	ampere
AARP	AppleTalk Address Resolution Protocol
AC	alternating current
ACLST	AC logic self-test
ADCCP	advanced data communication control procedures
AEP	AppleTalk Echo Protocol
AIPGM	array initialization program
AIX	Advanced Interactive Executive
AMA	arbitrary MAC addressing
AMI	alternate mark inversion
AMT	address mapping table
ANSI	American National Standards Institute
APAR	Authorized Program Analysis Report
API	application programming interface
APPN	Advanced Peer-to-Peer Networking
ARP	Address Resolution Protocol
AS	Australian standard
ASCII	American National Standard Code for Information Interchange
ASE	autonomous system externals
ASN	Autonomous System Number
ASN	abstract syntax notation
AST	array self test
ASYNC	asynchronous
AT	Attention
ATE	Asynchronous Terminal Emulation
ATP	AppleTalk Transaction Protocol
AUI	attachment unit interface
AWG	American Wire Gauge
BCR	branch-on-condition register
BECN	backward explicit congestion notification
BER	basic encoding rules
BER	Bit error rate
BIOS	basic input/output system
BGP	Border Gateway Protocol
BIST	built-in self-test
BIU	basic information unit
BPDU	bridge protocol data unit
bps	bits per second
BS	British Standard
BSCRW	binary synchronous read/write
BTU	British thermal unit
B8ZS	binary 8 zero suppression coding scheme
C	Celsius
CBA	common on-chip-processor bus address
CCITT	Consultative Committee on International Telegraph and Telephone
CD-ROM	compact disk read-only memory
CEE	International Commission for Conformity Certification of Electrical Equipment
CEI	Comitato Elettrotechnico Italiano
CEPT	Conference of European Post and Telecommunications Associations
CIO	common input/output
cm	centimeter
COS	class of service
CP	control point
CPMS	control point management services
CP-MSU	control point management services unit
CPS	call progress signal
CPU	central processing unit
CR	carriage return
CRC	cyclic redundancy check
CRS	configuration report server
CRT	cathode ray tube
CSA	Canadian Standards Association
CSMA/CD	carrier sense multiple access with collision detection
CSU	channel service unit
CTS	clear to send
CUG	closed user group
DA	destination address; diagnostic application
dB	decibel
DC	direct current
DCD	data carrier detect
DCE	data circuit-terminating equipment
DCLST	DC logic self-test

DDCMP Digital Data Communications Message Protocol

DDN Defense Data Network

DDP Datagram Delivery Protocol

DIS draft international standard

DISC disconnect character

DLC data link control

DLCI data link connection identifier

DLSw data link switching

DM data mode

DMA direct memory access

DNA Digital Network Architecture

DoD Department of Defense

DOS Disk Operating System

DRAM dynamic random access memory

DS directory services

DSAP destination service access point

DSE data switching equipment

DSE data switching exchange

DSPU downstream physical unit

DSR data set ready

DSU data service unit

DTE data terminal equipment

DTR data terminal ready

DUSCC dual universal serial communications controller

EC engineering change

ECC error correcting code

EGP Exterior Gateway Protocol

EIA Electronics Industries Association

EIB error information block

ELAP EtherTalk Link Access Protocol

EMEA Europe/Middle East/Africa

EMI electromagnetic interference

EN end node

EP entry point

EPOW early power on warning

EPROM erasable programmable read-only memory

ESD electrostatic discharge

ESF extended super frame

ETX end of text

F Fahrenheit

FCS frame check sequence

FDDI Fiber Distributed Data Interface

FDL facilities data link

FDX full duplex

FECN forward explicit congestion notification

FFC failing function code

FP focal point

FRP Fragmentation Protocol

FRU field replaceable unit

FSCK File System Check

ft foot, feet

FTP File Transfer Protocol

GDS general data stream

HDLC high-level data link control

HVPD hardware vital product data

Hz hertz

I information

IAB Internet Architecture Board

IANA Internet Assigned Numbers Authority

ICMP Internet Control Message Protocol

ICP Internet Control Protocol

ID identification

IDP Internet Datagram Protocol

IEC International Electrotechnical Commission

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IGP Interior Gateway Protocol

in. inch

InARP Inverse Address Resolution Protocol

IML initial machine load

I/O input/output

IOCC input/output channel control

ICP Internet Control Protocol

IP Internet Protocol

IPC Interprocess Communications Protocol

IPCP IP Control Protocol

IPL initial program load

IPRTS permanent request to send

IPX Internetwork Packet Exchange

IRTF Internet Research Task Force

ISDN integrated services digital network
ISO International Organization for Standardization
ISR intermediate session routing
KB kilobyte
Kbps kilobits per second
kg kilogram
KHz kilohertz
kVA kilovolt ampere
LAN local area network
LAPB link access protocol-balanced
LAPD link access procedure for D-channel of ISDN
lb pound
LBO line build out
LBS LAN bridge server
LCN logical channel number
LCP Link Control Protocol
LED light-emitting diode
LEN low-entry networking
LF line feed
LLC logical link control
LMI local management interface
LNM LAN Network Manager
LpAm level pressure A-weighted mean
LRM LAN reporting mechanism
LU logical unit
LVM logical volume manager
LWAd level watts A-weighted declared
m meter
MAC medium access control
MAN metropolitan area network
MAP maintenance analysis procedure
MAP Manufacturing Automation Protocol
Mb megabit
MB megabyte
Mbps megabits per second
MBps megabytes per second
MDS multiple domain support
MDS-MU multiple domain support message unit
MES Miscellaneous Equipment Specifications
MHz megahertz
MIB Management Information Base
MILNET military network
MLTG multi-link transmission group
mm millimeter
MPNP Multiprotocol Network Program
ms millisecond
MTU maximum transmission unit
NAU network addressable unit
NAUN nearest active upstream neighbor
NBP Name Binding Protocol
NCP Network Control Program
NCP Network Control Protocol
NCP Network Core Protocol
NCTE Network Customer Equipment
NEMA National Electrical Manufacturers Association
NetBIOS Network Basic Input/Output System
NetRPC Network Remote Procedure Calls
NFS Network File System
NI network interface
NIC Network Information Center
NIC network interface card
NICE Network Information and Control Exchange
NIO native input/output
NL new line
NLPID network layer protocol ID
NMVT network management vector transport
NN network node
NOC network operations center
NRM normal response mode
NRZ non-return-to-zero
NRZI non-return-to-zero inverted
NS/2 Networking Services/2
NSFNET National Science Foundation NETwork
NUA network user address
NUI network user identification
NVRAM non-volatile random access memory
NZS New Zealand Standard
OA Outgoing Access
OCS outboard communication server; on-card sequencer
ODI Open Datalink Interface
ODM object data manager

OEM original equipment manufacturer

OS/2 Operating System/2

OSI open systems interconnection

OSPF Open Shortest Path First

OSPFase Open Shortest Path First autonomous system external

PAL programmable array logic

PAP Password Authentication Protocol

PAP Printer Access Protocol

PC personal computer

PCSA Personal Computing Systems Architecture

PdAt Predefined Attributes

PDU protocol data unit

PIU path information unit

PMX Presentation Management X–Server

POR power-on reset

POS programmable option select

POST power-on self-test

PPP Point-to-Point Protocol

PROM programmable read-only memory

PRPQ programming request for price quotation

PRTS permanent request to send

PS/2 Personal System/2

PSDN packet switching data network

PSE packet switching equipment

PSP portable service platform

PSS packet switch stream

PTF program temporary fix

PTY pseudo teletype port

PU physical unit

PVC permanent virtual circuit

QLLC qualified link level control

RAM random access memory

REM ring error monitor

REXEC Remote Execution Protocol

RFC Request for Comments

RFI radio frequency interference

RH request header

RI routing information

RIP Routing Information Protocol

RISC reduced instruction-set computer

RLBT remote loopback test

RLSD received line signal detector

RNN reporting network node

RNR receive not ready

ROM read-only memory

ROS read-only storage

RPOA Recognized Private Operating Agency

RPS ring parameter server

RPQ request for price quotation

RR receive ready

RSCV route selection control vector

RSH Remote Shell Protocol

RSN resource sequence number

RTMP Routing Table Maintenance Protocol

RTP RouTing update Protocol

RU request/response unit

SA source address

SABS South African Bureau of Standards

SAP service access point

SAP Service Advertising Protocol

SABME set asynchronous balanced mode extended

SCRLL scroll

SCSI small computer systems interface

SDLC synchronous data link control

SELV safety extra low voltage

SEV Schweizerischer Elektrotechnischer Verein

SII Standards Institution of Israel

SIMM single inline memory module

SIO serial input/output

SIP single inline package

SLA serial link adapter

SLSS System Library Subscription Service

SMI Structure of Management Information

SNA Systems Network Architecture

SNA/MS Systems Network Architecture Management Services

SNAP Subnetwork Access Protocol

SNMP Simple Network Management Protocol

SOC sphere of control

SPP Sequenced Packet Protocol

SPX Sequenced Packet Exchange

SRAM static random access memory

SRN service request number

SRT source routing transparent (bridging)

SRTB source routing to transparent bridging

SR-TB source routing to transparent bridging

SSAP source service access point

SSCP system services control point

STP spanning tree protocol

STP shielded twisted pair

SVC switched virtual circuit

TCP Transmission Control Protocol

TCP/IP Transmission Control Protocol/Internet Protocol

TDU topology database update

TG transmission group

TLAP TokenTalk Link Access Protocol

TR terminal ready

TRB transparent bridging

TT terminal timing

UA unnumbered acknowledgment

UDP User Datagram Protocol

UI unnumbered information

UL Underwriter's Laboratories

UPS uninterruptible power supply

V AC volts alternating current

VAX virtual address extension

VCCI Voluntary Control Council for Interference

VGA video graphics adapter

VINES VIrtual NEtworking System

VMS virtual memory system

VPD vital product data

VRN virtual routing node

VTAM Virtual Telecommunications Access Method

WAN wide area network

X.25 packet-switched networks

XID exchange identification

XNS Xerox Network Systems

ZIP Zone Information Protocol

ZIT Zone Information Table

Glossary

This glossary includes terms and definitions from:

- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by the symbol (A) after the definition.
- The ANSI/EIA Standard—440-A, *Fiber Optic Terminology*. Copies may be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Definitions are identified by the symbol (E) after the definition.
- The *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- The Network Working Group Request for Comments: 1208.
- The *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994.

The following cross-references are used in this glossary:

Contrast with: This refers to a term that has an opposed or substantively different meaning.

Synonym for: This indicates that the term has the same meaning as a preferred term, which is defined in its proper place in the glossary.

Synonymous with: This is a backward reference from a defined term to all other terms that have the same meaning.

See: This refers the reader to multiple-word terms that have the same last word.

See also: This refers the reader to terms that have a related, but not synonymous, meaning.

Deprecated term for: This indicates that the term should not be used. It refers to a preferred term, which is defined in its proper place in the glossary.

A

AARP. AppleTalk Address Resolution Protocol.

abstract syntax. A data specification that includes all distinctions that are needed in data transmissions, but that omits (abstracts) other details such as those that depend on specific computer architectures. See also *abstract syntax notation 1 (ASN.1)* and *basic encoding rules (BER)*.

abstract syntax notation 1 (ASN.1). The Open Systems Interconnection (OSI) method for abstract syntax specified in ISO 8824. See also *basic encoding rules (BER)*.

ACCESS. In the Simple Network Management Protocol (SNMP), the clause in a Management Information Base (MIB) module that defines the minimum level of support that a managed node provides for an object.

access method. A technique, implemented in software, that controls the flow of information through a network.

acknowledgment. (1) The transmission, by a receiver, of acknowledge characters as an affirmative response to a sender. (T) (2) An indication that an item sent was received.

active. (1) Operational. (2) Pertaining to a node or device that is connected or is available for connection to another node or device.

adapter. A part that electrically or physically connects a device to a computer or to another device.

address. In data communication, the unique code assigned to each device or workstation connected to a network.

address mapping table (AMT). A table, maintained within the AppleTalk router, that provides a current mapping of node addresses to hardware addresses.

address mask. For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an internet address. Synonymous with *subnet mask* and *subnetwork mask*.

address resolution. A method for mapping network-layer addresses to media-specific addresses. See also *Address Resolution Protocol (ARP)* and *AppleTalk Address Resolution Protocol (AARP)*.

Address Resolution Protocol (ARP). In the Internet suite of protocols, the protocol that dynamically maps between Internet addresses and the addresses used by a supporting metropolitan or local area network such as Ethernet or token-ring.

addressing. In data communication, the way in which a station selects the station to which it is to send data.

Advanced Peer-to-Peer Networking (APPN). An extension to SNA featuring (a) greater distributed network control that avoids critical hierarchical dependencies, thereby isolating the effects of single points of failure; (b) dynamic exchange of network topology information to foster ease of connection, reconfiguration, and adaptive route selection; (c) dynamic definition of network resources; and (d) automated resource registration and directory lookup. APPN extends the LU 6.2 peer orientation for end-user services to network control and supports multiple LU types, including LU 2, LU 3, and LU 6.2.

Advanced Peer-to-Peer Networking (APPN) end node. A node that provides a broad range of end-user services and supports sessions between its local control point (CP) and the CP in an adjacent network node. It uses these sessions to dynamically register its resources with the adjacent CP (its network node server), to send and receive directory search requests, and to obtain management services. An APPN end node can also attach to a subarea network as a peripheral node or to other end nodes.

Advanced Peer-to-Peer Networking (APPN) network. A collection of interconnected network nodes and their client end nodes.

Advanced Peer-to-Peer Networking (APPN) network node. A node that offers a broad range of end-user services and that can provide the following:

- Distributed directory services, including registration of its domain resources to a central directory server
- Topology database exchanges with other APPN network nodes, enabling network nodes throughout the network to select optimal routes for LU-LU sessions based on requested classes of service
- Session services for its local LUs and client end nodes
- Intermediate routing services within an APPN network

Advanced Peer-to-Peer Networking (APPN) node. An APPN network node or an APPN end node.

AEP. AppleTalk Echo Protocol.

agent. A system that assumes an agent role.

AIX. Advanced Interactive Executive.

all-stations address. Synonym for *broadcast address.*

AMA. Arbitrary MAC addressing.

American National Standards Institute (ANSI). An organization consisting of producers, consumers, and general interest groups, that establishes the procedures by which accredited organizations create and maintain voluntary industry standards in the United States. (A)

AMT. Address mapping table.

analog. (1) Pertaining to data consisting of continuously variable physical quantities. (A) (2) Contrast with *digital.*

ANSI. American National Standards Institute.

API. (1) Application program interface. (2) Application programming interface.

AppleTalk. A network protocol developed by Apple Computer, Inc. This protocol is used to interconnect network devices, which can be a mixture of Apple and non-Apple products.

AppleTalk Address Resolution Protocol (AARP). In AppleTalk networks, a protocol that a) translates AppleTalk node addresses into hardware addresses and b) reconciles addressing discrepancies in networks that support more than one set of protocols.

AppleTalk Echo Protocol (AEP). In AppleTalk networks, a protocol that provides a node destination test function by means of a send and receive transaction where the packet received at the source node is identical to the packet sent to the destination node.

AppleTalk Transaction Protocol (ATP). In AppleTalk networks, a protocol that provides client/server request and response functions for hosts accessing the Zone Information Protocol (ZIP) for zone information.

application. A collection of software components used to perform specific types of user-oriented work on a computer.

application program interface (API). A functional interface used by an executing application program to access the specific functions and services provided by an underlying operating system or service program.

application programming interface (API). (1) The set of programming language constructs or statements that can be coded in an application program to obtain the specific functions and services provided by an underlying operating system or service program. (2) In VTAM, the language structure used in control blocks so

that application programs can reference them and be identified to VTAM.

APPN. Advanced Peer-to-Peer Networking.

APPN network. See *Advanced Peer-to-Peer Networking (APPN) network.*

APPN network node. See *Advanced Peer-to-Peer Networking (APPN) network node.*

APPN node. See *Advanced Peer-to-Peer Networking (APPN) node.*

arbitrary MAC addressing (AMA). In DECnet architecture, an addressing scheme used by DECnet Phase IV-Prime that supports universally administered addresses and locally administered addresses.

area. In Internet and DECnet routing protocols, a subset of a network or gateway grouped together by definition of the network administrator. Each area is self-contained; knowledge of an area's topology remains hidden from other areas.

ARP. Address Resolution Protocol.

ASCII (American National Standard Code for Information Interchange). The standard code, using a coded character set consisting of 7-bit coded characters (8 bits including parity check), that is used for information interchange among data processing systems, data communication systems, and associated equipment. The ASCII set consists of control characters and graphic characters. (A)

ASN.1. Abstract syntax notation 1.

ASYNC. Asynchronous.

asynchronous (ASYNC). Pertaining to two or more processes that do not depend upon the occurrence of specific events such as common timing signals. (T)

ATP. AppleTalk Transaction Protocol.

attachment unit interface (AUI). In a local area network, the interface between the medium attachment unit and the data terminal equipment within a data station. (I) (A)

AUI. Attachment unit interface.

autonomous system. In TCP/IP, a group of networks and routers under one administrative authority. These networks and routers cooperate closely to propagate network reachability (and routing) information among themselves using an interior gateway protocol of their choice.

autonomous system number. In TCP/IP, a number assigned to an autonomous system by the same central authority that also assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

basic encoding rules (BER). The rules specified in ISO 8825 for encoding data units described in abstract syntax notation 1 (ASN.1). The rules specify the encoding technique, not the abstract syntax.

basic information unit (BIU). In SNA, the unit of data and control information passed between half-sessions. It consists of a request/response header (RH) followed by a request/response unit (RU).

Basic Input/Output System (BIOS). Code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

baud. (1) A unit of signaling speed equal to the number of discrete conditions or signal events per second; for example, one baud equals one-half dot cycle per second in Morse code, one bit per second in a train of binary signals, and one 3-bit value per second in a train of signals each of which can assume one of eight different states. (A) (2) In asynchronous transmission, the unit of modulation rate corresponding to one unit interval per second; that is, if the duration of the unit interval is 20 milliseconds, the modulation rate is 50 baud. (A)

BER. Basic encoding rules.

BGP. Border Gateway Protocol.

BGP group. An autonomous system made up of neighbors that be configured or learned. The neighbors have the same group type, such as external, test, internal, or Interior Gateway Protocol.

BIOS. Basic Input/Output System. See also *NetBIOS.*

bit map. (1) A coded representation in which each bit, or group of bits, represents or corresponds to an item; for example, a configuration of bits in main storage in which each bit indicates whether a peripheral device or a storage block is available or in which each group of bits corresponds to one pixel of a display image. (2) A pixmap with a depth of one bit plane.

BIU. Basic information unit.

block. A string of data elements recorded or transmitted as a unit. The elements may be characters, words, or physical records. (T)

Border Gateway Protocol (BGP). An Internet Protocol (IP) routing protocol used between domains and autonomous systems. Contrast with *Exterior Gateway Protocol (EGP)*.

border router. In Internet communications, a router, positioned at the edge of an autonomous system, that communicates with a router that is positioned at the edge of a different autonomous system.

bps. Bits per second.

bridge. A functional unit that interconnects multiple LANs (locally or remotely) that use the same logical link control protocol but that can use different medium access control protocols. A bridge forwards a frame to another bridge based on the medium access control (MAC) address.

bridging. In LANs, the forwarding of a frame from one LAN segment to another. The destination is specified by the medium access control (MAC) sublayer address encoded in the destination address field of the frame header.

broadcast. (1) Transmission of the same data to all destinations. (T) (2) Simultaneous transmission of data to more than one destination. Contrast with *multicast*.

broadcast address. In SDLC, a station address (eight 1's) reserved as an address common to all stations on a link. Synonymous with *all-stations address*.

bus. (1) A facility for transferring data between several devices located between two end points, only one device being able to transmit at a given moment. (T) (2) A computer configuration in which processors are interconnected in series.

button. A word or picture on the screen that can be selected. Once selected and activated, a button begins an action in the same manner that pressing a key on the keyboard can begin an action.

C

cache. (1) A special-purpose buffer storage, smaller and faster than main storage, used to hold a copy of instructions and data obtained from main storage and likely to be needed next by the processor. (T) (2) A buffer storage that contains frequently accessed instructions and data; it is used to reduce access time. (3) An optional part of the directory database in network nodes where frequently used directory information may be stored to speed directory searches. (4) To place, hide, or store in a cache.

calling. (1) The process of transmitting selection signals in order to establish a connection between data stations. (I) (A) (2) In X.25 communications, pertaining to the location or user that makes a call.

CALLOUT. The logical channel type on which the data terminal equipment (DTE) can send a call, but cannot receive one.

carrier. An electric or electromagnetic wave or pulse train that may be varied by a signal bearing information to be transmitted over a communication system. (T)

carrier sense. In a local area network, an ongoing activity of a data station to detect whether another station is transmitting. (T)

carrier sense multiple access with collision detection (CSMA/CD). A protocol that requires carrier sense and in which a transmitting data station that detects another signal while transmitting, stops sending, sends a jam signal, and then waits for a variable time before trying again. (T) (A)

CCITT. International Telegraph and Telephone Consultative Committee. An organization (one of four permanent organs of the International Telecommunication Union [ITU], headquartered in Geneva, Switzerland) that is concerned with the problems relating to international telephony and telegraphy. The CCITT Plenary Assembly meets at regular intervals to prepare a list of technical questions related to telephone and telegraph services. The Assembly assigns these questions to study groups, which then prepare recommendations to be presented at the next plenary meeting. Approved recommendations are published for the use of engineers, scientists, and manufacturers around the world.

central processing unit (CPU). The part of a computer that includes the circuits that control the interpretation and execution of instructions.

Note: A CPU is the circuitry and storage that executes instructions. Traditionally, the complete processing unit was often regarded as the CPU, whereas today the CPU is often a microchip. In either case, the centrality of a processor or processing unit depends on the configuration of the system or network in which it is used.

change management. The process of planning (for example, scheduling) and controlling (for example, distributing, installing, and tracking) changes in an SNA network.

channel. (1) A path along which signals can be sent, for example, data channel, output channel. (A) (2) A functional unit, controlled by the processor, that handles the transfer of data between processor storage and local peripheral equipment. See *input/output channel*.

channel service unit (CSU). A unit that provides the interface to a digital network. The CSU provides line conditioning (or equalization) functions, which keep the signal's performance consistent across the channel bandwidth; signal reshaping, which constitutes the binary pulse stream; and loopback testing, which includes the transmission of test signals between the CSU and the network carrier's office channel unit. See *data service unit (DSU).*

checksum. (1) The sum of a group of data associated with the group and used for checking purposes. (T) (2) In error detection, a function of all bits in a block. If the written and calculated sums do not agree, an error is indicated. (3) On a diskette, data written in a sector for error detection purposes; a calculated checksum that does not match the checksum of data written in the sector indicates a bad sector. The data are either numeric or other character strings regarded as numeric for the purpose of calculating the checksum.

circuit. (1) One or more conductors through which an electric current can flow. See *physical circuit* and *virtual circuit.* (2) A logic device.

circuit switching. (1) A process that, on demand, connects two or more data terminal equipment (DTEs) and permits the exclusive use of a data circuit between them until the connection is released. (I) (A) (2) Synonymous with *line switching.*

class. In object-oriented design or programming, a group of objects that share a common definition and that therefore share common properties, operations, and behavior. Members of the group are called instances of the class.

client. (1) A functional unit that receives shared services from a server. (T) (2) A user.

closed user group (CUG). In data communication, a group of users who can communicate with other users in the group, but not with users outside the group.

Note: A data terminal equipment (DTE) may belong to more than one closed user group.

collision. An unwanted condition that results from concurrent transmissions on a channel. (T)

collision detection. In carrier sense multiple access with collision detection (CSMA/CD), a signal indicating that two or more stations are transmitting simultaneously.

community. In the Simple Network Management Protocol (SNMP), an administrative relationship between entities.

community name. In the Simple Network Management Protocol (SNMP), a string of octets identifying a community.

component. Hardware or software that is part of a functional unit.

configuration. (1) The manner in which the hardware and software of an information processing system are organized and interconnected. (T) (2) The devices and programs that make up a system, subsystem, or network.

configuration file. A file that specifies the characteristics of a system device or network.

configuration parameter. A variable in a configuration definition, the values of which can characterize the relationship of a product to other products in the same network or can define characteristics of the product itself.

congestion. See *network congestion.*

connection. In data communication, an association established between functional units for conveying information. (I) (A)

connectivity. (1) The capability of a system or device to be attached to other systems or devices without modification. (T) (2) The capability to attach a variety of functional units without modifying them.

control point (CP). (1) A component of an APPN or LEN node that manages the resources of that node. In an APPN node, the CP is capable of engaging in CP-CP sessions with other APPN nodes. In an APPN network node, the CP also provides services to adjacent end nodes in the APPN network. (2) A component of a node that manages resources of that node and optionally provides services to other nodes in the network. Examples are a system services control point (SSCP) in a type 5 subarea node, a network node control point (NNCP) in an APPN network node, and an end node control point (ENCP) in an APPN or LEN end node. An SSCP and an NNCP can provide services to other nodes.

control point management services (CPMS). A component of a control point, consisting of management services function sets, that provides facilities to assist in performing problem management, performance and accounting management, change management, and configuration management. Capabilities provided by the CPMS include sending requests to physical unit management services (PUMS) to test system resources, collecting statistical information (for example, error and performance data) from PUMS about the system resources, and analyzing and presenting test results and statistical information collected about the

system resources. Analysis and presentation responsibilities for problem determination and performance monitoring can be distributed among multiple CPMSs.

control point management services unit (CP-MSU). The message unit that contains management services data and flows between management services function sets. This message unit is in general data stream (GDS) format. See also *management services unit (MSU)* and *network management vector transport (NMVT).*

CP. Control point.

CP-MSU. Control point management services unit.

CPMS. Control point management services.

CPU. Central processing unit.

CSMA/CD. Carrier sense multiple access with collision detection.

CSU. Channel service unit.

CUG. Closed user group.

D

daemon. A program that runs unattended to perform a standard service. Some daemons are triggered automatically to perform their task; others operate periodically.

DASD. Direct access storage device.

data circuit. (1) A pair of associated transmit and receive channels that provide a means of two-way data communication. (I) (2) In SNA, synonym for *link connection.* (3) See also *physical circuit* and *virtual circuit.*

Notes:

1. Between data switching exchanges, the data circuit may include data circuit-terminating equipment (DCE), depending on the type of interface used at the data switching exchange.
2. Between a data station and a data switching exchange or data concentrator, the data circuit includes the data circuit-terminating equipment at the data station end, and may include equipment similar to a DCE at the data switching exchange or data concentrator location.

data circuit-terminating equipment (DCE). In a data station, the equipment that provides the signal conversion and coding between the data terminal equipment (DTE) and the line. (I)

Notes:

1. The DCE may be separate equipment or an integral part of the DTE or of the intermediate equipment.
2. A DCE may perform other functions that are usually performed at the network end of the line.

data communication. (1) Transfer of data among functional units by means of data transmission according to a protocol. (T) (2) The transmission, reception, and validation of data. (A)

data link connection identifier (DLCI). The numeric identifier of a frame-relay subport or PVC segment in a frame-relay network. Each subport in a single frame-relay port has a unique DLCI. The following table, excerpted from the American National Standards Institute (ANSI) Standard T1.618 and the International Telegraph and Telephone Consultative Committee (CCITT) Standard Q.922, indicates the functions associated with certain DLCI values:

DLCI Values	Function
0	in-channel signaling
1–15	reserved
16–991	assigned using frame-relay connection procedures
992–1007	layer 2 management of frame-relay bearer service
1008–1022	reserved
1023	in-channel layer management

data link control (DLC). A set of rules used by nodes on a data link (such as an SDLC link or a token ring) to accomplish an orderly exchange of information.

data link control (DLC) layer. In SNA, the layer that consists of the link stations that schedule data transfer over a link between two nodes and perform error control for the link. Examples of data link control are SDLC for serial-by-bit link connection and data link control for the System/370 channel.

Note: The DLC layer is usually independent of the physical transport mechanism and ensures the integrity of data that reaches the higher layers.

data link layer. In the Open Systems Interconnection reference model, the layer that provides services to transfer data between entities in the network layer over a communication link. The data link layer detects and possibly corrects errors that may occur in the physical layer. (T) See also *Open Systems Interconnection (OSI) reference model.*

data link level. (1) In the hierarchical structure of a data station, the conceptual level of control or processing logic between high level logic and the data link that maintains control of the data link. The data link

level performs such functions as inserting transmit bits and deleting receive bits; interpreting address and control fields; generating, transmitting, and interpreting commands and responses; and computing and interpreting frame check sequences. See also *packet level* and *physical level.* (2) In X.25 communications, synonym for *frame level.*

data link switching (DLSw). A method of transporting network protocols that use IEEE 802.2 logical link control (LLC) type 2. SNA and NetBIOS are examples of protocols that use LLC type 2. See also *encapsulation* and *spoofing.*

data network. An arrangement of data circuits and switching facilities for establishing connections between data terminal equipment. (I)

data service unit (DSU). A device that provides a digital data service interface directly to the data terminal equipment. The DSU provides loop equalization, remote and local testing capabilities, and a standard EIA/CCITT interface.

data stream. A continuous stream of data elements being transmitted, or intended for transmission, in character or binary-digit form, using a defined format.

data switching exchange (DSE). The equipment installed at a single location to provide switching functions, such as circuit switching, message switching, and packet switching. (I)

data terminal equipment (DTE). That part of a data station that serves as a data source, data sink, or both. (I) (A)

data terminal ready (DTR). A signal to the modem used with the EIA 232 protocol.

datagram. (1) In packet switching, a self-contained packet, independent of other packets, that carries information sufficient for routing from the originating data terminal equipment (DTE) to the destination DTE without relying on earlier exchanges between the DTEs and the network. (I) (2) In TCP/IP, the basic unit of information passed across the Internet environment. A datagram contains a source and destination address along with the data. An Internet Protocol (IP) datagram consists of an IP header followed by the transport layer data. See also *packet* and *segment.*

Datagram Delivery Protocol (DDP). In AppleTalk networks, a protocol that provides network connectivity by means of connectionless socket-to-socket delivery service on the internet layer.

DCE. Data circuit-terminating equipment.

DDP. Datagram Delivery Protocol.

DECnet. A network architecture that defines the operation of a family of software modules, databases, and hardware components typically used to tie Digital Equipment Corporation systems together for resource sharing, distributed computation, or remote system configuration. DECnet network implementations follow the Digital Network Architecture (DNA) model.

designated router. A router that informs end nodes of the existence and identity of other routers. The selection of the designated router is based upon the router with the highest priority. When several routers share the highest priority, the router with the highest station address is selected.

destination node. The node to which a request or data is sent.

destination service access point (DSAP). In SNA and TCP/IP, a logical address that allows a system to route data from a remote device to the appropriate communications support. Contrast with *source service access point (SSAP).*

device. A mechanical, electrical, or electronic contrivance with a specific purpose.

digital. (1) Pertaining to data that consist of digits. (T)
(2) Pertaining to data in the form of digits. (A)
(3) Contrast with *analog.*

Digital Network Architecture (DNA). The model for all DECnet hardware and software implementations.

direct access storage device (DASD). A device in which access time is effectively independent of the location of the data.

direct memory access (DMA). The system facility that allows a device on the Micro Channel bus to get direct access to the system or bus memory without the intervention of the system processor.

directory. A table of identifiers and references to the corresponding items of data. (I) (A)

directory service (DS). An application service element that translates the symbolic names used by application processes into the complete network addresses used in an OSI environment. (T)

directory services (DS). A control point component of an APPN node that maintains knowledge of the location of network resources.

disabled. (1) Pertaining to a state of a processing unit that prevents the occurrence of certain types of interruptions. (2) Pertaining to the state in which a transmission control unit or audio response unit cannot accept incoming calls on a line.

DLC. Data link control.

DLCI. Data link connection identifier.

DLSw. Data link switching.

DMA. Direct memory access.

DNA. Digital Network Architecture.

DNS. Domain name system.

domain. (1) That part of a computer network in which the data processing resources are under common control. (T) (2) In the Internet, a part of a naming hierarchy in which the domain name consists of a sequence of names (labels) separated by periods (dots). (3) In Open Systems Interconnection (OSI), a part of a distributed system or a set of managed objects to which a common policy applies.

domain name system (DNS). The online distributed database system used to map domain names to internet addresses.

DR. In SNA, definite response.

DS. (1) Directory service. (2) Directory services.

DSAP. Destination service access point.

DSE. Data switching exchange.

DSU. Data service unit.

DTE. Data terminal equipment. (A)

DTR. Data terminal ready.

dump. (1) Data that has been dumped. (T) (2) To copy the contents of all or part of virtual storage for the purpose of collecting error information.

E

EBCDIC. Extended binary-coded decimal interchange code. A coded character set of 256 8-bit characters.

echo. In data communication, a reflected signal on a communications channel. On a communications terminal, each signal is displayed twice, once when entered at the local terminal and again when returned over the communications link. This allows the signals to be checked for accuracy.

EGP. Exterior Gateway Protocol.

EIA. Electronic Industries Association.

EIA 232. In data communications, a specification of the Electronic Industries Association (EIA) that defines the interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE), using serial binary data interchange.

Electronic Industries Association (EIA). An organization of electronics manufacturers that advances the technological growth of the industry, represents the views of its members, and develops industry standards.

enable. To make functional.

enabled. (1) Pertaining to a state of the processing unit that allows the occurrence of certain types of interruptions. (2) Pertaining to the state in which a transmission control unit or an audio response unit can accept incoming calls on a line.

encapsulation. In communications, a technique used by layered protocols by which a layer adds control information to the protocol data unit (PDU) from the layer it supports. In this respect, the layer encapsulates the data from the supported layer. In the Internet suite of protocols, for example, a packet would contain control information from the physical layer, followed by control information from the network layer, followed by the application protocol data. See also *data link switching*.

entry point (EP). In SNA, a type 2.0, type 2.1, type 4, or type 5 node that provides distributed network management support. It sends network management data about itself and the resources it controls to a focal point for centralized processing, and it receives and executes focal-point initiated commands to manage and control its resources.

EP. Entry point.

ER. (1) Explicit route. (2) Exception response.

Ethernet. A 10-Mbps baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and delayed retransmission. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD).

exception. An abnormal condition such as an I/O error encountered in processing a data set or a file.

exception response (ER). In SNA, a protocol requested in the form-of-response-requested field of a request header that directs the receiver to return a response only if the request is unacceptable as received or cannot be processed; that is, a negative response, but not a positive response, can be returned. Contrast with *definite response* and *no response*.

exchange identification (XID). A specific type of basic link unit that is used to convey node and link

characteristics between adjacent nodes. XIDs are exchanged between link stations before and during link activation to establish and negotiate link and node characteristics, and after link activation to communicate changes in these characteristics.

explicit route (ER). In SNA, a series of one or more transmission groups that connect two subarea nodes. An explicit route is identified by an origin subarea address, a destination subarea address, an explicit route number, and a reverse explicit route number. Contrast with *virtual route (VR)*.

exterior gateway. In Internet communications, a gateway on one autonomous system that communicates with another autonomous system. Contrast with *interior gateway*.

Exterior Gateway Protocol (EGP). In the Internet suite of protocols, a protocol, used between domains and autonomous systems, that enables network reachability information to be advertised and exchanged. IP network addresses in one autonomous system are advertised to another autonomous system by means of EGP-participating routers. Contrast with *Border Gateway Protocol (BGP)*.

F

FDDI. Fiber Distributed Data Interface.

Fiber Distributed Data Interface (FDDI). An American National Standards Institute (ANSI) standard for a 100-megabit-per-second LAN using optical fiber cables.

field replaceable unit (FRU). An assembly that is replaced in its entirety when any one of its components fails. In some cases, a field replaceable unit may contain other field replaceable units.

File Transfer Protocol (FTP). In the Internet suite of protocols, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter. A device or program that separates data, signals, or material in accordance with specified criteria. (A)

focal point (FP). See *management services focal point (MSFP)*.

FP. Focal point.

fragmentation. The process of dividing a datagram into smaller parts, or fragments, to match the capabilities of the physical medium over which it is to be transmitted. See also *segmenting*.

frame. (1) In Open Systems Interconnection architecture, a data structure pertaining to a particular area of knowledge and consisting of slots that can accept the values of specific attributes and from which inferences can be drawn by appropriate procedural attachments. (T) (2) The unit of transmission in some local area networks, including the IBM Token-Ring Network. It includes delimiters, control characters, information, and checking characters. (3) In SDLC, the vehicle for every command, every response, and all information that is transmitted using SDLC procedures.

frame level. See *link level*.

frame relay. (1) An interface standard describing the boundary between a user's equipment and a fast-packet network. In frame-relay systems, flawed frames are discarded; recovery comes end-to-end rather than hop-by-hop. (2) A technique derived from the integrated services digital network (ISDN) D channel standard. It assumes that connections are reliable and dispenses with the overhead of error detection and control within the network.

frequency. The rate of signal oscillation, expressed in hertz.

FRU. Field replaceable unit.

FTP. File Transfer Protocol.

G

gateway. (1) A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. (T) (2) In the IBM Token-Ring Network, a device and its associated software that connect a local area network to another local area network or a host that uses different logical link protocols.

GDS. General data stream.

general data stream (GDS). The data stream used for conversations in LU 6.2 sessions.

general data stream (GDS) variable. A type of RU substructure that is preceded by an identifier and a length field and includes either application data, user control data, or SNA-defined control data.

H

hard disk. (1) A rigid magnetic disk such as the internal disks used in the system units of personal computers and in external hard disk drives. (2) A rigid disk used in a hard disk drive.

HDLC. High-level data link control.

header. (1) System-defined control information that precedes user data. (2) The portion of a message that contains control information for the message such as one or more destination fields, name of the originating station, input sequence number, character string indicating the type of message, and priority level for the message.

hierarchy. The resource types, display types, and data types that make up the organization, or levels, in a network.

high-level data link control (HDLC). In data communication, the use of a specified series of bits to control data links in accordance with the International Standards for HDLC: ISO 3309 Frame Structure and ISO 4335 Elements of Procedures.

hop. (1) In APPN, a portion of a route that has no intermediate nodes. It consists of only a single transmission group connecting adjacent nodes. (2) To the routing layer, the logical distance between two nodes in a network.

host. In the Internet suite of protocols, an end system. The end system can be any workstation; it does not have to be a mainframe.

I

i-node. In the AIX operating system, the internal structure that describes the individual files in the operating system; there is one i-node for each file. An i-node contains the node, type, owner, and location of a file. A table of i-nodes is stored near the beginning of a file system.

I/O. Input/output.

IAB. Internet Architecture Board.

ICMP. Internet Control Message Protocol.

ICP. Internet Control Protocol.

IEEE. Institute of Electrical and Electronics Engineers.

IETF. Internet Engineering Task Force.

IGP. Interior Gateway Protocol.

InARP. Inverse Address Resolution Protocol.

inbound. In communications, data that is received from the network.

information (I) frame. A frame in I format used for numbered information transfer.

inoperative. The condition of a resource that has been active but is not currently active. A resource may be inoperative for reasons such as the following: a) it may have failed, b) it may have received an INOP request, or c) it may be suspended while a reactivate command is being processed. See also *inactive*.

input/output channel. In a data processing system, a functional unit that handles transfer of data between internal and peripheral equipment. (I) (A)

insert. In LANs, to make an attaching device an active part of the LAN.

integrated services digital network (ISDN). A digital end-to-end telecommunication network that supports multiple services including, but not limited to, voice and data.

Note: ISDNs are used in public and private network architectures.

interface. (1) A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics, as appropriate. The concept includes the specification of the connection of two devices having different functions. (T) (2) Hardware, software, or both, that links systems, programs, or devices.

interior gateway. In Internet communications, a gateway that communicates only with its own autonomous system. Contrast with *exterior gateway*.

Interior Gateway Protocol (IGP). In the Internet suite of protocols, a protocol used to propagate network reachability and routing information within an autonomous system. Examples of IGPs are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

intermediate session routing (ISR). A type of routing function within an APPN network node that provides session-level flow control and outage reporting for all sessions that pass through the node but whose end points are elsewhere.

International Organization for Standardization (ISO). An organization of national standards bodies from various countries established to promote development of standards to facilitate international exchange of goods and services, and develop

cooperation in intellectual, scientific, technological, and economic activity.

internet. A collection of networks interconnected by a set of routers that allow them to function as a single, large network. See also *Internet*.

Internet. The internet administered by the Internet Architecture Board (IAB), consisting of large national backbone networks and many regional and campus networks all over the world. The Internet uses the Internet suite of protocols.

Internet address. See *IP address*.

Internet Architecture Board (IAB). The technical body that oversees the development of the Internet suite of protocols that are known as TCP/IP.

Internet Control Message Protocol (ICMP). The protocol used to handle errors and control messages in the Internet Protocol (IP) layer. Reports of problems and incorrect datagram destinations are returned to the original datagram source. ICMP is part of the Internet Protocol.

Internet Control Protocol (ICP). The VIrtual NEtworking System (VINES) protocol that provides exception notifications, metric notifications, and PING support. See also *RouTing update Protocol (RTP)*.

Internet Engineering Task Force (IETF). The task force of the Internet Architecture Board (IAB) that is responsible for solving the short-term engineering needs of the Internet.

Internet Protocol (IP). A connectionless protocol that routes data through a network or interconnected networks. IP acts as an intermediary between the higher protocol layers and the physical network. However, this protocol does not provide error recovery and flow control and does not guarantee the reliability of the physical network.

Internetwork Packet Exchange (IPX). The network protocol used to connect Novell's servers, or any workstation or router that implements IPX, with other workstations. Although similar to the Internet Protocol (IP), IPX uses different packet formats and terminology. See also *Xerox Network Systems (XNS)*.

Inverse Address Resolution Protocol (InARP). In the Internet suite of protocols, the protocol used for locating a protocol address through the known hardware address. In a frame-relay context, the data link connection identifier (DLCI) is synonymous with the known hardware address.

IP. Internet Protocol.

IP address. The 32-bit address defined by the Internet Protocol, standard 5, Request for Comment (RFC) 791. It is usually represented in dotted decimal notation.

IP router. A device in an IP internet that is responsible for making decisions about the paths over which network traffic will flow. Routing protocols are used to gain information about the network and to determine the best route over which the datagram should be forwarded toward the final destination. The datagrams are routed based on IP destination addresses.

IPX. Internetwork Packet Exchange.

ISDN. Integrated services digital network.

ISO. International Organization for Standardization.

ISR. Intermediate session routing.

K

Kbps. Kilobits per second.

L

LAN. Local area network.

LAPB. Link access protocol-balanced.

layer. (1) In network architecture, a group of services that is complete from a conceptual point of view, that is one out of a set of hierarchically arranged groups, and that extends across all systems that conform to the network architecture. (T) (2) In the Open Systems Interconnection reference model, one of seven conceptually complete, hierarchically arranged groups of services, functions, and protocols, that extend across all open systems. (T) (3) In SNA, a grouping of related functions that are logically separate from the functions in other groups. Implementation of the functions in one layer can be changed without affecting functions in other layers.

LEN. Low-entry networking.

line switching. Synonym for *circuit switching*.

link. The combination of the link connection (the transmission medium) and two link stations, one at each end of the link connection. A link connection can be shared among multiple links in a multipoint or token-ring configuration.

link access protocol-balanced (LAPB). A protocol used for accessing an X.25 network at the link level. LAPB is a duplex, asynchronous, symmetric protocol, used in point-to-point communication.

link-attached. Pertaining to devices that are connected to a controlling unit by a data link. Contrast with *channel-attached*. Synonymous with *remote*.

link connection. The physical equipment providing two-way communication between one link station and one or more other link stations; for example, a telecommunication line and data circuit-terminating equipment (DCE). Synonymous with *data circuit*.

link level. A part of Recommendation X.25 that defines the link protocol used to get data into and out of the network across the full-duplex link connecting the subscriber's machine to the network node. LAP and LAPB are the link access protocols recommended by the CCITT. See *data link level*.

link-state. In routing protocols, the advertised information about the usable interfaces and reachable neighbors of a router or network. The protocol's topological database is formed from the collected link-state advertisements.

LLC. Logical link control.

LMI. Local management interface.

local. Pertaining to a device accessed directly without use of a telecommunication line. Synonym for *channel-attached*.

local area network (LAN). (1) A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. (T) (2) A network in which a set of devices are connected to one another for communication and that can be connected to a larger network. See also *Ethernet* and *token ring*. (3) Contrast with *metropolitan area network (MAN)* and *wide area network (WAN)*.

local management interface (LMI). See *local management interface (LMI) protocol*.

local management interface (LMI) protocol. In NCP, a set of frame-relay network management procedures and messages used by adjacent frame-relay nodes to exchange line status information over DLCI X'00'. NCP supports both the American National Standards Institute (ANSI) and International Telegraph and Telephone Consultative Committee (CCITT) versions of LMI protocol. These standards refer to LMI protocol as *link integrity verification tests (LIVT)*.

locally administered address. In a local area network, an adapter address that the user can assign to override the universally administered address. Contrast with *universally administered address*.

lock. The means by which integrity of data is ensured by preventing more than one user from accessing or changing the same data or object at the same time.

logical channel. In packet mode operation, a sending channel and a receiving channel that together are used to send and receive data over a data link at the same time. Several logical channels can be established on the same data link by interleaving the transmission of packets.

logical link. A pair of link stations, one in each of two adjacent nodes, and their underlying link connection, providing a single link-layer connection between the two nodes. Multiple logical links can be distinguished while they share the use of the same physical media connecting two nodes. Examples are 802.2 logical links used on local area network (LAN) facilities and LAP E logical links on the same point-to-point physical link between two nodes. The term logical link also includes the multiple X.25 logical channels that share the use of the access link from a DTE to an X.25 network.

logical link control (LLC). The data link control (DLC) LAN sublayer that provides two types of DLC operation for the orderly exchange of information. The first type is connectionless service, which allows information to be sent and received without establishing a link. The LLC sublayer does not perform error recovery or flow control for connectionless service. The second type is connection-oriented service, which requires establishing a link prior to the exchange of information. Connection-oriented service provides sequenced information transfer, flow control, and error recovery.

logical link control (LLC) protocol. In a local area network, the protocol that governs the exchange of transmission frames between data stations independently of how the transmission medium is shared. (T)

Note: The LLC protocol was developed by the IEEE 802 committee and is common to all LAN standards.

logical link control (LLC) protocol data unit. A unit of information exchanged between link stations in different nodes. The LLC protocol data unit contains a destination service access point (DSAP), a source service access point (SSAP), a control field, and user data.

logical unit (LU). A type of network accessible unit that enables end users to gain access to network resources and communicate with each other.

low-entry networking (LEN). A capability of nodes to attach directly to one another using basic peer-to-peer protocols to support multiple and parallel sessions between logical units.

low-entry networking (LEN) end node. A LEN node receiving network services from an adjacent APPN network node.

low-entry networking (LEN) node. A node that provides a range of end-user services, attaches directly to other nodes using peer protocols, and derives network services implicitly from an adjacent APPN network node, that is, without the direct use of CP-CP sessions.

LU. Logical unit.

M

MAC. Medium access control.

MAN. Metropolitan area network.

Management Information Base (MIB). (1) A collection of objects that can be accessed by means of a network management protocol. (2) A definition for management information that specifies the information available from a host or gateway and the operations allowed. (3) In OSI, the conceptual repository of management information within an open system.

management services (MS). Services that assist in the management of systems and networks in areas such as problem management, performance management, business management, operations management, configuration management, and change management.

management services focal point (MSFP). For any given management services discipline (for example, problem determination or response time monitoring), the control point that is responsible for that type of network management data for a sphere of control. This responsibility may include collecting, storing or displaying the data or all of these. (For example, a problem determination focal point is a control point that collects, stores, and displays problem determination data.)

management station. In Internet communications, the system responsible for managing all, or a portion of, a network. The management station communicates with network management agents that reside in the managed node by means of a network management protocol, such as the Simple Network Management Protocol (SNMP).

manager. A system that assumes a manager role.

mapping. The process of converting data that is transmitted in one format by the sender into the data format that can be accepted by the receiver.

mask. (1) A pattern of characters used to control retention or elimination of portions of another pattern of characters. (I) (A) (2) To use a pattern of characters to control retention or elimination of portions of another pattern of characters. (I) (A)

maximum transmission unit (MTU). In LANs, the largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the MTU for Ethernet is 1500 bytes.

Mbps. One million bits per second.

MDS. Multiple-domain support.

MDS-MU. Multiple-domain support message unit.

medium access control (MAC). In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium.

medium access control (MAC) protocol. In a local area network, the protocol that governs access to the transmission medium, taking into account the topological aspects of the network, in order to enable the exchange of data between data stations. (T) See also *logical link control protocol*.

medium access control (MAC) sublayer. In a local area network, the part of the data link layer that applies a medium access method. The MAC sublayer supports topology-dependent functions and uses the services of the physical layer to provide services to the logical link control sublayer. (T)

metric. In Internet communications, a value, associated with a route, which is used to discriminate between multiple exit or entry points to the same autonomous system. The route with the lowest metric is preferred.

metropolitan area network (MAN). A network formed by the interconnection of two or more networks which may operate at higher speed than those networks, may cross administrative boundaries, and may use multiple access methods. (T) Contrast with *local area network (LAN)* and *wide area network (WAN)*.

MIB. (1) MIB module. (2) Management Information Base.

MIB module. In the Simple Network Management Protocol (SNMP), a collection of objects relating to a common management area. See also *Management Information Base (MIB)* and *MIB object*.

MIB object. In the Simple Network Management Protocol (SNMP), an object contained in the Management Information Base (MIB). Synonymous with *MIB variable*.

MIB variable. In the Simple Network Management Protocol (SNMP), a specific instance of a specific data object in a MIB module. Synonym for *MIB object*.

MILNET. The military network that was originally part of ARPANET. It was partitioned from ARPANET in 1984. MILNET provides a reliable network service for military installations.

modem (modulator/demodulator). (1) A functional unit that modulates and demodulates signals. One of the functions of a modem is to enable digital data to be transmitted over analog transmission facilities. (T) (A) (2) A device that converts digital data from a computer to an analog signal that can be transmitted on a telecommunication line, and converts the analog signal received to data for the computer.

monitor. (1) A device that observes and records selected activities within a data processing system for analysis. Possible uses are to indicate significant departure from the norm, or to determine levels of utilization of particular functional units. (T) (2) Software or hardware that observes, supervises, controls, or verifies operations of a system. (A) (3) The function required to initiate the transmission of a token on the ring and to provide soft-error recovery in case of lost tokens, circulating frames, or other difficulties. The capability is present in all ring stations.

MPNP. Multiprotocol Network Program.

MS. Management services.

MSFP. Management services focal point.

MTU. Maximum transmission unit.

multicast. (1) Transmission of the same data to a selected group of destinations. (T) (2) A special form of broadcast in which copies of a packet are delivered to only a subset of all possible destinations.

multiple-domain support (MDS). A technique for transporting management services data between management services function sets over LU-LU and CP-CP sessions. See also *multiple-domain support message unit (MDS-MU)*.

multiple-domain support message unit (MDS-MU). The message unit that contains management services data and flows between management services function sets over the LU-LU and CP-CP sessions used by multiple-domain support. This message unit, as well as the actual management services data that it contains, is in general data stream (GDS) format. See also *control point management services unit (CP-MSU)*, *management services unit (MSU)*, and *network management vector transport (NMVT)*.

Multiprotocol Network Program (MPNP). The IBM software that controls the functions of the IBM 6611 Network Processor. It is a licensed program made up of base code and the Configuration Program.

N

Name Binding Protocol (NBP). In AppleTalk networks, a protocol that provides name translation function from the AppleTalk entity (resource) name (character string) into an AppleTalk internet address (16-bit number) on the transport layer.

name resolution. In Internet communications, the process of mapping a machine name to the corresponding Internet Protocol (IP) address. See also *domain name system (DNS)*.

name server. In Internet communications, the station that translates host names into their respective internet addresses when requested by the stations on the network.

NAU. (1) Network accessible unit.

NAUN. Nearest active upstream neighbor.

NBP. Name Binding Protocol.

NCP. Network Control Program.

nearest active upstream neighbor (NAUN). In the IBM Token-Ring Network, the station sending data directly to a given station on the ring.

neighbor. A router on a common subnetwork that has been designated by a network administrator to receive routing information.

NetBIOS. (1) Network Basic Input/Output System. A standard interface to networks, IBM personal computers (PCs), and compatible PCs, that is used on LANs to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not need to handle the details of LAN data link control (DLC) protocols. (2) See also *BIOS*.

network. (1) A configuration of data processing devices and software connected for information interchange. (2) A group of nodes and the links interconnecting them.

network accessible unit (NAU). A logical unit (LU), physical unit (PU), control point (CP), or system services control point (SSCP). It is the origin or the

destination of information transmitted by the path control network. Synonymous with *network addressable unit*.

network address. According to ISO 7498-3, a name, unambiguous within the OSI environment, that identifies a set of network service access points.

network addressable unit (NAU). Synonym for *network accessible unit*.

network architecture. The logical structure and operating principles of a computer network. (T)

Note: The operating principles of a network include those of services, functions, and protocols.

network congestion. An undesirable overload condition caused by traffic in excess of what a network can handle.

Network Information Center (NIC). In Internet communications, local, regional, and national groups throughout the world who provide assistance, documentation, training, and other services to users.

network layer. In Open Systems Interconnection (OSI) architecture, the layer that is responsible for routing, switching, and link-layer access across the OSI environment.

network management. The process of planning, organizing, and controlling a communication-oriented data processing or information system.

network management vector transport (NMVT). A management services request/response unit (RU) that flows over an active session between physical unit management services and control point management services (SSCP-PU session).

network manager. A program or group of programs that is used to monitor, manage, and diagnose the problems of a network.

network node (NN). Synonym for *Advanced Peer-to-Peer Networking (APPN) network node*.

network operations center (NOC). Any center that has responsibility for the operational aspects of a production network. Examples of NOC tasks are monitoring and control, troubleshooting, and user assistance.

network operator. In a multiple-domain network, a person or program responsible for controlling all domains. Contrast with *domain operator*.

network user address (NUA). In X.25 communications, the X.121 address containing up to 15 binary code digits.

NIC. Network Information Center.

NMVT. Network management vector transport.

NN. Network node.

NOC. Network operations center.

node. (1) In a network, a point at which one or more functional units connect channels or data circuits. (I) (2) Any device, attached to a network, that transmits and receives data.

nonseed router. In AppleTalk networks, a router that acquires network number range and zone list information from a seed router attached to the same network.

notification. An unscheduled, spontaneously generated report of an event that has occurred.

NRZ. Non-return-to-zero recording.

NRZ-1. Non-return-to-zero change-on-ones recording. (I) (A)

NRZI. Non-return-to-zero (inverted) recording. Deprecated term for *non-return-to-zero change-on-ones recording (NRZ-1)*.

NUA. Network user address.

O

object. In object-oriented design or programming, an abstraction consisting of data and the operations associated with that data. See also *class*.

open. (1) A break in an electrical circuit. (2) To make an adapter ready for use.

Open Shortest Path First (OSPF). In the Internet suite of protocols, a function that provides intradomain information transfer. An alternative to the Routing Information Protocol (RIP), OSPF allows the lowest-cost routing and handles routing in large regional or corporate networks.

Open Systems Interconnection (OSI). (1) The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information. (T) (A) (2) The use of standardized procedures to enable the interconnection of data processing systems.

Note: OSI architecture establishes a framework for coordinating the development of current and future standards for the interconnection of computer systems. Network functions are divided into seven layers. Each layer represents a group of related data processing and

communication functions that can be carried out in a standard way to support different applications.

Open Systems Interconnection (OSI) architecture. Network architecture that adheres to that particular set of ISO standards that relates to Open Systems Interconnection. (T)

Open Systems Interconnection (OSI) reference model. A model that describes the general principles of the Open Systems Interconnection, as well as the purpose and the hierarchical arrangement of its seven layers. (T)

OSI. Open Systems Interconnection.

OSPF. Open Shortest Path First.

outbound. In communications, data that is transmitted to the network.

P

packet. In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals, and, possibly, error control information are arranged in a specific format. (I)

packet internet groper (PING). (1) In Internet communications, a program used in TCP/IP networks to test the ability to reach destinations by sending the destinations an Internet Control Message Protocol (ICMP) echo request and waiting for a reply. (2) In communications, a test of reachability.

packet mode operation. Synonym for *packet switching*.

packet switching. (1) The process of routing and transferring data by means of addressed packets so that a channel is occupied only during transmission of a packet. On completion of the transmission, the channel is made available for transfer of other packets. (I) (2) Synonymous with *packet mode operation*. See also *circuit switching*.

page. (1) In a virtual storage system, a fixed-length block that has a virtual address and is transferred as a unit between real storage and auxiliary storage. (I) (A) (2) The information displayed at the same time on the screen of a display device. (3) To replace the information displayed on the screen with prior or subsequent information from the same file.

parallel port. An access point through which a computer transmits or receives data that consists of several bits sent simultaneously on separate wires. Contrast with *serial port*.

parallel transmission groups. Multiple transmission groups between adjacent nodes, with each group having a distinct transmission group number.

path. (1) In a network, any route between any two nodes. A path may include more than one branch. (T) (2) The series of transport network components (path control and data link control) that are traversed by the information exchanged between two network accessible units. See also *explicit route (ER)*, *route extension*, and *virtual route (VR)*.

path control (PC). The function that routes message units between network accessible units in the network and provides the paths between them. It converts the basic information units (BIUs) from transmission control (possibly segmenting them) into path information units (PIUs) and exchanges basic transmission units containing one or more PIUs with data link control. Path control differs by node type: some nodes (APPN nodes, for example) use locally generated session identifiers for routing, and others (subarea nodes) use network addresses for routing.

path cost. In link-state routing protocols, the sum of the link costs along the path between two nodes or networks.

path information unit (PIU). A message unit consisting of a transmission header (TH) alone, or a TH followed by a basic information unit (BIU) or a BIU segment. See also *transmission header*.

pattern-matching character. A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace a pattern-matching character. Synonymous with *global character* and *wildcard character*.

PC. Path control.

PDU. Protocol data unit.

permanent virtual circuit (PVC). In X.25 and frame-relay communications, a virtual circuit that has a logical channel permanently assigned to it at each data terminal equipment (DTE). Call-establishment protocols are not required. Contrast with *switched virtual circuit (SVC)*.

physical circuit. A circuit established without multiplexing. See also *data circuit*. Contrast with *virtual circuit*.

physical unit (PU). The component that manages and monitors the resources (such as attached links and adjacent link stations) associated with a node, as requested by an SSCP via an SSCP-PU session. An SSCP activates a session with the physical unit in order

to indirectly manage, through the PU, resources of the node such as attached links. This term applies to type 2.0, type 4, and type 5 nodes only. See also *peripheral PU* and *subarea PU*.

PING. Packet internet groper.

PIU. Path information unit.

Point-to-Point Protocol (PPP). A protocol that provides a method for encapsulating and transmitting packets over serial point-to-point links.

polling. (1) On a multipoint connection or a point-to-point connection, the process whereby data stations are invited, one at a time, to transmit. (I) (2) Interrogation of devices for such purposes as to avoid contention, to determine operational status, or to determine readiness to send or receive data. (A)

port. (1) An access point for data entry or exit. (2) A connector on a device to which cables for other devices such as display stations and printers are attached. Synonymous with *socket*. (3) The representation of a physical connection to the link hardware. A port is sometimes referred to as an adapter; however, there can be more than one port on an adapter. There may be one or more ports controlled by a single DLC process. (4) In the Internet suite of protocols, a 16-bit number used to communicate between TCP or the User Datagram Protocol (UDP) and a higher-level protocol or application. Some protocols, such as File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP), use the same well-known port number in all TCP/IP implementations. (5) An abstraction used by transport protocols to distinguish among multiple destinations within a host machine.

port number. In Internet communications, the identification of an application entity to the transport service.

PPP. Point-to-Point Protocol.

preferential closed user group (CUG). In X.25 communications, the default closed user group.

problem determination. The process of determining the source of a problem; for example, a program component, machine failure, telecommunication facilities, user or contractor-installed programs or equipment, environmental failure such as a power loss, or user error.

processor. In a computer, a functional unit that interprets and executes instructions. A processor consists of at least an instruction control unit and an arithmetic and logic unit. (T)

protocol. (1) A set of semantic and syntactic rules that determine the behavior of functional units in achieving communication. (I) (2) In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. (T) (3) In SNA, the meanings of, and the sequencing rules for, requests and responses used for managing the network, transferring data, and synchronizing the states of network components. Synonymous with *line control discipline* and *line discipline*. See *bracket protocol* and *link protocol*.

protocol data unit (PDU). A unit of data specified in a protocol of a given layer and consisting of protocol control information of this layer, and possibly user data of this layer. (T)

PU. Physical unit.

PVC. Permanent virtual circuit.

R

read-only memory (ROM). Memory in which stored data cannot be modified by the user except under special conditions.

receive not ready (RNR). In communications, a data link command or response that indicates a temporary condition of being unable to accept incoming frames.

receive not ready (RNR) packet. See *RNR packet*.

received line signal detector (RLSD). A signal defined in the EIA-232 standard that indicates to the data terminal equipment (DTE) that it is receiving a signal from the remote data circuit-terminating equipment (DCE).

Recognized Private Operating Agency (RPOA). Any individual, company, or corporation, other than a government department or service, that operates a telecommunication service and is subject to the obligations undertaken in the Convention of the International Telecommunication Union and in the Regulations; for example, a communication common carrier.

Recommendation X.21. See *X.21*.

Recommendation X.25. See *X.25*.

reduced instruction-set computer (RISC). A computer that uses a small, simplified set of frequently used instructions for rapid execution.

remote. Pertaining to a system, program, or device that is accessed through a telecommunication line. Contrast with *local*. Synonym for *link-attached*.

Remote Execution Protocol (REXEC). A protocol that allows the execution of a command or program on any host in the network. The local host receives the results of the command execution.

remote procedure call (RPC). A facility that a client uses to request the execution of a procedure call from a server. This facility includes a library of procedures and an external data representation.

Request for Comments (RFC). In Internet communications, the document series that describes a part of the Internet suite of protocols and related experiments. All Internet standards are documented as RFCs.

reset. On a virtual circuit, reinitialization of data flow control. At reset, all data in transit are eliminated.

Reverse Address Resolution Protocol (RARP). A TCP/IP protocol that maintains a database of mappings between physical hardware addresses and IP addresses. Contrast with *Address Resolution Protocol (ARP)*.

REX. Route extension.

REXEC. Remote Execution Protocol.

RFC. Request for Comments.

RH. Request/response header.

ring. See *ring network*.

ring network. (1) A network in which every node has exactly two branches connected to it and in which there are exactly two paths between any two nodes. (T) (2) A network configuration in which devices are connected by unidirectional transmission links to form a closed path.

RIP. Routing Information Protocol.

RISC. Reduced instruction-set computer.

rlogin (remote login). A service, offered by Berkeley UNIX-based systems, that allows authorized users of one machine to connect to other UNIX systems across an internet and interact as if their terminals were connected directly. The rlogin software passes information about the user's environment (for example, terminal type) to the remote machine.

RLSD. Received line signal detector.

RNR. Receive not ready.

RNR packet. A packet used by a data terminal equipment (DTE) or by a data circuit-terminating equipment (DCE) to indicate a temporary inability to accept additional packets for a virtual call or permanent virtual circuit.

ROM. Read-only memory. (A)

route. (1) An ordered sequence of nodes and transmission groups (TGs) that represent a path from an origin node to a destination node traversed by the traffic exchanged between them. (2) The path that network traffic uses to get from source to destination.

route bridge. A function of an IBM bridge program that allows two bridge computers to use a telecommunication link to connect two LANs. Each bridge computer is connected directly to one of the LANs, and the telecommunication link connects the two bridge computers.

route extension (REX). In SNA, the path control network components, including a peripheral link, that make up the portion of a path between a subarea node and a network addressable unit (NAU) in an adjacent peripheral node. See also *explicit route (ER)*, *path*, and *virtual route (VR)*.

Route Selection control vector (RSCV). A control vector that describes a route within an APPN network. The RSCV consists of an ordered sequence of control vectors that identify the TGs and nodes that make up the path from an origin node to a destination node.

router. (1) A computer that determines the path of network traffic flow. The path selection is made from several paths based on information obtained from specific protocols, algorithms that attempt to identify the shortest or best path, and other criteria such as metrics or protocol-specific destination addresses. (2) An attaching device that connects two LAN segments, which use similar or different architectures, at the reference model network layer. Contrast with *bridge* and *gateway*. (3) In OSI terminology, a function that determines a path by which an entity can be reached.

routing. (1) The assignment of the path by which a message is to reach its destination. (2) In SNA, the forwarding of a message unit along a particular path through a network, as determined by parameters carried in the message unit, such as the destination network address in a transmission header.

Routing Information Protocol (RIP). In the Internet suite of protocols, an interior gateway protocol used to exchange intradomain routing information and to determine optimum routes between internet hosts. RIP determines optimum routes on the basis of route metrics, not link transmission speed.

routing protocol. A technique used by a router to find other routers and to remain up to date about the best way to get to reachable networks.

routing table. A collection of routes used to direct datagram forwarding or to establish a connection. The information is passed among routers to identify network topology and destination feasibility.

Routing Table Maintenance Protocol (RTMP). In AppleTalk networks, a protocol that provides routing information generation and maintenance on the transport layer by means of the AppleTalk routing table. The AppleTalk routing table directs packet transmission through the internet from source socket to destination socket.

RouTing update Protocol (RTP). The VIrtual NEtworking System (VINES) protocol that maintains the routing database and allows the exchange of routing information between VINES nodes. See also *Internet Control Protocol (ICP).*

RPC. Remote procedure call.

RPOA. Recognized Private Operating Agency.

RSCV. Route Selection control vector.

rsh. A variant of the rlogin command that invokes a command interpreter on a remote UNIX machine and passes the command-line arguments to the command interpreter, skipping the login step completely.

RTMP. Routing Table Maintenance Protocol.

RTP. RouTing update Protocol.

RU. Request/response unit.

S

SAP. (1) Service access point. (2) Service Advertising Protocol.

SCSI. Small computer system interface.

SDLC. Synchronous Data Link Control.

seed router. In AppleTalk networks, a router that maintains configuration data (network range numbers and zone lists, for example) for the network. Each network must have at least one seed router. The seed router must be initially set up using the configurator tool. Contrast with *nonseed router.*

segment. (1) A section of cable between components or devices. A segment may consist of a single patch cable, several patch cables that are connected, or a combination of building cable and patch cables that are connected. (2) In Internet communications, the unit of transfer between TCP functions in different machines. Each segment contains control and data fields; the current byte-stream position and actual data bytes are identified along with a checksum to validate received data.

segmenting. In OSI, a function performed by a layer to map one protocol data unit (PDU) from the layer it supports into multiple PDUs.

sequence number. In communications, a number assigned to a particular frame or packet to control the transmission flow and receipt of data.

serial port. An access point through which a computer transmits or receives data, one bit at a time. Contrast with *parallel port.*

server. A functional unit that provides shared services to workstations over a network; for example, a file server, a print server, a mail server. (T)

service access point (SAP). (1) In Open Systems Interconnection (OSI) architecture, the point at which the services of a layer are provided by an entity of that layer to an entity of the next higher layer. (T) (2) A logical point made available by an adapter where information can be received and transmitted. A single service access point can have many links terminating in it.

Service Advertising Protocol (SAP). In Internetwork Packet Exchange (IPX), a protocol that provides the following:

- A mechanism that allows IPX servers on an internet to advertise their services by name and type. Servers using this protocol have their name, service type, and internet address recorded in all file servers running NetWare.
- A mechanism that allows a workstation to broadcast a query to discover the identities of all servers of all types, all servers of a specific type, or the nearest server of a specific type.
- A mechanism that allows a workstation to query any file server running NetWare to discover the names and addresses of all servers of a specific type.

session. (1) In network architecture, for the purpose of data communication between functional units, all the activities which take place during the establishment, maintenance, and release of the connection. (T) (2) A logical connection between two network accessible units (NAUs) that can be activated, tailored to provide various protocols, and deactivated, as requested. Each session is uniquely identified in a transmission header (TH) accompanying any transmissions exchanged during the session.

Simple Network Management Protocol (SNMP). In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol.

Information on devices managed is defined and stored in the application's Management Information Base (MIB).

small computer system interface (SCSI). A standard hardware interface that enables a variety of peripheral devices to communicate with one another.

SMI. Structure of Management Information.

SNA. Systems Network Architecture.

SNA management services (SNA/MS). The services provided to assist in management of SNA networks.

SNA/MS. SNA management services.

SNAP. Subnetwork Access Protocol.

SNMP. Simple Network Management Protocol.

SOC. Sphere of control.

socket. The abstraction provided by Berkeley Software Distribution (BSD) that serves as an endpoint for communication between processes or applications.

source route bridging. In LANs, a bridging method that uses the routing information field in the IEEE 802.5 medium access control (MAC) header of a frame to determine which rings or token-ring segments the frame must transit. The routing information field is inserted into the MAC header by the source node. The information in the routing information field is derived from explorer packets generated by the source host.

source service access point (SSAP). In SNA and TCP/IP, a logical address that allows a system to send data to a remote device from the appropriate communications support. Contrast with *destination service access point (DSAP)*.

spanning tree. In LAN contexts, the method by which bridges automatically develop a routing table and update that table in response to changing topology to ensure that there is only one route between any two LANs in the bridged network. This method prevents packet looping, where a packet returns in a circuitous route back to the sending router.

sphere of control (SOC). The set of control point domains served by a single management services focal point.

sphere of control (SOC) node. A node directly in the sphere of control of a focal point. A SOC node has exchanged management services capabilities with its focal point. An APPN end node can be a SOC node if it supports the function to exchange management services capabilities.

spoofing. For data links, a technique in which a protocol initiated from an end station is acknowledged and processed by an intermediate node on behalf of the final destination. In IBM 6611 data link switching, for example, SNA frames are encapsulated into TCP/IP packets for transport across a non-SNA wide area network, unpacked by another IBM 6611, and passed to the final destination. A benefit of spoofing is the prevention of end-to-end session timeouts.

SSAP. Source service access point.

station. An input or output point of a system that uses telecommunication facilities; for example, one or more systems, computers, terminals, devices, and associated programs at a particular location that can send or receive data over a telecommunication line.

StreetTalk. In the VIrtual NEtworking System (VINES), a unique network-wide naming and addressing system that allows users to locate and access any resource on the network without knowing the network topology. See also *Internet Control Protocol (ICP)* and *RouTing update Protocol (RTP)*.

Structure of Management Information (SMI). (1) In the Simple Network Management Protocol (SNMP), the rules used to define the objects that can be accessed by means of a network management protocol. (2) In OSI, the set of standards relating to management information. The set includes the *Management Information Model* and the *Guidelines for the Definition of Managed Objects*.

subnet. (1) In TCP/IP, a part of a network that is identified by a portion of the Internet address. (2) Synonym for *subnetwork*.

subnet mask. Synonym for *address mask*.

subnetwork. (1) Any group of nodes that have a set of common characteristics, such as the same network ID. (2) Synonymous with *subnet*.

Subnetwork Access Protocol (SNAP). In LANs, a 5-byte protocol discriminator that identifies the non-IEEE standard protocol family to which a packet belongs. The SNAP value is used to differentiate between protocols that use `$AA` as their source access point (SAP) value.

subnetwork mask. Synonym for *address mask*.

subsystem. A secondary or subordinate system, usually capable of operating independently of, or asynchronously with, a controlling system. (T)

SVC. Switched virtual circuit.

switched connection. A mode of operating a data link in which a circuit or channel is established to switching

facilities as, for example, in a public switched network. (T)

switched virtual circuit (SVC). An X.25 circuit that is dynamically established when needed. The X.25 equivalent of a switched line.

synchronous. (1) Pertaining to two or more processes that depend upon the occurrence of specific events such as common timing signals. (T) (2) Occurring with a regular or predictable time relationship.

Synchronous Data Link Control (SDLC). A discipline conforming to subsets of the Advanced Data Communication Control Procedures (ADCCP) of the American National Standards Institute (ANSI) and High-level Data Link Control (HDLC) of the International Organization for Standardization, for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex or half-duplex over switched or nonswitched links. The configuration of the link connection may be point-to-point, multipoint, or loop. (I) Contrast with *binary synchronous communication (BSC)*.

SYNTAX. In the Simple Network Management Protocol (SNMP), a clause in the MIB module that defines the abstract data structure that corresponds to a managed object.

system. In data processing, a collection of people, machines, and methods organized to accomplish a set of specific functions. (I) (A)

system configuration. A process that specifies the devices and programs that form a particular data processing system.

Systems Network Architecture (SNA). The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks. The layered structure of SNA allows the ultimate origins and destinations of information, that is, the end users, to be independent of and unaffected by the specific SNA network services and facilities used for information exchange.

T

TCP. Transmission Control Protocol.

TCP/IP. Transmission Control Protocol/Internet Protocol.

Telnet. In the Internet suite of protocols, a protocol that provides remote terminal connection service. It allows users of one host to log on to a remote host and interact as directly attached terminal users of that host.

TG. Transmission group.

threshold. (1) In IBM bridge programs, a value set for the maximum number of frames that are not forwarded across a bridge due to errors, before a "threshold exceeded" occurrence is counted and indicated to network management programs. (2) An initial value from which a counter is decremented to 0, or a value to which a counter is incremented or decremented from an initial value.

time to live (TTL). A technique used by best-effort delivery protocols to inhibit endlessly looping packets. The packet is discarded if the TTL counter reaches 0.

timeout. (1) An event that occurs at the end of a predetermined period of time that began at the occurrence of another specified event. (I) (2) A time interval allotted for certain operations to occur; for example, response to polling or addressing before system operation is interrupted and must be restarted.

token. (1) In a local area network, the symbol of authority passed successively from one data station to another to indicate the station temporarily in control of the transmission medium. Each data station has an opportunity to acquire and use the token to control the medium. A token is a particular message or bit pattern that signifies permission to transmit. (T) (2) In LANs, a sequence of bits passed from one device to another along the transmission medium. When the token has data appended to it, it becomes a frame.

token ring. (1) According to IEEE 802.5, network technology that controls media access by passing a token (special packet or frame) between media-attached stations. (2) A FDDI or IEEE 802.5 network with a ring topology that passes tokens from one attaching ring station (node) to another. (3) See also *local area network (LAN)*.

token-ring network. (1) A ring network that allows unidirectional data transmission between data stations, by a token passing procedure, such that the transmitted data return to the transmitting station. (T) (2) A network that uses a ring topology, in which tokens are passed in a circuit from node to node. A node that is ready to send can capture the token and insert data for transmission.

topology. In communications, the physical or logical arrangement of nodes in a network, especially the relationships among nodes and the links between them.

TP. Transaction program.

trace. (1) A record of the execution of a computer program. It exhibits the sequences in which the

instructions were executed. (A) (2) For data links, a record of the frames and bytes transmitted or received.

Transmission Control Protocol (TCP). A communications protocol used in Internet and in any network that follows the U.S. Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It assumes that the Internet Protocol is the underlying protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks.

transmission group (TG). (1) A connection between adjacent nodes that is identified by a transmission group number. See also *parallel transmission groups.* (2) In a subarea network, a single link or a group of links between adjacent nodes. When a transmission group consists of a group of links, the links are viewed as a single logical link, and the transmission group is called a *multilink transmission group (MLTG).* A *mixed-media multilink transmission group (MMMLTG)* is one that contains links of different medium types (for example, token-ring, switched SDLC, nonswitched SDLC, and frame-relay links). (3) In an APPN network, a single link between adjacent nodes.

transmission header (TH). Control information, optionally followed by a basic information unit (BIU) or a BIU segment, that is created and used by path control to route message units and to control their flow within the network. See also *path information unit.*

transparent bridging. In LANs, a method for tying individual local area networks together through the medium access control (MAC) level. A transparent bridge stores the tables that contain MAC addresses so that frames seen by the bridge can be forwarded to another LAN if the tables indicate to do so.

trap. In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

TTL. Time to live.

T1. In the United States, a 1.544-Mbps public access line. It is available in twenty-four 64-Kbps channels. The European version (E1) transmits 2.048 Mbps. The Japanese version (J1) transmits 1.544 Mbps.

U

UA. Unnumbered acknowledgment.

UDP. User Datagram Protocol.

universally administered address. In a local area network, the address permanently encoded in an adapter at the time of manufacture. All universally administered addresses are unique. Contrast with *locally administered address.*

User Datagram Protocol (UDP). In the Internet suite of protocols, a protocol that provides unreliable, connectionless datagram service. It enables an application program on one machine or process to send a datagram to an application program on another machine or process. UDP uses the Internet Protocol (IP) to deliver datagrams.

V

V.35. In data communications, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at various data rates.

variable. In the Simple Network Management Protocol (SNMP), a match of an object instance name with an associated value.

version. A separately licensed program that usually has significant new code or new function.

VINES. VIrtual NEtworking System.

virtual circuit. (1) In packet switching, the facilities provided by a network that give the appearance to the user of an actual connection. (T) See also *data circuit.* Contrast with *physical circuit.* (2) A logical connection established between two DTEs.

VIrtual NEtworking System (VINES). The network operating system and network software from Banyan Systems, Inc. In a VINES network, virtual linking allows all devices and services to appear to be directly connected to each other, when they may actually be thousands of miles apart. See also *StreetTalk.*

virtual route (VR). In SNA, either a) a logical connection between two subarea nodes that is physically realized as a particular explicit route or b) a logical connection that is contained wholly within a subarea node for intranode sessions. A virtual route between distinct subarea nodes imposes a transmission priority on the underlying explicit route, provides flow control through virtual route pacing, and provides data integrity through sequence numbering of path

information units (PIUs). See also *explicit route (ER)*, *path*, and *route extension (REX)*.

vital product data (VPD). Information that uniquely defines system, hardware, software, and microcode elements of a processing system.

VPD. Vital product data.

VR. Virtual route.

W

WAN. Wide area network.

wide area network (WAN). (1) A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. (T) (2) A data communications network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. Contrast with *local area network (LAN)* and *metropolitan area network (MAN)*.

wildcard character. Synonym for *pattern-matching character*.

X

X.21. An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for a general-purpose interface between data terminal equipment and data circuit-terminating equipment for synchronous operations on a public data network.

X.25. An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for the interface between data terminal equipment and packet-switched data networks. See also *packet switching*.

Xerox Network Systems (XNS). The suite of internet protocols developed by the Xerox Corporation. Although similar to TCP/IP protocols, XNS uses different packet formats and terminology. See also *Internetwork Packet Exchange (IPX)*.

XID. Exchange identification.

XNS. Xerox Network Systems.

Z

ZIP. Zone Information Protocol.

ZIT. Zone information table.

zone. In AppleTalk networks, a subset of nodes within an internet.

Zone Information Protocol (ZIP). In AppleTalk networks, a protocol that provides zone management service by maintaining a mapping of the zone names and network numbers across the internet on the session layer.

zone information table (ZIT). A listing of network numbers and their associated zone name mappings in the internet. This listing is maintained by each internet router in an AppleTalk internet.

Bibliography

IBM 6611 Network Processor and Multiprotocol Network Program Publications

The IBM 6611 Network Processor and the Multiprotocol Network Program library includes the:

Multiprotocol Network Program Configuration Guide, SC31-6691

Multiprotocol Network Program Operations and Problem Management, SC31-6692

6611 Network Processor Cable Labels, GX27-3910

6611 Network Processor Connectivity Poster, SX75-0096

6611 Network Processor Customer Setup Guide, GA27-3993

6611 Network Processor Introduction and Planning Guide, GK2T-0334

6611 Network Processor Maintenance Information, GA27-3941

6611 Network Processor Network Management Reference, GC30-3567

6611 Network Processor Operations Pocket Guide, GX27-3909

6611 Network Processor Translated Safety Information, GA27-3954

Related IBM Product Publications

The following list of publications contains information concerning IBM products related to the use of the IBM 6611 Network Processor and the Multiprotocol Network Program:

AIX NetView/6000 Administration Reference, SC31-6196

AIX NetView/6000 at a Glance, GC31-6175

AIX SystemView NetView/6000 Concepts, GC31-6179

AIX SystemView NetView/6000 User's Guide, SC31-7024

AIX SystemView NetView/6000 Problem Determination, SC31-7021

AIX SystemView NetView/6000 Installation and Configuration, SC31-7020

Getting Started with LAN Network Manager, SC31-7104

LAN Cabling System Planning and Installation Guide, GA27-3361

LAN Network Manager Reference, SC31-7106

LAN Station Manager User's Guide, SC31-7108

Local Area Network Manager Reference, SC31-7106

NetBIOS Application Development Guide, S68X-2270

IBM Remote Token-Ring Bridge/DOS Version 1.0.1, part number P71G9347 includes publications and diskettes

Systems Network Architecture Concepts and Products, GC30-3072

Systems Network Architecture Formats, GA27-3136

Systems Network Architecture Management Services Reference, SC30-3346

Systems Network Architecture Technical Overview, GC30-3073

Systems Network Architecture Type 2.1 Node Reference, SC30-3422

TCP/IP Tutorial and Technical Overview, GG24-3376

Token-Ring Network Introduction and Planning Guide, GA27-3677

Token-Ring Network Architecture Reference, SC30-3374

Token-Ring Network Bridge Program Version 2.2.4 User's Guide (shipped with the product)

Token-Ring Network Introduction and Planning Guide, GA27-3677

The IBM Network Processor, GG24-3870

Using LAN Network Manager, SC31-7105

Using the IBM Cabling System and Communication Products, GA27-3620

8209 LAN Bridge: Attachment Module Guide for Ethernet and IEEE 802.3 LANs, GA27-3891

6611 Network Processor folder, SX75-0102, which includes these brochures:

- *6611 Network Processors and the IBM Multiprotocol Network Program*, G325-6503
- *6611 SNA/NetBIOS Internetworking*, G325-6504
- *6611 World-Class Multiprotocol Support*, G325-6505
- *6611 Network Management and the AIX Router and Bridge Manager/6000*, G325-6506
- *6611 Configuration Program and System Manager*, G325-6507

Other Publications

The following list is of known publications that contain information about internetworking, network design, and the protocols that the IBM 6611 supports. Other useful publications may already exist or may be published after the date of this book.

Internet Activities Board (IAB)

Internet Official Protocol Standards, Request for Comments 1600, Jon Postel (editor), March 1994

Internet Activities Board, Request for Comments 1160, Vinton G. Gerf, DDN Network Information Center, SRI International, May 1990

Internetworking

FYI on "What Is the Internet?", Request for Comments 1462, Krol, E., Hoffman, E, May 1993

FYI on Introducing the Internet–A Short Bibliography of Introductory Internetworking Readings for the Network Novice, Request for Comments, 1463, Hoffman, E., Jackson, L., May 1993

Internetworking: A Guide to Communications, Mark A. Miller, M&T Books, 1991

Internetworking Computer Systems: Interconnecting Networks and Systems, John McConnell, Prentice Hall, 1988.

Internetworking with TCP/IP Volume I: Principles, Protocols, and Architecture, Second Edition, Douglas E. Comer, Prentice Hall, 1991

Network Design

IBM Multisegment LAN Design Guidelines, GG24-3398

The IBM 6611 Network Processor as an IP Router, GG24-4064

Protocols

ANSI T1.617-1991, *Telecommunications — Digital Subscriber Signaling Service 1—Signaling Specification for Frame Relay Bearer Service*, June 18, 1991

Banyan VINES-The Professional Reference, Jim Krochmal, New Riders Publishing, 1994

CCITT Recommendation I.122 — Framework for Providing Additional Packet-Mode Bearer Services

CCITT Recommendation Q.922 — ISDN Data Link Layer Specification for Frame Mode Bearer Services, April 19, 1991

CCITT Recommendation X.21, Interface between Data Terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE) for Synchronous Operation on Public Data Networks (Geneva, 1984)

CCITT Recommendation X.25, Interface between Data Terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE) for Terminals Operating in the Packet Mode on Public Data Networks (Geneva, 1976; amended Geneva, 1980)

DECnet Digital Network Architecture (Phase IV): General Description, AA-N149A-TC, Digital Equipment Corporation, 1982

DECnet Digital Network Architecture (Phase IV): Ethernet Data Link Functional Specification, AA-Y298A-TK, Digital Equipment Corporation, 1983

DECnet Digital Network Architecture (Phase IV): Routing Layer Functional Specification, AA-X435A-TK, Digital Equipment Corporation, 1983

DECnet Digital Network Architecture (Phase IV): Token Ring Data Link and Node Product Functional Specifications, EK-DNAP4-TR-001, Digital Equipment Corporation, 1992

Inside AppleTalk, Second Edition, Gursharan Sidhu, Richard Andrews, Alan Oppenheimer, Addison-Wesley Publishing Company, Inc., 1990

Internet Transport Protocols, XNSS 028112, Xerox Corporation, 1981

Internetworking with TCP/IP Volume I: Principles, Protocols, and Architecture, Second Edition, Douglas E. Comer, Prentice Hall, 1991

IPX Router Specification, Part Number 107-000029-001, Novell, Inc., October 16, 1992

NetWare Communications Processes, Paul Turner, Novell Corporation, 1990

Novell NetWare Link Services Protocol Specification, Revision 1, Novell part number 100-001708-002, February 1994

VINES Protocol Definition, Order Number 003673, Banyan Systems Incorporated, June 1993

VINES Architecture Definition, Order Number 002645, Banyan Systems Incorporated, April 1993

Network Management

IEEE 802.1D-1990, IEEE Standards for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges, The Institute of Electrical and Electronics Engineers, Inc., May 1990

Interconnections: Bridges and Routers, Perlman, Radia, Addison-Wesley Publishing Company, Inc., 1992

Networking with Banyan VINES, Laubach, Edwin G., McGraw-Hill, Inc., 1991

Specification of Abstract Syntax Notation One (ASN.1), Information technology–Open Systems Interconnection, International Standard ISO/IEC 8824, December 1991

The IBM LAN Bridge, Latif, A., Rowlance, E.J., Adams, R. Holt, IEEE Network, Volume 6 Number 3, May 1992

The Simple Book: An Introduction to Management of TCP/IP-based Internets, Marshall T. Rose, Prentice Hall, 1991

Internet Requests for Comments (RFCs)

Obtaining RFCs

This section describes three methods for obtaining copies of Internet RFCs.

Electronic Copies via FTP:

If you have FTP running on a workstation that is connected to the Internet, you may retrieve RFCs from the Network Information Center by following this procedure:

1. Use FTP to connect to host ds.internic.net.
2. Issue the command **user anonymous** to identify yourself to the host.
3. When prompted for a password, type **guest**.
4. Type the command **cd rfc** to change to the RFC directory.
5. Type the command **get rfc.nnn.txt**, where *nnn* represents the requested RFC number.

Electronic Copies via Electronic Mail:

The Network Information Center provides an automated service called service@ds.internic.net. This service allows you to access RFCs (and other documents) via ordinary electronic mail. This is especially useful for users who do not have access to the Network Information Center via a direct Internet link. Follow this procedure to obtain an RFC via electronic mail:

1. Send a mail message to service@ds.internic.net.
2. In the Subject field, type **rfc.nnn.**, where *nnn* is the RFC number. To obtain a list of all of the RFCs available, substitute the word *index* for *nnn*.

Large files will be broken into smaller separate messages. The information you request will be sent back to you as soon as possible.

Printed Copies:

Printed copies of RFCs are available for a fee from:

SRI International, Room EJ291
333 Ravenswood Avenue
Menlo Park, CA 94025
(415) 859-3695
(415) 859-6387
FAX (415) 859-6028

RFCs Implemented by the IBM 6611 and the IBM Multiprotocol Network Program

This section provides a list of Internet RFCs and drafts that relate to the IBM 6611 and the IBM Multiprotocol Network Program.

RFC	Title
768	*User Datagram Protocol*, Postel, J.B., August 1980
791	*Internet Protocol*, Postel, J.B., September 1981
792	*Internet Control Message Protocol*, Postel, J.B., September 1981
793	*Transmission Control Protocol*, Postel, J.B., September 1981
826	*Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48 Bit Ethernet Address for Transmission on Ethernet Hardware*, D.C. Plummer, November 1982
854	*Telnet Protocol Specification*, Postel, J.B.; Reynolds J.K., May 1983

855 *Telnet Option Specifications*, Postel, J.; Reynolds J., May 1983

862 *Echo Protocol*, Postel, J., May 1983

868 *Time Protocol*, Postel, J.; Harrenstien, K., May 1983

877 *Standard for the Transmission of IP Datagrams over Public Data Networks*, Korb, J.T., September 1983

891 *DCN Local-Network Protocols*, Mills, D.L., December 1983

894 *Standard for the Transmission of IP Datagrams over Ethernet Networks*, Hornig, C., April 1984

904 *Exterior Gateway Protocol Formal Specification*, Mills, D.L., April 1984

919 *Broadcasting Internet Datagrams*, Mogul, J., October 1984

922 *Broadcasting Internet Datagrams in the Presence of Subnets* , Mogul, J., October 1984

950 *Internet Standard Subnetting Procedure*, Mogul, J; Postel, J., August 1985

951 *Bootstrap Protocol*, Croft, W., Gilmore, J., September 1985

959 *File Transfer Protocol*, Postel, J.B.; Reynolds J.K., October 1985

1009 *Requirements for Internet Gateways*, Braden, R.; Postel, J., June 1987

1042 *Standard for the Transmission of IP Datagrams over IEEE 802 Networks*, Postel J.B.; Reynolds J.K., February 1988

1058 *Routing Information Protocol*, Hendrick, C., June 1988

1155 *Structure and Identification of Management Information for TCP/IP-Based Internets*, Rose, M.; McCloghrie, K., May 1990

1156 *Management Information Base for Network Management of TCP/IP-Based Internets*, McCloghrie, K; Rose, M.T., May 1990

1157 *Simple Network Management Protocol (SNMP)*, Case, J.D.; Fedor M.; Schoffstall, M.L.; Davin, C., May 1990

1171 *Point-to-Point Protocol for the Transmission of Multiprotocol Datagrams over Point-to-Point Links*, Perkins, D., July 1990

1212 *Concise MIB Definitions*, Rose, M.T. & McCloghrie, K. (editors), March 1991

1213 *Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II*, McCloghrie, K. & Rose, M.T. (editors), March 1991

1219 *On the Assignment of Subnet Numbers*, Tsuchiya, P, April 1991

1220 *Point-to-Point Protocol Extensions for Bridging*, Baker, F. (editor), April 1991

1229 *Extensions to the Generic-Interface MIB*, McCloghrie, K. (editor), May 1991

1231 *IEEE 802.5 Token-Ring MIB*, McCloghrie, K.; Fox, R.; Decker, E., May 1991

1232 *Definitions of Managed Objects for the DS1 Interface Type*, Baker, F. & Kolb, C. (editors), May 1991

1243 *AppleTalk Management Information Base*, Waldbusser, S. (editor), July 1991

1245 *OSPF Protocol Analysis*, Moy, J. (editor), July 1991

1247 *OSPF Version 2*, Moy, J., July 1991

1253 *OSPF Version 2: Management Information Base*, Baker, F.; Coltun, R., August 1991

1267 *A Border Gateway Protocol 3 (BGP-3)*, Lougheed, K.; Rekhter, Y., October 1991

1268 *Application of the Border Gateway Protocol in the Internet*, Rekhter, Y. & Gross, P. (editors), October 1991

1269 *Definitions of Managed Objects for the Border Gateway Protocol (Version 3)*, Willis, S.; Burruss, J.W., October 1991

1284 *Definitions of Managed Objects for the Ethernet-Like Interface Types*, Cook, J. (editor), December 1991

1289 *DECnet Phase IV MIB Extensions*, Saperia, J., December 1991

1293 *Inverse Address Resolution Protocol*, Brown, C., January 1992

1294 *Multiprotocol Interconnect over Frame Relay*, Bradley, T.; Brown, C.; Malis, A., January 1992

1315 *Management Information Base for Frame Relay DTEs*, Brown, C.; Baker, F.; Carvalho, C., April 1992

1331 *The Point-to-Point Protocol (PPP) for the Transmission of Multiprotocol Datagrams over Point-to-Point Links*, Simpson, W., May 1992

1332 *The PPP Internet Protocol Control Protocol (IPCP)*, McGregor, G., May 1992

1333 *PPP Link Quality Monitoring*, Simpson, W., May 1992

1340 *Assigned Numbers*, Reynolds, J.; Postel, J., July 1992

1354 *IP Forwarding Table MIB*, Baker, F., July 1992

1356 *Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode*, Malis, A.; Robinson, D.; Ullman, R., August 1992

1370 *Applicability Statement for OSPF*, Internet Architecture Board, October 1992

1376 *The PPP DECnet Phase IV Control Protocol (DNCP)*, Senum, S., November 1992

1378 *The PPP AppleTalk Control Protocol (ATCP)*, Parker, B., November 1992

1388 *RIP Version 2-Carrying Additional Information*, Malkin, G., January 1993

1389 *RIP Version 2 MIB Extension*, Malkin, G., January 1993

1397 *Default Route Advertisement in BGP2 and BGP3 Versions of the Border Gateway Protocol*, Haskin, D., January 1993

1403 *BGP OSPF Interaction*, Varadhan, K., January 1993

1434 *Data Link Switching: Switch-to-Switch Protocol*, Dixon. R.; Kushi, D., March 1993

1490 *Multiprotocol Interconnect over Frame Relay*, Bradley, T; Brown, C.; Malis, A., July 1993

1493 *Definitions of Managed Objects for Bridges*, Decker, E.; Langille, P.; Rijsinghani, A.; McCloghrie, K., July 1993

1525 *Definitions of Managed Objects for Source Route Bridges*, Decker, E.; McCloghrie, K.; Langille, P.; Rijsinghani, A., September 1993

1548 *The Point-to-Point Protocol (PPP)*, Simpson, W., December 1993

1549 *PPP in HDLC Framing*, Simpson, W. (editor), December 1993

1551 *Novell IPX over Various WAN Media (IPXWAN)*, Allen, M., December 1993

1570 *PPP LCP Extensions*, Simpson, W. (editor), January 1994

1600 *Internet Official Protocol Standards*, Postel, J. (editor), March 1994

1638 *PPP Bridging Control Protocol (BCP)*, Baker, F., Bowen, R., June 1994

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

X

Communicating Your Comments to IBM

Multiprotocol Network Program
Operations and Problem Management
Version 1 Release 3

Publication No. SC31-6692-01

If you especially like or dislike anything about this book, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

If you are mailing a readers' comment form (RCF) from a country other than the United States, you can give the RCF to the local IBM branch office or IBM representative for postage-paid mailing.

- If you prefer to send comments by mail, use the RCF at the back of this book.
- If you prefer to send comments by FAX, use this number:

  United States and Canada: **1-800-227-5088**
- If you prefer to send comments electronically, use this network ID:
  - IBM Mail Exchange: **USIB2HPD at IBMMAIL**
  - IBMLink: **CIBMORCF at RALVM13**
  - Internet: **USIB2HPD@VNET.IBM.COM**

Make sure to include the following in your note:

- Title and publication number of this book
- Page number or topic to which your comment applies.

Help us help you!

Multiprotocol Network Program
Operations and Problem Management
Version 1 Release 3

Publication No. SC31-6692-01

We hope you find this publication useful, readable and technically accurate, but only you can tell us! Your comments and suggestions will help us improve our technical publications. Please take a few minutes to let us know what you think by completing this form.

Overall, how satisfied are you with the information in this book?	Satisfied	Dissatisfied
	☐	☐

How satisfied are you that the information in this book is:	Satisfied	Dissatisfied
Accurate	☐	☐
Complete	☐	☐
Easy to find	☐	☐
Easy to understand	☐	☐
Well organized	☐	☐
Applicable to your task	☐	☐

Specific Comments or Problems:

Please tell us how we can improve this book:

Thank you for your response. When you send information to IBM, you grant IBM the right to use or distribute the information without incurring any obligation to you. You of course retain the right to use the information in any way you choose.

Name

Address

Company or Organization

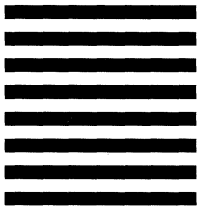
Phone No.

Help us help you!
SC31-6692-01

Cut or
Along l

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Information Development
Department E15
International Business Machines Corporation
PO BOX 12195
RESEARCH TRIANGLE PARK NC 27709-9990

Fold and Tape **Please do not staple** Fold and Tape

SC31-6692-01

Cut or Fc
Along Lin

Help us help you!

Multiprotocol Network Program
Operations and Problem Management
Version 1 Release 3

Publication No. SC31-6692-01

We hope you find this publication useful, readable and technically accurate, but only you can tell us! Your comments and suggestions will help us improve our technical publications. Please take a few minutes to let us know what you think by completing this form.

Overall, how satisfied are you with the information in this book?	Satisfied	Dissatisfied
	☐	☐

How satisfied are you that the information in this book is:	Satisfied	Dissatisfied
Accurate	☐	☐
Complete	☐	☐
Easy to find	☐	☐
Easy to understand	☐	☐
Well organized	☐	☐
Applicable to your task	☐	☐

Specific Comments or Problems:

Please tell us how we can improve this book:

Thank you for your response. When you send information to IBM, you grant IBM the right to use or distribute the information without incurring any obligation to you. You of course retain the right to use the information in any way you choose.

Name

Address

Company or Organization

Phone No.

Help us help you!
SC31-6692-01

Cut or F
Along L

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Information Development
Department E15
International Business Machines Corporation
PO BOX 12195
RESEARCH TRIANGLE PARK NC 27709-9990

Fold and Tape **Please do not staple** Fold and Tape

SC31-6692-01

Cut or F
Along Li

Help us help you!

Multiprotocol Network Program
Operations and Problem Management
Version 1 Release 3

Publication No. SC31-6692-01

We hope you find this publication useful, readable and technically accurate, but only you can tell us! Your comments and suggestions will help us improve our technical publications. Please take a few minutes to let us know what you think by completing this form.

Overall, how satisfied are you with the information in this book?	Satisfied	Dissatisfied
	☐	☐

How satisfied are you that the information in this book is:	Satisfied	Dissatisfied
Accurate	☐	☐
Complete	☐	☐
Easy to find	☐	☐
Easy to understand	☐	☐
Well organized	☐	☐
Applicable to your task	☐	☐

Specific Comments or Problems:

Please tell us how we can improve this book:

Thank you for your response. When you send information to IBM, you grant IBM the right to use or distribute the information without incurring any obligation to you. You of course retain the right to use the information in any way you choose.

Name

Address

Company or Organization

Phone No.

Help us help you!
SC31-6692-01

Cut or F
Along Li

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Information Development
Department E15
International Business Machines Corporation
PO BOX 12195
RESEARCH TRIANGLE PARK NC 27709-9990

Fold and Tape | **Please do not staple** | Fold and Tape

SC31-6692-01

Cut or Fol
Along Lin

Part Number: 92G8804

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber

The IBM 6611 Network Processor and Multiprotocol Network Program Library

IBM Multiprotocol Network Program Configuration Guide, SC31-6691
IBM Multiprotocol Network Program Operations and Problem Management, SC31-6692
IBM 6611 Network Processor Cable Labels, GX27-3910
IBM 6611 Network Processor Connectivity poster, SX75-0096
IBM 6611 Network Processor Customer Setup Guide, GA27-3993
IBM 6611 Network Processor Introduction and Planning Guide, GK2T-0334
IBM 6611 Network Processor Maintenance Information, GA27-3941
IBM 6611 Network Processor Network Management Reference, GC30-3567
IBM 6611 Network Processor Operations Pocket Guide, GX27-3909
IBM 6611 Network Processor Translated Safety Information, GA27-3954

SC31-6692-01