Getting Started with ADSM AIX Clients

Document Number GG24-4243-00

November 1994

International Technical Support Organization
San Jose Center

Take Note!

Before using this information and the product it supports, be sure to read the general information under “Special Notices” on page xi.

First Edition (November 1994)

This edition applies to Release 2 of ADSTAR Distributed Storage Manager (5648-020) and all subsequent releases and modifications unless otherwise indicated.

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

An ITSO Technical Bulletin Evaluation Form for reader's feedback appears facing Chapter 1. If the form has been removed, comments may be addressed to:

IBM Corporation, International Technical Support Organization
Dept. 471 Building 70B
5600 Cottle Road
San Jose, California 95193-0001

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

© **Copyright International Business Machines Corporation 1994. All rights reserved.**
Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Abstract

This document describes the ADSTAR Distributed Storage Manager (ADSM) client for AIX. It provides information for the installation, customization, and expanded use of the ADSM client. The types of data supported by ADSM backup and archive functions, the connectivity options of client/server communications, requirements for running the ADSM client in the AIX environment, and samples of recovery are included.

This document is written for ADSM administrators, AIX server administrators, storage administrators, LAN and networking specialists, and technical personnel interested in the ADSM client.

The document is an introductory discussion of using ADSM in the AIX environment. Thus, it is not intended for AIX specialists interested in advanced ADSM implementation considerations or integration of ADSM with other AIX products. Some knowledge of ADSM and AIX is assumed.

ST (119 pages)

© Copyright IBM Corp. 1994

Contents

Abstract . . . iii

Special Notices . . . xi

Preface . . . xiii
How This Document Is Organized . . . xiii

Related Publications . . . xv
International Technical Support Organization Publications . . . xvi

Acknowledgments . . . xvii

Chapter 1. Introduction to ADSM . . . 1
1.1 Structure . . . 1
1.1.1 Client/Server . . . 1
1.1.2 Storage Management . . . 2
1.1.3 Enterprise Support . . . 3
1.1.4 Communications Protocols . . . 5
1.2 Components . . . 6
1.2.1 Server . . . 6
1.2.2 Backup/Archive Client . . . 7
1.2.3 User Interfaces . . . 7
1.2.4 Storage Administration . . . 7
1.2.5 Administrative Client . . . 8
1.2.6 Application Client . . . 8
1.2.7 Security . . . 8
1.3 Storage Management Services . . . 9
1.3.1 Backup Processing . . . 9
1.3.2 Restore Processing . . . 10
1.3.3 Archive Processing . . . 11
1.3.4 Retrieve Processing . . . 11
1.3.5 General File Support . . . 11
1.3.6 Policy Management . . . 12
1.3.7 Function Execution . . . 17
1.3.8 Client System and User Options Files . . . 18

Chapter 2. Introduction to AIX . . . 21
2.1 System Structure . . . 21
2.2 Shells . . . 23
2.3 Processes . . . 23
2.4 Logical Volume Storage . . . 25
2.4.1 Logical Volume Manager . . . 26
2.4.2 Physical Volumes, Groups, and Partitions . . . 27
2.4.3 Logical Volumes and Partitions . . . 27
2.5 File Systems . . . 27
2.5.1 File System Types . . . 28
2.5.2 Files and Directories . . . 29
2.6 AIX Extensions to UNIX . . . 29
2.6.1 Logical Volume Manager . . . 30
2.6.2 System Resource Controller . . . 30
2.6.3 Object Data Manager . . . 30

© Copyright IBM Corp. 1994

2.6.4 Software Vital Product Data . . . 30
2.7 File Security . . . 30
2.7.1 Ownership . . . 31
2.7.2 Access . . . 31
2.8 Communication Services . . . 32
2.8.1 Hardware . . . 32
2.8.2 Communication Protocols . . . 33
2.9 AIX User Interfaces . . . 34
2.9.1 System Management Interface Tool . . . 34
2.9.2 AIXwindows . . . 36

Chapter 3. Implementing the ADSM AIX Client . . . 37
3.1 Installing the ADSM Client . . . 37
3.1.1 Hardware Requirements . . . 37
3.1.2 Software Requirements . . . 37
3.1.3 Installation . . . 38
3.2 Tailoring the ADSM Client . . . 40
3.2.1 Updating the Client System Options File . . . 40
3.2.2 Updating the Client User Options File . . . 44
3.3 TCP/IP Connectivity . . . 46
3.3.1 System Requirements . . . 46
3.3.2 Configuration . . . 46
3.3.3 Problem Determination . . . 49
3.3.4 Performance Considerations . . . 50
3.4 APPC (LU6.2) Connectivity . . . 52
3.4.1 System Requirements . . . 54
3.4.2 Configuration . . . 55
3.4.3 Problem Determination . . . 79
3.4.4 Performance Considerations . . . 80

Chapter 4. Using the ADSM AIX Client . . . 83
4.1 Running the ADSM Client . . . 83
4.1.1 Authorization and Security . . . 83
4.1.2 Starting the ADSM Client . . . 83
4.2 Using ADSM Functions . . . 84
4.2.1 Incremental Backup . . . 84
4.2.2 Management Classes . . . 85
4.2.3 Creating an Include/Exclude File . . . 86
4.2.4 Selective Backup . . . 88
4.2.5 Restore . . . 89
4.2.6 Archive . . . 91
4.2.7 Retrieve . . . 93
4.2.8 Sharing Access to Files . . . 93
4.3 Automatic Scheduling . . . 94
4.3.1 ADSM Server Implementation . . . 94
4.3.2 ADSM Client Implementation . . . 95

Chapter 5. Exploiting the ADSM AIX Client . . . 97
5.1 ADSM Client with Multiple ADSM Servers . . . 97
5.1.1 Setting Up Options Files for Multiple ADSM Servers . . . 98
5.1.2 Automating Use of Multiple ADSM Servers . . . 99
5.1.3 Setting Up Multiple Schedules . . . 100
5.2 Recovery of the AIX System . . . 101
5.3 Recovery of the ADSM Client . . . 101
5.3.1 Using a Backup Image of the ADSM Client . . . 102

5.3.2 Using Multiple ADSM Clients and File Systems and Physical Disks 103
5.3.3 Using Other ADSM AIX Clients 104
5.3.4 Using Backup to Diskette or Tape 105
5.4 Recovery of Applications and User Data 106
5.4.1 Recovering a File 107
5.4.2 Recovering a Directory 107
5.4.3 Recovering a File System 107
5.4.4 Recovering a Physical Disk 108
5.5 Performance Considerations 108
5.5.1 General Environment 108
5.5.2 Compression 109
5.5.3 Colocation 109
5.5.4 Incremental Backup 109
5.5.5 Migration 109
5.5.6 Tuning Considerations 110

Appendix A. Sample ADSM Client Options Files 111
A.1 Client Options File for TCP/IP 111
A.2 Client Options File for APPC 111
A.3 Client Options File for Authorization 111
A.4 Client Options File for Backup and Archive 112
A.5 Client Options File for Scheduling 112
A.6 Include File Statement 113

Appendix B. Sample ADSM MVS Server APPC Definitions 115
B.1 VTAM Start List 115
B.2 VTAM Application Major Node 115
B.3 VTAM Logmode Table 116
B.4 VTAM Workstation Definitions 116
B.4.1 VTAM 3745 Switched Major Node Definition 116
B.4.2 VTAM Cross Domain Definition 117
B.4.3 VTAM 3174 Local Node Definitions 117

Index 119

Figures

1. AIX As an ADSM Client . . . 2
2. ADSM MVS and VM Servers . . . 4
3. ADSM AIX for RISC System/6000 Server . . . 4
4. ADSM OS/2 Server . . . 5
5. Administrative Client GUI . . . 8
6. ADSM Policy Management . . . 13
7. Policy Domains . . . 14
8. Policy Sets . . . 15
9. Copy Groups . . . 16
10. UNIX System Structure . . . 22
11. Listing of Running Processes . . . 25
12. Logical Volume Storage . . . 26
13. AIX Version 3 File Structure . . . 28
14. Listing of File Permissions . . . 31
15. SMIT GUI . . . 35
16. SMIT Text Interface . . . 35
17. Installing the ADSM AIX Client: Install Software at Latest Available Level . . . 39
18. Installing the ADSM AIX Client: Software to Install . . . 39
19. TCP/IP Configuration: Available Network Interfaces . . . 47
20. TCP/IP Configuration: Minimum Configuration & Startup . . . 48
21. PING Example . . . 50
22. TCP/IP Sliding Window . . . 51
23. APPC Configuration Parameters . . . 53
24. ADSM APPC Options for ADSM AIX Client and MVS Server . . . 55
25. APPC Configuration: SNA Server/6000 . . . 57
26. APPC Configuration: Configure SNA Profiles . . . 57
27. APPC Configuration: Initial Node Setup . . . 58
28. APPC Configuration: Initial Node Setup . . . 58
29. APPC Configuration: Advanced Configuration . . . 60
30. APPC Configuration: Links . . . 60
31. APPC Configuration: Token Ring Physical Units . . . 61
32. APPC Configuration: Token Ring SNA DLC . . . 61
33. APPC Configuration: Add Token Ring SNA DLC Profile . . . 62
34. APPC Configuration: Token Ring Physical Units . . . 64
35. APPC Configuration: Token Ring Link Station . . . 64
36. APPC Configuration: Add Token Ring Link Station Profile . . . 65
37. APPC Configuration: Sessions . . . 67
38. LU 6.2 . . . 68
39. LU 6.2 Partner LU . . . 69
40. Add LU 6.2 Partner LU Profile . . . 69
41. Partner LU 6.2 Location Profile . . . 70
42. Add Partner LU 6.2 Location Profile . . . 71
43. APPC Configuration: LU 6.2 . . . 72
44. APPC Configuration: LU 6.2 Mode . . . 72
45. APPC Configuration: Add LU 6.2 Mode Profile . . . 73
46. APPC Configuration: LU 6.2 . . . 74
47. APPC Configuration: LU 6.2 Side Information . . . 74
48. APPC Configuration: Add LU 6.2 Side Information Profile . . . 75
49. APPC Configuration: Advanced Configuration . . . 76
50. APPC Configuration: Verify Configuration Profiles . . . 77

© Copyright IBM Corp. 1994

51. Export SNA Profiles: Advanced Configuration 78
52. Export SNA Profiles: Export Configuration Profiles 78
53. Start and Check SNA/6000 Services 79
54. Aping Command 80
55. ADSM Incremental Backup 85
56. ADSM Selective Backup by File Specification 88
57. ADSM Selective Backup by Directory Tree 89
58. ADSM Restore by File Specification 90
59. ADSM Restore by Directory Tree 90
60. ADSM Restore by Subdirectory Path 91
61. ADSM Archive by File Specification 92
62. ADSM Archive by Directory Tree 92
63. ADSM Retrieve by File Specification 93
64. Set Authorization 94
65. ADSM Client with Multiple ADSM Servers 97
66. ADSM Client Executable Files 102
67. Two Copies of the ADSM Client on One AIX System 103
68. Two Disks on One AIX System 104
69. One ADSM Client Backs Up Another ADSM Client 105
70. Diskette or Tape Backups for an AIX Client 106

Special Notices

This document is written for ADSM administrators, AIX server administrators, storage administrators, LAN and networking specialists, and technical personnel interested in the ADSM client.

The document is an introductory discussion of using ADSM in the AIX environment. Thus, it is not intended for AIX specialists interested in advanced ADSM implementation considerations or integration of ADSM with other AIX products.

The information in this publication is not intended as the specification of any programming interfaces that are provided by ADSTAR Distributed Storage Management (5648-020). See the PUBLICATIONS section of the IBM Programming Announcement for ADSTAR Distributed Storage Management for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these 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 IBM′s product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM′s intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter 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 the IBM Director of Licensing, IBM Corporation, 208 Harbor Drive, Stamford, CT 06904 USA.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM (VENDOR) products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer′s ability to evaluate and integrate them into the customer′s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

© Copyright IBM Corp. 1994

The following terms, which are denoted by an asterisk (*) in this publication, are trademarks of the International Business Machines Corporation in the United States and/or other countries:

ADSTAR	AIX
AIXwindows	AS/400
DB2/6000	IBM
OS/2	RACF
RISC System/6000	VSE/ESA
VTAM	

The following terms, which are denoted by a double asterisk (**) in this publication, are trademarks of other companies:

DEC	Digital Equipment Corporation
HP-UX	Hewlett-Packard Company
INFORMIX On-Line	Informix, Inc.
Internet	Internet, Inc.
Macintosh	Apple Computer, Inc.
NetWare	Novell, Inc.
Oracle	Oracle, Inc.
SCO	The Santa Cruz Operation, Inc.
Solaris	Sun Microsystems, Inc.
SPARC	SPARC International, Inc.
Sun	Sun Microsystems, Inc.
Sybase	Sybase, Inc.
ULTRIX	Digital Equipment Corporation
UNIX	X/Open Company Limited
Windows	Microsoft Corporation

Preface

This document describes the ADSTAR Distributed Storage Manager (ADSM) client for AIX. It provides information for the installation, customization, and expanded use of the ADSM client. The types of data supported by ADSM backup and archive functions, the connectivity options of client/server communications, requirements for running the ADSM client in the AIX environment, and samples of recovery are included.

This document is written for ADSM administrators, AIX server administrators, storage administrators, LAN and networking specialists, and technical personnel interested in the ADSM client.

The document is an introductory discussion of using ADSM in the AIX environment. Thus, it is not intended for AIX specialists interested in advanced ADSM implementation considerations or integration of ADSM with other AIX products. Some knowledge of ADSM and AIX is assumed.

How This Document Is Organized

The document is organized as follows:

- Chapter 1, “Introduction to ADSM” provides an overview of ADSM.
- Chapter 2, “Introduction to AIX” provides an overview of the AIX operating enviornment.
- Chapter 3, “Implementing the ADSM AIX Client” provides information on planning for, connecting to, and implementing the ADSM backup and archive client.
- Chapter 4, “Using the ADSM AIX Client” explains how to use the ADSM backup and archive client.
- Chapter 5, “Exploiting the ADSM AIX Client” describes how to take full advantage of the ADSM client, including how to use ADSM in various backup and recovery scenarios.
- Appendix A, “Sample ADSM Client Options Files” contains sample parameters of the various DSM.SYS files.
- Appendix B, “Sample ADSM MVS Server APPC Definitions” contains sample parameters for APPC connection between the ADSM AIX client and an ADSM MVS server.

© Copyright IBM Corp. 1994

Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this document.

- *ADSTAR Distributed Storage Manager: User's Guide and Reference for UNIX*, SH35-0120
- *ADSTAR Distributed Storage Manager: General Information*, GH35-0114
- *ADSTAR Distributed Storage Manager: Administrator's Guide*, SH35-0117
- *ADSTAR Distributed Storage Manager/2: Administrator's Guide*, SH26-4003
- *ADSTAR Distributed Storage Manager/6000: Administrator's Guide*, SH26-4005
- *ADSTAR Distributed Storage Manager: Administrator's Reference*, SH35-0130
- *ADSTAR Distributed Storage Manager/2: Administrator's Reference*, SH26-4004
- *ADSTAR Distributed Storage Manager/6000: Administrator's Reference*, SH26-4006
- *ADSTAR Distributed Storage Manager/2: Installing the Server and Administrative Client*, SH26-4014
- *ADSTAR Distributed Storage Manager/6000: Installing the Server and Administrative Client*, SH26-4013
- *ADSTAR Distributed Storage Manager: Administration Messages*, SH35-0129
- *ADSTAR Distributed Storage Manager: Performance Tuning Guide Release 2*, SH26-4034
- *ADSTAR Distributed Storage Manager Presentation Guide*, GG24-4146
- *ADSTAR Distributed Storage Manager Storage Management Services: Implementation Examples*, GG24-4034
- *ADSTAR Distributed Storage Manager Advanced Implementation Experiences*, GG24-4221
- *Getting Started with ADSM/2*, GG24-4321
- *Getting Started with ADSM/6000*, GG24-4421
- *Using ADSM to Back Up Databases*, GG24-4335
- *IBM RISC System/6000 System Overview and Planning*, GC23-2406
- *AIX Version 3.2 Management Guide: Communications and Networks*, GC23-2487
- *Systems Management Guide for AIX Version 3.2*, SC23-2457
- *AIX Version 3.2 for RISC System/6000 Installation Guide*, SC23-2341
- *AIX SNA Server/6000: User's Guide*, SC31-7002
- *AIX SNA Server/6000: Configuration Reference*, SC31-7014
- *AIX SNA Server/6000: Command Reference*, SC31-7100
- *AIX SNA Server/6000: Diagnosis Guide and Messages*, SC31-7101
- *AIX Operating System TCP/IP User's Guide*, SC23-2309

© Copyright IBM Corp. 1994

- *A Guided Tour of SNA Server/6000 Version 2.1*, GG24-4189

International Technical Support Organization Publications

A complete list of International Technical Support Organization publications, with a brief description of each, may be found in:

International Technical Support Organization Bibliography of Redbooks, GG24-3070.

Those books that may be of particular interest to someone installing ADSM include:

- *ADSTAR Distributed Storage Manager Presentation Guide*, GG24-4146
- *ADSTAR Distributed Storage Manager Storage Management Services: Implementation Examples*, GG24-4034
- *ADSTAR Distributed Storage Manager Advanced Implementation Experiences*, GG24-4221
- *Getting Started with ADSM/2*, GG24-4321
- *Getting Started with ADSM/6000*, GG24-4421
- *Getting Started with ADSM NetWare Clients*, GC24-4242
- *Using ADSM to Back Up Databases*, GG24-4335

Acknowledgments

This publication is the result of residency projects conducted at the International Technical Support Organization, San Jose Center.

The project was designed and managed by:

Sally J. Montera, Storage Products Assignee, ITSO - San Jose Center.

This book was written by:

Mark Blunden, IBM Australia
Walter Majonica, IBM Germany
Carolina von Hinrichs, IBM Germany
Calvin Wu, IBM Taiwan.

Thanks to the following people for the invaluable advice and guidance provided in the production of this document:

Deeporn Beardsley, IBM Storage Systems Division
Cybelle Beaulieu, IBM Storage Systems Division
Doug Case, IBM Storage Systems Division
Maggie Cutler, Technical Editor
Guido De Simoni, ITSO San Jose
Dale Freeman, ITSO San Jose
M.J. Lopatin, IBM Storage Systems Division.

International Technical Support Organization, San Jose Center.

November 1994

© Copyright IBM Corp. 1994

Chapter 1. Introduction to ADSM

ADSTAR* Distributed Storage Manager (ADSM) is an IBM* product that provides backup, recovery, and archive services for user and system data on a wide variety of computing platforms.

This chapter introduces ADSM to AIX* users and administrators and telecommunications and local area network (LAN) support specialists involved in the implementation of ADSM in an AIX environment. If you are already familiar with ADSM′s concepts and facilities, you may want to go directly to Chapter 2.

The focus of the entire book is on the ADSM AIX client. It is assumed that an ADSM server that supports AIX is available and that an ADSM AIX supported communications protocol product is installed on the ADSM server and client.

1.1 Structure

ADSM provides storage management services for data in a client/server environment. It is structured to support many client and server platforms and communications protocols. The details of this support are described below.

1.1.1 Client/Server

ADSM is a client/server product. Part of ADSM runs as the client, typically on a programmable workstation (PWS), and part of ADSM runs as the server, usually in a larger machine. A user of ADSM has data on a client machine that uses the storage management services that ADSM provides on a server machine.

In an AIX system the term *server* is also used. The AIX server provides data storage, printer, and application serving support to the workstation. Thus, in an ADSM context, an AIX server can also be an ADSM client as is shown in Figure 1 on page 2.

In Figure 1 on page 2, the machines at the top are ADSM servers running OS/2*, MVS, and AIX. The machine in the middle is an AIX server. This system is also an ADSM AIX client called **YELLOW**. The machines at the bottom are possible workstations on the AIX server. Although not shown, an ADSM AIX client could be installed on the AIX workstation at the bottom right hand side of the figure. Thus, the ADSM AIX client can be installed on and used from either an AIX server or an AIX stand-alone system.

© Copyright IBM Corp. 1994

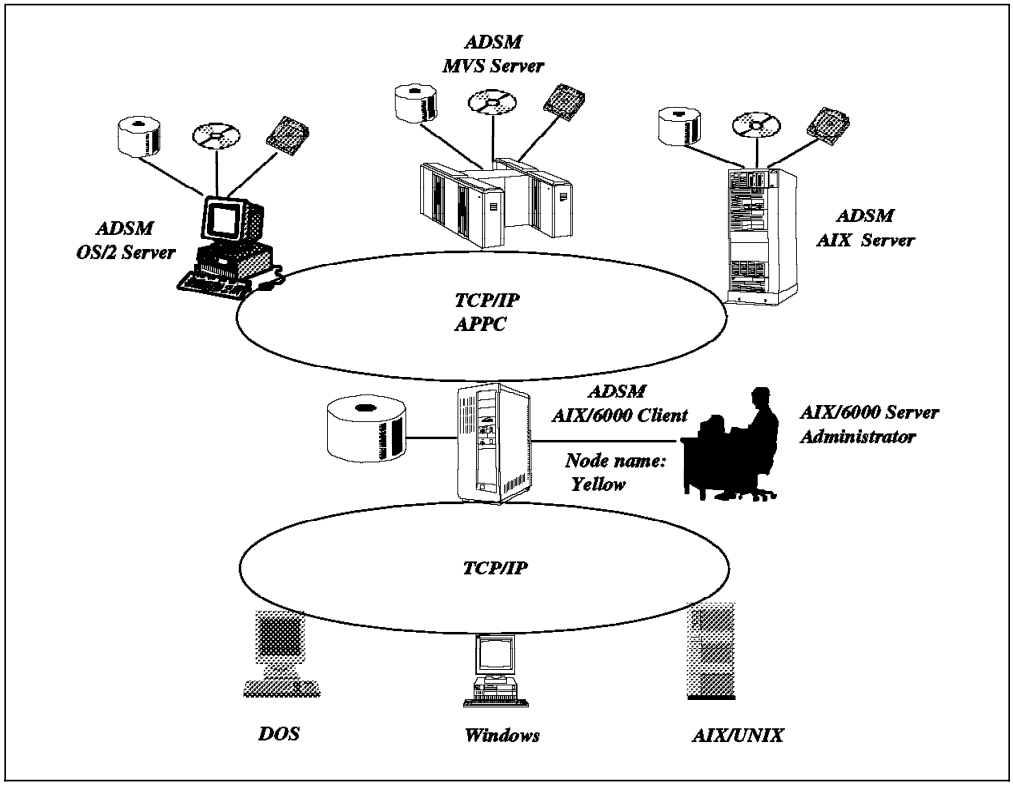


Figure 1. AIX As an ADSM Client

The term *node* is also used within ADSM to identify an ADSM client. A *node name* is the name given to a particular ADSM client or node. It is used like a user ID when the system connects to the ADSM server.

1.1.2 Storage Management

The major storage management functions that ADSM provides are:

- Backup and restore
- Archive and retrieve.

Backup in ADSM means creating a version of a file to be used for recovery. This backup version is stored separately, on the ADSM server, from the master copy of the data. Potentially, you can make several backup versions of the data, each version at a different point in time. These versions are closely tied together and to the original file as a group of backups.

If the master file is invalid or lost, *restore* is the process of using a backup version of the data to re-create the master copy. The most current version of the data would typically be used, but you can restore from any of the backup versions that exist.

The number of backup versions for a file is usually controlled. Old backup versions may be automatically deleted as new versions are created. You can also delete them after a certain period of time.

Archive in ADSM means creating a copy of a file as a separate file. Usually you would use this function to create an additional copy of the data to be saved for

historical reasons. This type of data is called vital records, that is, data that must be kept by law or for other business reasons.

As the archive copy of data is created on the server, you can delete the original copy. Thus, you can use archive to make additional space available on the ADSM client. Archive should not be thought of as a complete space management function because automatic recall is not available.

You can access archived data by *retrieve* to return it to the ADSM client if the data is needed at some future time. To help determine which archived data is required, you can add a description to the data at the time the file is archived. Later, when you want the data again, you can use the description for a search to determine which file to retrieve.

Thus, the difference between backup and archive is that backup creates and controls multiple backup versions that are directly attached to the original file, whereas archive creates an additional file that is usually kept for vital records.

ADSM provides functions that automate backup and archive based on predefined policies. You can build these policies to tailor services for ADSM users and allow the inclusion or exclusion of files from backup processing.

Data recovery includes recovery of:

- Incorrectly modified data
- Prematurely deleted data
- Data lost because of disk, media, or other hardware failures
- Data lost because of site damage or disaster.

The backup and restore facilities of ADSM provide support for all such recoveries. Be aware that other recovery tools and processes may be required in certain situations. For example, before ADSM can recover your data, it and your client's operating system must be up and running on your machine. ADSM cannot be used to recover itself, so other tools must be used.

ADSM provides additional function to support the recovery associated with site damage or disaster. You may want to remove selected data, using *export/import* services, from the ADSM server's site and store it at another location so it will not be damaged during a disaster. This function is only available for data on the ADSM server.

An additional component of ADSM is the storage administrator. The storage administrator is one or more persons who determine how data should be managed within ADSM through tailored policies for backup and restore of data between the ADSM client and ADSM server.

1.1.3 Enterprise Support

One of the key advantages of ADSM is that it can manage storage in your entire enterprise. ADSM supports a wide variety of client/server platforms as shown in Figure 2 on page 4, Figure 3 on page 4, and Figure 4 on page 5.

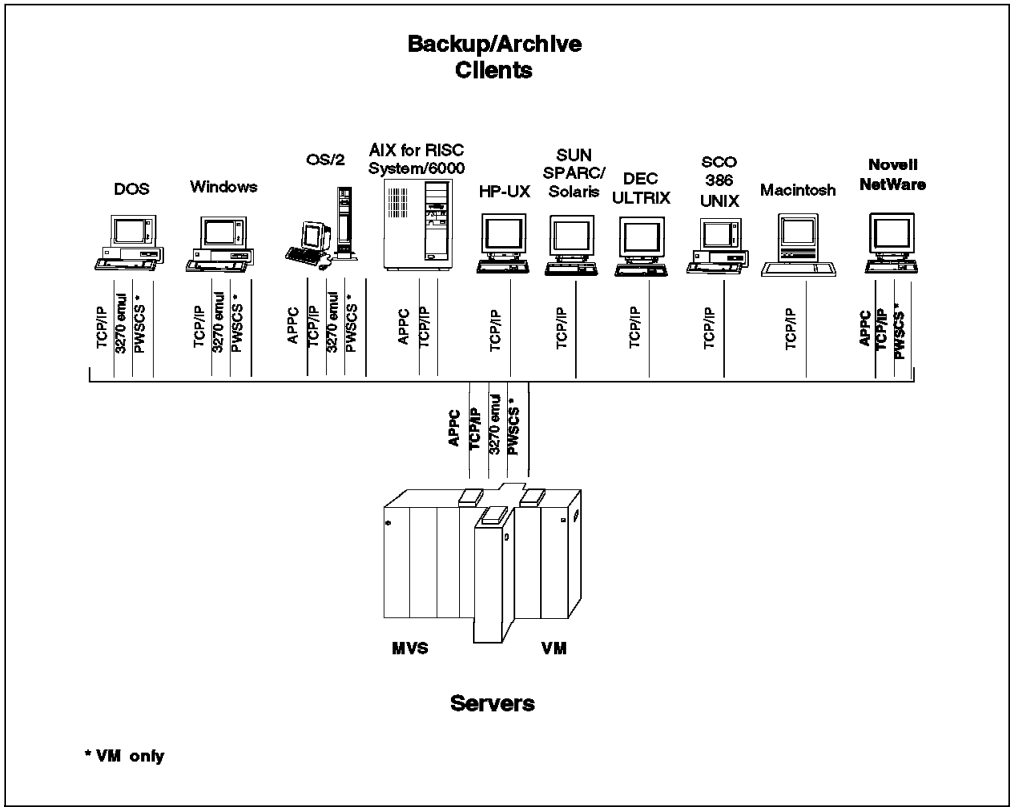


Figure 2. ADSM MVS and VM Servers

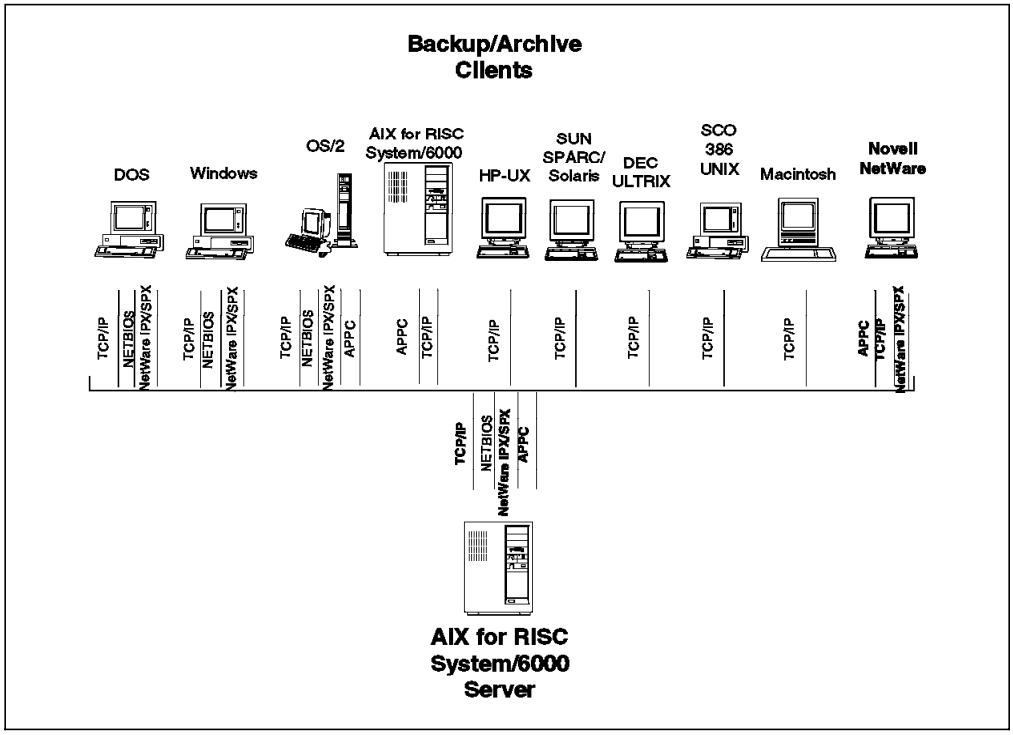


Figure 3. ADSM AIX for RISC System/6000 Server

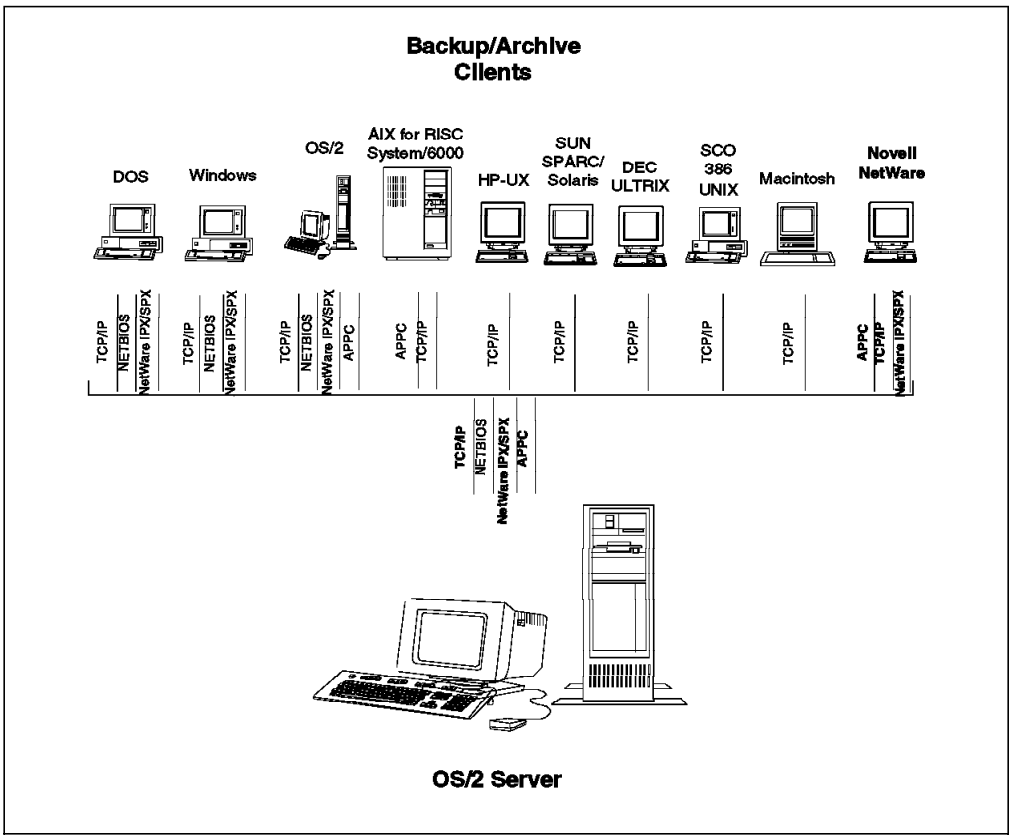


Figure 4. ADSM OS/2 Server

AIX is currently supported as an ADSM client to four ADSM servers using two communications protocols. The AIX environments for ADSM include:

- ADSM MVS server support using TCP/IP and APPC
- ADSM VM server support using TCP/IP and APPC
- ADSM/6000 server support using TCP/IP and APPC
- ADSM/2 server support using TCP/IP and APPC.

With each future release of ADSM, additional servers and clients will be added, so that you can have a single storage management strategy for all of your data.

Note: Since this document was initially written, two additional ADSM servers for AS/400* and VSE/ESA* have become available.

1.1.4 Communications Protocols

As noted in the above discussion, you can use a wide variety of communications protocols to connect the ADSM client with an ADSM server. APPC and TCP/IP are available with AIX. The protocol you select depends on the type of ADSM server that is being used.

TCP/IP is the communications protocol commonly used in most AIX and UNIX** environments. It is an open system, standardized capability for sending information between common or dissimilar systems in a heterogeneous environment. All ADSM servers support ADSM AIX clients using TCP/IP.

APPC is part of IBM's Systems Network Architecture (SNA). It allows two partner programs to communicate with each other as peers. APPC is available between all ADSM servers and ADSM AIX clients.

Although ADSM is a storage management product, the communications protocol component is one of the most important areas for successful implementation of ADSM. It is mandatory to coordinate the communications protocol parameters for the ADSM client and the ADSM server as well as have them fit with other uses, if any, of the communications protocol.

1.2 Components

In this section we introduce specific components of ADSM. Not all components are presented because this discussion is meant to be an introduction to the implementation of the ADSM AIX client. In particular, detailed descriptions of the components of an ADSM server are omitted. These descriptions can be found in the ADSM administrator's guide for the particular server platform of interest and are listed in the Related Publications section of this book.

1.2.1 Server

Currently ADSM has servers for MVS, VM, OS/2, and AIX systems. Customer requirements indicate that additional servers will be added over time.

Note: Since this document was initially written, two additional ADSM servers for AS/400* and VSE/ESA* have become available.

Each server is implemented in a client-independent manner; that is, the server provides a standard set of functions independent of the type of ADSM client that is supported. The ADSM server uses different device types and communications protocols appropriate to its base platform. For example, the ADSM MVS server uses 3420, 3480, or 3490 tape drives, whereas the ADSM OS/2 server uses a variety of SCSI-attached tape products including 8200, 8500, and 8505.

The main role of the ADSM server is to store the backup or archive data from the ADSM clients it supports. It also has a database of information to keep track of the backup and archive data that it manages.

The ADSM server uses a variety of device types to store the backup and archive data received from its ADSM clients. The device types can be arranged in an ADSM-managed storage hierarchy for a cost-efficient way of providing the best support for ADSM users. For example, you can have three storage pools, one made up of tape devices, one made up of DASD devices, and one made up of optical storage devices, with automated movement of the backup and archive data from one storage pool to another. This arrangement allows less used data to reside on the less expensive storage medium.

ADSM servers are stand-alone servers. An enterprise may have many ADSM servers, on either different platforms or the same platform, but each ADSM server is independent of all other ADSM servers. There is no hierarchical or distributed ADSM server support at this time.

1.2.2 Backup/Archive Client

ADSM has several client programs. These programs typically run at the user's workstation or on a LAN server machine to provide ADSM services. The most important of these is the backup/archive client.

The ADSM *backup/archive client* is the program that allows you to register your workstations with an ADSM server as a client node. Then, you can maintain backup versions of workstation (ADSM client) files, which can be restored if the original files are lost or damaged. You can also archive files that you no longer need on your workstation and retrieve the archived files only when necessary.

1.2.3 User Interfaces

You have have two methods of interacting with the system from your ADSM client workstation: the command line interface (CLI) and the graphical user interface (GUI). The CLI consists of a set of specific commands with a syntax similar to other commands that you issue from the ADSM client platform.

The GUI enables you to interact with the system through windows and action bars. Both interfaces are available for most ADSM clients, including AIX.

1.2.4 Storage Administration

ADSM has two type of users. The first is the typical user, who has data on the ADSM client system and wants ADSM server support for that data. In the AIX environment this user is the person who works at a stand-alone AIX system or uses, from a workstation, an AIX system as a data, print, or application server.

The second type of ADSM user is an ADSM administrator. An ADSM implementation can have one or more administrators, each with his or her own administrative functions and ADSM capabilities. Administrator functions include:

- Registering new users and their ADSM client systems
- Managing security for the ADSM environment
- Managing the storage management policies that provide tailored backup and archive support for user data on the ADSM client systems
- Managing the scheduling of automated backup and archive
- Determining the hierarchy of administrators (if necessary) and their specific authorities
- Initiating the disaster recovery export/import function for data stored on the ADSM server.

Several levels of authority can be given to an administrator. There must be at least one high-level administrator who has authority over the entire system.

1.2.5 Administrative Client

The administrative functions can be invoked from the ADSM server's system consoles. A more user-friendly interface is another ADSM client, the *administrative client*. This program provides functions that enable a storage administrator to:

- Control and monitor ADSM server activities
- Define storage management policies for ADSM client workstation files
- Set up schedules to provide backup and archive services at regular intervals.

The administrative client can be run from an ADSM client or ADSM server workstation. Figure 5 shows the GUI for the administrative client functions. A CLI for the administrative client is also available.

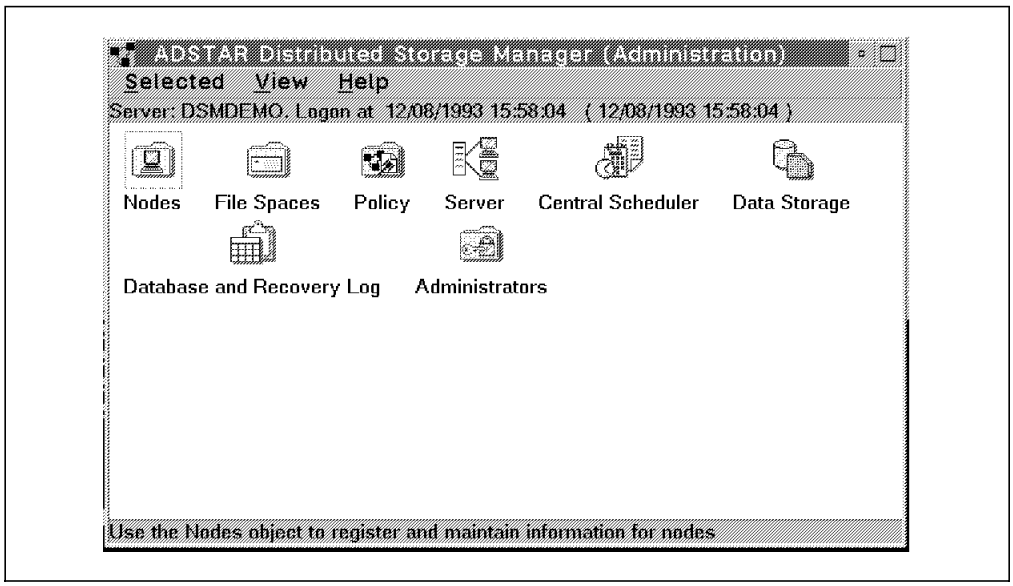


Figure 5. Administrative Client GUI

1.2.6 Application Client

The *application client* program allows other IBM and non-IBM products to use the storage management services of ADSM with a standard interface. The application client runs on the ADSM client workstation and uses an application programming interface (API) to back up, archive, restore, or retrieve objects from an ADSM server.

1.2.7 Security

Before an ADSM client can begin requesting backup or archive services, the client must be registered with the ADSM server. ADSM clients are referred to as nodes. Clients, or nodes, can be added to ADSM through either closed or open registration.

With *closed* registration, an administrator must register each ADSM client workstation in advance. With *open* registration, ADSM clients can register their own workstations with the ADSM server. When you try to access the ADSM server from an unregistered client node, ADSM prompts you for a password and contact information to dynamically register the client.

ADSM provides client/server authentication to validate that administrative or backup/archive ADSM clients are communicating with an authorized ADSM server and that the server is communicating with registered clients. You could call this “mutually suspicious” validation because the ADSM client suspects that the server is not valid, and the ADSM server suspects that the clients are not valid.

ADSM can ensure authentication by requiring a password from each ADSM client. An optional process for some of the ADSM client platforms allows you to set up the system such that users are not required to enter a password every time authentication occurs.

ADSM does not currently use platform-specific authentication and authorization procedures because it was designed to provide a common interface across multiple platforms. Thus, for example, ADSM has no interaction with RACF* when MVS is used as the ADSM server platform.

1.3 Storage Management Services

This section discusses the storage management services provided to the ADSM client. Additional details on the backup/archive client and the storage administration policies for managing ADSM client files are provided.

1.3.1 Backup Processing

The main functions of ADSM are backup and restore. You can back up all of your files (full), select specific files you want to back up (selective), or only back up the files that have changed since your last backup (incremental).

The backup process creates a copy of a client file, such as **/home/proj2/myfile**, on the ADSM server. The backup process also backs up the directory in which the file resides. You can request a backup by command, or ADSM can automatically create a backup. The administrator can establish a schedule where backup is done automatically.

All backups of a particular file are related and are called *versions*. The most current version is the *active* backup, and the other versions are *inactive* backups.

1.3.1.1 Selective Backup

You can specifically include or exclude certain files from being backed up. For example, you might not want everyone to back up their local copies of the AIX operating system. For a selective backup, use **include** and **exclude** statements, which are processed in a bottom-up order. Thus, if you have several **include**

and **exclude** statements, their order is important in determining which files are selected.

Selective backup specifies which files you want to back up. A selective backup can consist of a single file, or you can select a directory or subdirectory tree to back up. Wildcards, such as "*," are allowed in the specification, so there is great flexibility in file selection.

The files are backed up according to policies that the administrator has predefined. The policies define, for example, how many backup versions should be retained in the ADSM storage pools, how long to retain those versions, and whether to try to back up files that are in use.

1.3.1.2 Incremental Backup

Incremental backup sends the files that have changed since the last backup to the server. The first time an incremental backup is done, all files are sent to the ADSM server. Incremental backup is the most common backup approach, particularly when it is done on an automatic schedule that the storage administrator has predefined.

Incremental backup is also controlled by the use of **include** and **exclude** statements to filter in or out specific files that are considered for incremental processing. To be backed up the files need to be included and have changed since the last backup. An amount of time between backups can also be specified to prevent backups from occurring too often.

1.3.2 Restore Processing

Restore is the process of copying a backup version from the ADSM server to the ADSM client. This process is system assisted, which means that the system performs the restore at your request without having to call the ADSM administrator.

When you need to restore a file, you can either restore the latest backup copy or use an older version of the file. If you are restoring a file, ADSM provides help to prevent you from overlaying your current copy of the file.

Protection is built in to ADSM to prevent you from overwriting a file on your workstation during the restore process. A collision occurs when you restore a file and the original file still exists on the workstation. You can ask ADSM to prompt you every time a collision occurs so that you can respond on a file-by-file basis, or you can instruct ADSM never to overwrite the original files or always to overwrite the original files.

You can also protect yourself from overwriting the original files on your workstation by restoring the files to an alternative path. This would place the file into a different directory but maintain the same file name.

1.3.3 Archive Processing

ADSM has a separate archive function that lets you store files that you need to retain for long-term storage. Because the archived copy is expected to be retained for a long time, automatic deletion is not provided.

The archive process creates a copy of an ADSM client file, such as **/home/proj2/myfile**, on the ADSM server. Like backup, archived files are managed on the basis of policies, and archive can be initiated by user command or by ADSM automatic scheduling.

A key difference between backing up a file and archiving a file is that you can erase the original file after archiving it with no impact on the archived copies. Archive can be used in this way to reduce the used disk space on your workstation.

Because the archive function does not use versioning, it can be difficult to retrieve the desired copy of a file that has multiple archives. You can save a description of an archived file so that it will be easy to retrieve the file if multiple archived copies exist with the same file name.

1.3.4 Retrieve Processing

You use retrieve to obtain copies of files that you have archived on the ADSM server. You can retrieve a single file, a group of files, or all files in a directory or subdirectory. When you retrieve a file, ADSM provides support to prevent you from overwriting an existing copy on the ADSM client. The retrieved file remains intact on the ADSM server.

If a description was stored with the file on the ADSM server, you can use it to select the copy to retrieve. Selection using the description can include wildcards. You can also use the date when the file was archived to help determine which copy to retrieve.

1.3.5 General File Support

In general, ADSM supports all ordinary file types that are possible on each ADSM client.

1.3.5.1 Data Compression

Data compression is an optional feature that you can use. The data is compressed on the ADSM client workstation, thus reducing the network traffic and the storage required on the ADSM server to hold the file. The ADSM compression algorithm on average compresses the file approximately 50%.

Compression reduces the amount of ADSM server data storage space and data that must be sent across the network between the ADSM client and server. The disadvantage of compression is that it requires additional processor time on the ADSM client workstation, and thus backup runs slower on the ADSM client.

1.3.5.2 Cross-Platform Restore and Retrieve

One powerful feature of ADSM is the ability to back up and restore or archive and retrieve from different client platforms. For example, you can back up your files from your AIX workstation and then restore them on a UNIX workstation. This is very useful, for example, when all of your users migrate to a new platform or work out of multiple locations that have different client platforms.

The cross-platform restore and retrieve feature works among all UNIX clients (AIX for RISC System/6000*, Sun** SPARC** Solaris**, HP-UX**, DEC** ULTRIX**, and SCO** 386) or among DOS, Windows**, and OS/2 clients. Cross-platform restore and retrieve is also support between NetWare** ADSM clients. It is not supported between UNIX and non-UNIX clients. It is also not supported for the Macintosh** client.

1.3.5.3 Cross-User Restore and Retrieve

Another powerful feature of ADSM is the ability to have other users restore or retrieve the files you backed up. You can authorize other users access to the files you have backed up or archived on a file-by-file basis. This capability is fully available for the AIX user.

You use ADSM commands to allow other users access to your files. You also establish access for cross-user restore and retrieve through these commands.

1.3.6 Policy Management

A key power of ADSM comes from its ability to use storage management policies to invoke automatic services. Both backup and archive are examples of ADSM client services that you can control by predefined policies. In each case, you, as the administrator, can adjust the process by command parameters.

The granularity of control that you have is down to the file level. You can choose how granular you want your policies to be. You can establish an overall system policy, policies by department or organizational structure, or policies by user or file name. Policy management makes ADSM a true system-managed storage implementation.

The backup and archive functions can also be run on a predefined schedule. This feature, along with policy management, provides the power of ADSM. The ADSM administrator establishes the default policies and schedules for ADSM clients.

The elements of policy management are:

- Policy domains
- Policy sets
- Management classes
- Copy groups.

Figure 6 on page 13 shows the general relationship of these elements. Each is discussed in the sections that follow.

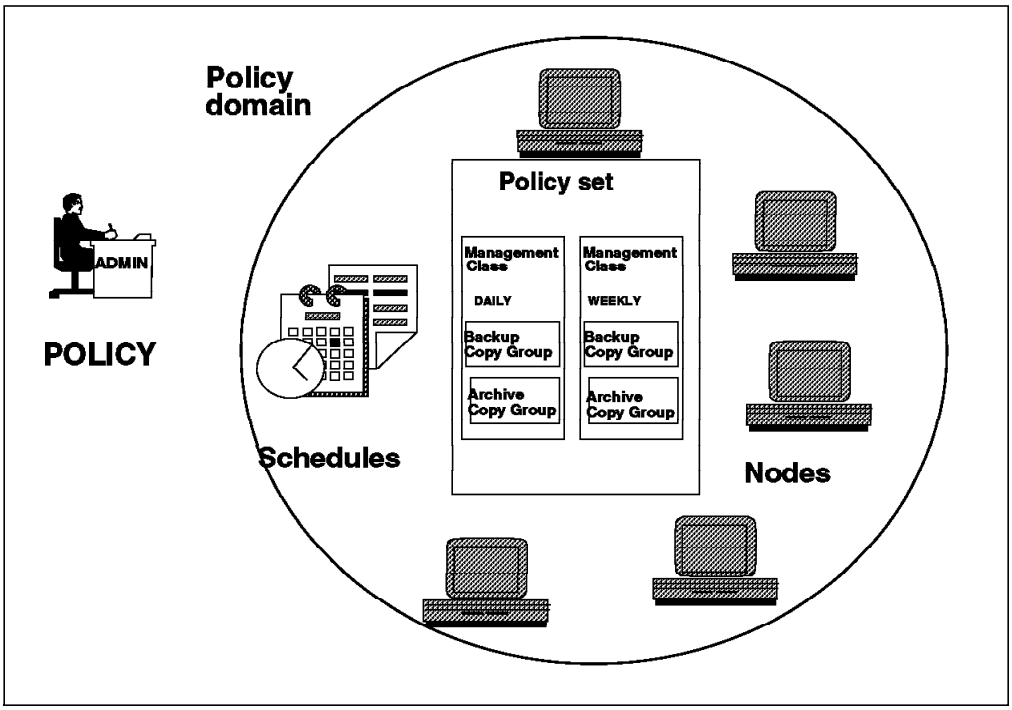


Figure 6. ADSM Policy Management

Policy management is both an ADSM client and server function. On the ADSM server the administrator is responsible for creating default policies. The ADSM client, however, can overwrite the default management class or select another management class in the client's policy domain. Clients can only select and use defined and activated policies; a client cannot define its own policies.

1.3.6.1 Policy Domain

A *policy domain* is a group of ADSM clients that use the same set of policies. All or a group of ADSM AIX clients might be associated with one domain, while ADSM OS/2 clients might be associated with another domain. Thus, policy domain provides a logical way of managing backup and archive policies for a group of client nodes.

Policy domains can be used to provide standard storage management policies to most users by grouping together ADSM clients that have similar storage management requirements. They can be used to limit the number of clients that need to be managed by a single policy administrator or restrict the number of management classes to which users have access.

A policy domain contains one or more policy sets. Each domain contains the following information:

- The domain's name
- The associated policy set(s)
- Grace period backup and archive retention periods.

Grace period backup and archive retention periods act as a safety net to ensure that backed up and archived data cannot be accidentally deleted if it loses its copy group.

Figure 7 shows three policy domains, which might reflect different departments in your organization or users with different data requirements. The first domain is used by a group of AIX users and workstations. The second and third domains support different sets of users and workstation platforms.

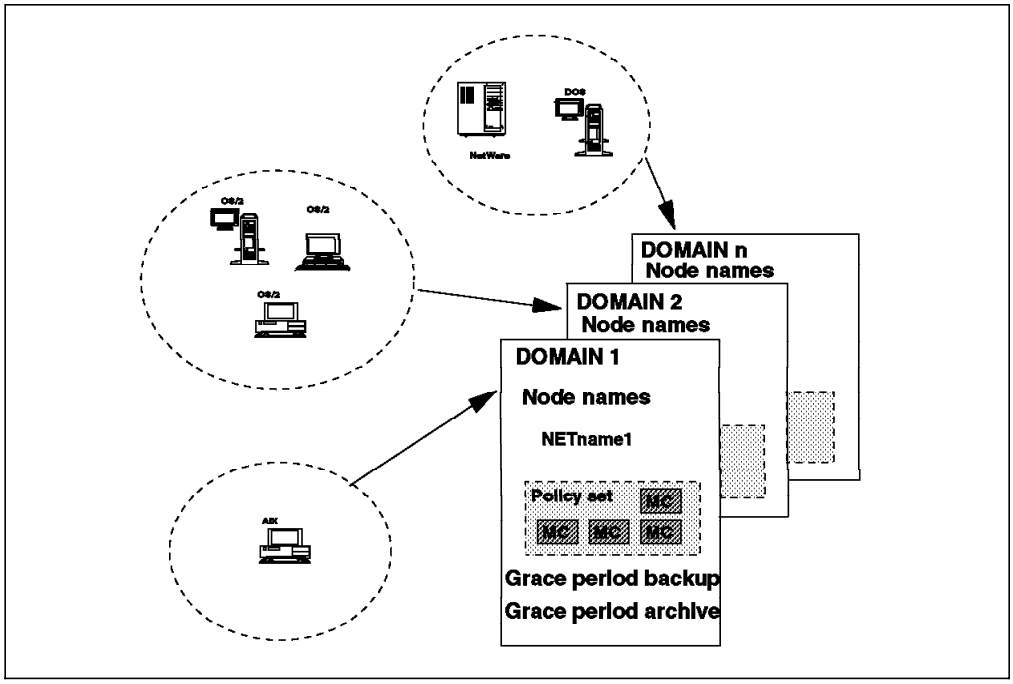


Figure 7. Policy Domains

1.3.6.2 Policy Set

A policy domain can have more than one *policy set*, but only one policy set can be activated at any point in time. In Figure 8 on page 15 you can see the ACTIVE policy set and both a NEW and OLD policy set. The OLD might be used for fallback, while the NEW policy set might still be in development for future requirements.

Each policy set contains a default management class and can contain any number of additional management classes. A management class typically contains a backup copy group and an archive copy group. Both management classes and copy groups are discussed in more detail in the sections that follow.

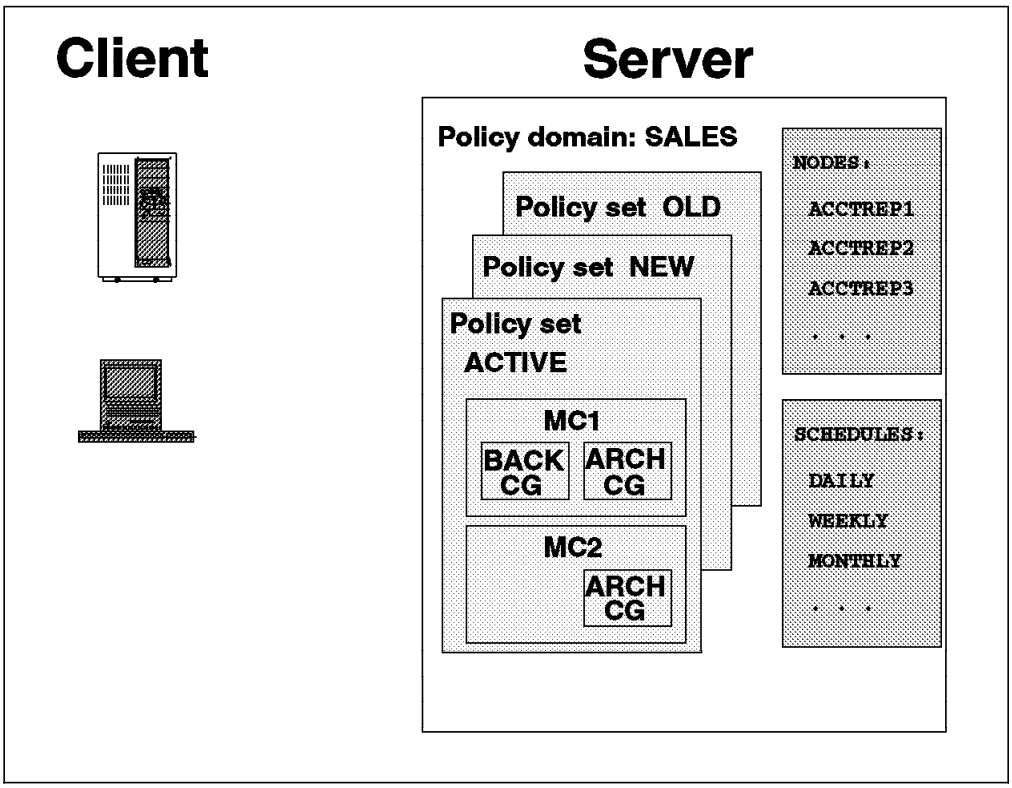


Figure 8. Policy Sets

1.3.6.3 Management Class

Policy sets contain one or more *management classes*. Management classes contain a backup copy group and/or an archive copy group or no copy group. The default management class must have a backup copy group. You can think of management classes as a Service Level Agreement you have with your clients on how their backup and archive data will be handled.

You can bind and thus associate a management class to a file when it is backed up or archived. You can rebind a file with a new management class. You can use the default management class or explicitly select a management class that is within the policy sets to which you have access. You select a management class other than the default by use of the INCLUDE statement.

1.3.6.4 Copy Group

You specify in *copy groups* the parameters that control the generation and expiration of backup and archive data. There is a separate copy group for backup and one for archive. Figure 9 on page 16 shows a backup and an archive copy group. The values shown are the defaults that are provided as part of ADSM.

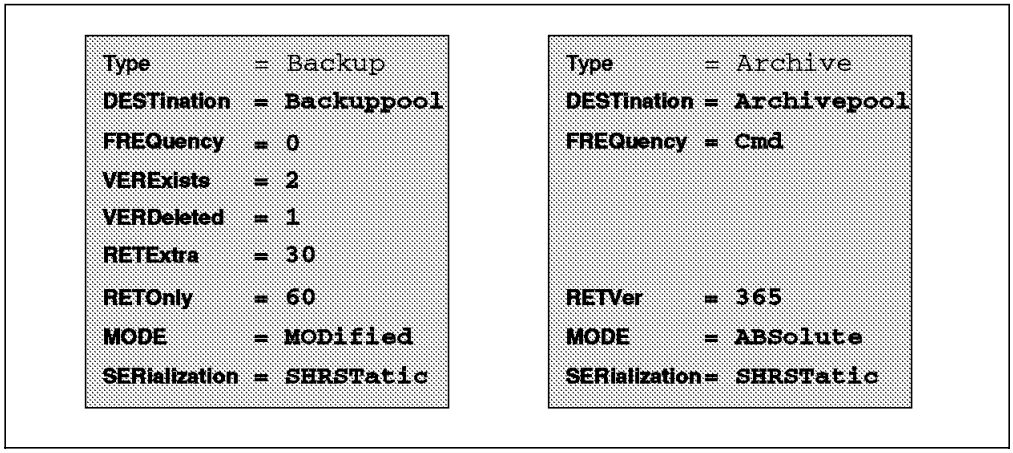


Figure 9. Copy Groups

Both backup and archive copy groups have similar parameters, except that the version parameters apply only to backup files. The parameters are:

DESTINATION Specifies the name of the storage pool where the ADSM server initially stores the backed up or archived files. The default destination for a backup copy group is BACKUPPOOL. The default destination for an archive copy group is ARCHIVEPOOL.

FREQUENCY Specifies, for a backup file, the minimum number of days that must elapse between incremental backups. This parameter is different for an archived file. A file is archived only when a client issues an archive request. The default for a backup copy group is 0 and must be cmd for an archive copy group.

Number of VERSIONS Applies only to backup files. You can specify two different parameters to tell ADSM how many versions of a backup file you want it to maintain.

The first parameter, VEREXISTS, specifies the maximum number of different backup versions the ADSM server retains for files and directories that currently exist on the ADSM client workstation. When the maximum number of versions is exceeded, ADSM rolls off the oldest version.

The second parameter, VERDELETED, specifies the maximum number of different backup versions that ADSM retains for files and directories that have been erased from the ADSM client workstation.

The default values are 2 if the file exists and 1 if the file has been deleted.

RETENTION periods Specifies how long to retain the backed up and archived files. The two retention parameters, RETEXTRA and RETONLY, for backed up files correspond to the two types of versions, VEREXISTS and VERDELETED. There is one retention parameter for archived files.

The default is 30 days for RETEXTRA and 60 days for RETONLY. The default for archived file retention is 365 days.

MODE

Specifies file backup according to whether the file has changed since the last backup. This parameter applies to incremental backups, not selective backups. The options for mode are MODIFIED and ABSOLUTE.

MODIFIED indicates that you want to back up the file only if it has changed. MODIFIED is the default value for backup copy groups. ABSOLUTE indicates that you want to back up the file regardless of whether it has changed. For archive files, the mode is always ABSOLUTE.

SERIALIZATION

Specifies how files or directories are handled if they are in use during the backup or archive process. There are four options with the serialization parameter: STATIC, SHRSTATIC, SHRDYNAMIC, and DYNAMIC.

STATIC specifies that if a file or directory is modified during the backup or archive process, ADSM will not back up or archive the file. The STATIC option is not supported on the DOS platform.

SHRSTATIC, shared static, specifies that ADSM will retry the backup operation as many times as specified in the client system options file. The default is four retries. If the file or directory is modified during each backup or archive attempt, ADSM will not back up or archive the file.

SHRDYNAMIC, shared dynamic, specifies that if a file is modified during a backup or archive attempt, ADSM will back up or archive the file only on its last retry.

DYNAMIC specifies that even if the file is modified during the backup or archive attempt, ADSM will back up or archive the file anyway. No retries are required.

The default for both backup and archive copy groups is SHRSTATIC.

1.3.7 Function Execution

An end user who has access to the ADSM client can initiate both the backup and archive functions. These functions can also be initiated with ADSM′s central scheduling facility. Thus you can decide whether you want end users to be responsible for their backups or whether you prefer the backup process to be transparent to them.

1.3.7.1 Central Scheduling

The central scheduling facility is designed to automate both the backup and archive functions. Schedules can be established to begin on certain days or times, giving you the flexibility to manage your systems on a time schedule that makes sense for your business.

The central scheduler consists of ADSM client and server processes that cooperate to execute the scheduled functions. Therefore the ADSM client workstation must communicate with the ADSM server. If you want to automate your backups for off-hours or weekends, you need to enforce a policy that requires users to leave their workstations powered on.

The administrator is responsible for defining and maintaining the schedules and has the authority to prioritize clients so that clients that contain more important data are given preferential treatment. The administrator also can limit the number of concurrent sessions that ADSM uses.

Central scheduling is not designed for automatically restoring or retrieving files. These functions must be user initiated.

1.3.7.2 Scheduling Methods

There are two scheduling modes. The first, client polling, is started by the ADSM client. The second, server prompted, is started by the ADSM server. In both cases the backup or archive is scheduled on the basis of predefined policies. The scheduler must be started at the ADSM client before either scheduling mode can begin.

With *client polling*, an ADSM client periodically queries the ADSM server for a scheduled operation. The server sends the start date and time of the operation to the ADSM client. The client waits until that time, starts the operation, and notifies the ASDM server. On completing the operation, the ADSM client notifies the ADSM server that the operation has completed.

With *server prompted*, the ADSM client registers its TCP/IP address with the ADSM server and waits. The ADSM server connects to the client according to a predefined schedule. The ADSM client starts the operation (backup or archive) and at completion notifies the ADSM server that the operation has completed. Because server prompted scheduling is controlled by the ADSM server, it maximizes the use of scheduled sessions and other ADSM resources.

The administrator sets the schedule by specifying start time windows for those days on which either backup or archive should run. A schedule could be daily, twice a week, once a month, or whatever is appropriate for the data.

The client must start the operation within the startup window. If the client cannot perform the operation within that window (for example, because the network is down or the terminal is turned off), the client waits until the next occurrence of the startup window. Although the operation must start within the window, it may complete outside the window.

1.3.8 Client System and User Options Files

The ADSM client environment has many parameters with which you can request services, tailor the way services process, or customize the ADSM client/server system. Most of these parameters can be predefined, but you also can enter them on commands.

These parameters also can be included in ADSM files at both the server and client for automatic execution. The file on the ADSM server is the server options file. The files on the ADSM client are the client system options file, **dsm.sys**, and the client user options file, **dsm.opt**. The client system options file includes options that are in effect for the entire AIX client system. The client user options file includes options for a single user of the ADSM client. There may be multiple client user options files on the ADSM AIX client system. These options can also be entered on ADSM client commands, such as those used to back up, archive, restore, or retrieve data.

1.3.8.1 Communications Options

The client system options file must contain the control statements that select the communications protocols that will be used between the ADSM client and server. This is where you would choose either TCP/IP or APPC. Depending on the protocol you select, other communications parameters may also be required in the options file.

The client user options file must contain the control statement that selects the ADSM server that you want to use for this execution of ADSM. The server control statement in the client user options file is used to select the server control statements and the communications protocol to be used from the client system options file.

1.3.8.2 Scheduling Options

The client system options file also includes information that affects backup and archive scheduling. The type of scheduling to be used, client polling or server prompted, is specified along with other scheduling information including how long the ADSM client scheduler should wait between attempts to contact the ADSM server for scheduled work.

1.3.8.3 Backup and Archive Options

You can use **include** and **exclude** statements in an include/exclude file to control the selection of user files that will or will not be processed during backup or archive. The name of the include/exclude file is provided in a control statement in the client system options file. Data compression can be selected for the ADSM client by an entry in the client system options file.

You use the **domain** statement in the client user options file to identify the volumes that should be processed during incremental backup.

ADSM provides a command to control whether subdirectories should be included or excluded when processing their directories for backup and archive. This control statement is provided in the client user options file.

You can add a parameter to the client user options file to control whether the ADSM client will allow overwriting files on either a restore or retrieve request. The option to have the user prompted for each file is also available.

1.3.8.4 User Interface Commands

You can specify in the client user options file the format of how ADSM will display dates, time, and numbers at the ADSM client's workstations. There is also a statement that can select the national language in which ADSM messages will be displayed. All languages are not available, but this statement will be useful as additional languages are added to ADSM.

Chapter 2. Introduction to AIX

The AIX operating system is IBM′s UNIX implementation. In this chapter we explain the basic characteristics of the IBM AIX version 3 operating system.

If you are an experienced AIX or UNIX user you should skip this chapter. This entire book is an introductory discussion of using ADSM with AIX. Advanced ADSM implementation considerations, the integration of ADSM with other AIX products, or other topics oriented only to an AIX specialist are not found in this book.

The AIX for RISC System/6000 operating system is designed to optimize performance with RISC System/6000 hardware and provides user and programming environments that support open systems. AIX for RISC System/6000 supports multiple users and multiple concurrent tasks.

To provide AIX system users with compatible operating system features, AIX for RISC System/6000 has been designed to comply with a number of industry standards. AIX for RISC System/6000 is upwardly compatible with the following standards:

- AT&T System V Interface Definition (SVID) issue 2
- Version 4.3 Berkeley Software Distribution (BSD)
- Portable Operating System for Computer Environments (POSIX), IEEE Standard 1003.1-1990
- International Standards Organization (ISO) 9945/1-1990, X/Open Portability Guide Issue 3(XPG3).

The following AIX operating system features are described below:

- System structure
- Shells (command interpreters)
- Processes
- Logical volume storage
- File systems
- AIX extensions to UNIX
- File security
- Communication services
- AIX user interfaces.

2.1 System Structure

The AIX operating system is an implementation based on the original UNIX system from AT&T. Figure 10 on page 22 shows the basic system structure of the UNIX operating system.

© Copyright IBM Corp. 1994

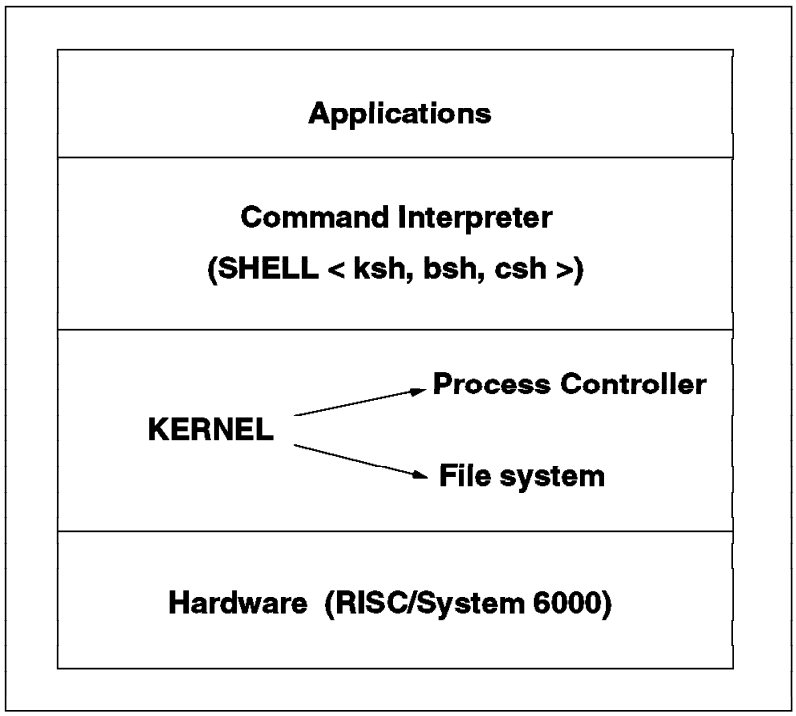


Figure 10. UNIX System Structure

The user interface to the UNIX operating system is called a command interpreter or shell. Shells provide a way for the user to communicate with the operating system. They can be used either interactively (input from the keyboard is acted on immediately) or from a script. A shell script is a file that contains operating system commands and statements that the shell understands.

When a shell program is executed, a command prompt is displayed and waits for user responses. When you type a command or shell script after the prompt and press Enter, the shell evaluates the command or shell script and executes it.

The kernel is the memory resident part of the AIX operating system. It contains the system functions that are most frequently used. The kernel acts as the interface between processes and the hardware.

A process is the term used for a program that is executing on AIX. If several users simultaneously use the same program, each user has his or her own process, but there is only a single program.

You request AIX functions through commands. Because AIX commands are case sensitive, with an ADSM AIX client you must enter ADSM commands, which normally can be either uppercase or lowercase, as lowercase. The system management interface tool (SMIT) is a menu-driven interface that you can use to request AIX functions instead of using commands.

2.2 Shells

Three types of shell are available in the AIX operating system:

- Bourne shell - **bsh**
- Korn shell - **ksh**
- C shell - **csh**.

The Bourne shell is an interactive command interpreter and program language. It provides I/O redirection capabilities, variable substitution, and filename substitution. You use the **bsh** command to invoke the Bourne shell.

The Korn shell offers a superset of the Bourne shell. It provides several additional commands and programming language features such as arithmetic evaluation, command history, a coprocess facility, and editing. The Korn shell is used most often by commercial sites interested in transactional database work and is the default shell for the AIX operating system. You use the **ksh** command to invoke the Korn shell.

The C shell offers an environment that is familiar to C programmers. It uses syntax that is similar to the C programming language. The C shell is used most often by sites involved in engineering, research, computer-aided design, or education. You use the **csh** command to invoke the C shell.

2.3 Processes

In this section we describe AIX processes and show how to check which processes are active in your system. A program or command that is actually running on the RISC System/6000 is referred to as a process. A program that starts another program is called a parent process. A child process is the product of the parent process. The mechanism that the parent uses to create a child is referred to as spawning.

Each process is assigned a process identification (PID) number as it starts. The parent's PID is referred to as the parent process identification (PPID) number. When a process is started on a system, the process uses available system resources. When more than one process is running, processes are prioritized to share the system resources.

There are several ways to categorize processes:

- Foreground
- Background
- Daemons
- Defunct
- Zombie.

Foreground and background processes essentially perform the same function but are started in different ways. Foreground processes are spawned from the user's shell and run as a child process. The user does not regain control of the

shell until the command has completed execution. This is the normal method of submitting and interacting with commands. When you use the ADSM backup and archive services or invoke some applications, you usually perform a foreground process.

Background processes are spawned from the current shell, like foreground processes, but they run independently of the shell. You regain control as soon as the background process has started.

Commands can be placed in the background by appending an ampersand, **&**, to the command. For example, the **ls -la** command produces a directory listing in the foreground and only returns control of the shell to you when it has completed. The **ls -la&** command produces the same listing in the background independent of the shell, and you regain control of the shell immediately after entering the command.

Processes requiring interactions with the display terminal are generally designed to operate as foreground processes. They may be started as background processes, but their execution is suspended when they require terminal interaction (for example, input from the keyboard).

Daemon processes are long-running background processes performing independently of operator intervention. An example of a daemon is the **inetd** process. This process waits for incoming requests to use a particular service and then connects the incoming request to the correct application. The **inetd** process always runs as a background process, with no intervention from a display or user.

The printing and communication services are available for all AIX users as default daemons. The ADSM client can be run as a daemon by adding the execution files to the **/etc/rc** file. Every time the machine is started up, the ADSM client will start up and establish communication with the ADSM server.

Defunct processes are those that have a PID number and are still recognized in the process table but have no other system space allocated to them in either the user or kernel space. Defunct processes exist until their parent stops or the system is shut down and restarted.

Zombie processes are like defunct processes, but they do not have a parent associated with them. They can be removed only by shutting down the system. Defunct and zombie processes are usually the result of an abnormal ending of some process.

Many processes run whenever the system is active. Some may belong to you, some to other users, and some to the root or system supervisor user. You can use the **ps -ef** command to query which processes are running and display information about those processes as shown in Figure 11 on page 25.

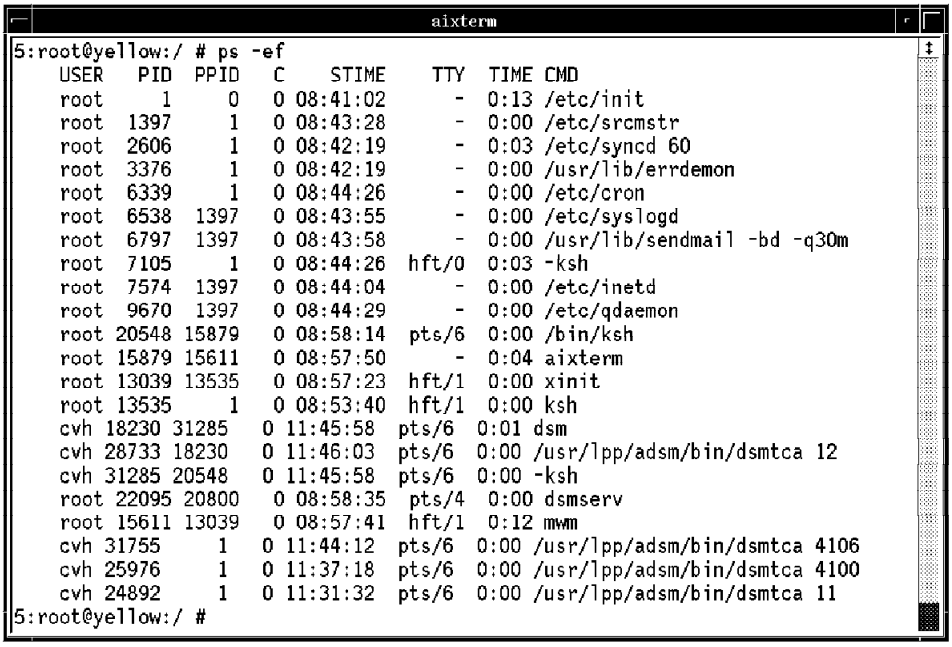


Figure 11. Listing of Running Processes

Using the **ps -ef** command you can find information about all processes. For example, the **dsm** process (nine lines from the bottom), issued by user **cvh**, is assigned a process ID of 18230. The parent process ID of 18230 is 31285. The information also indicates the process starting time and how long this process has been executing. By tracking back through the PID and PPID information, you can trace the original parent process, **/etc/init**, which was created when the system was started.

2.4 Logical Volume Storage

Logical volume storage provides a mechanism, invisible to users and applications, of dividing and allocating storage space on the AIX system′s read/write disks.

At the base of the logical volume storage system lies the hard disk drive, or disk. To be used by the operating system, the storage space on a disk must go through a process of configuration and manipulation. Figure 12 on page 26 provides an overview of how the AIX operating system manages logical volume storage.

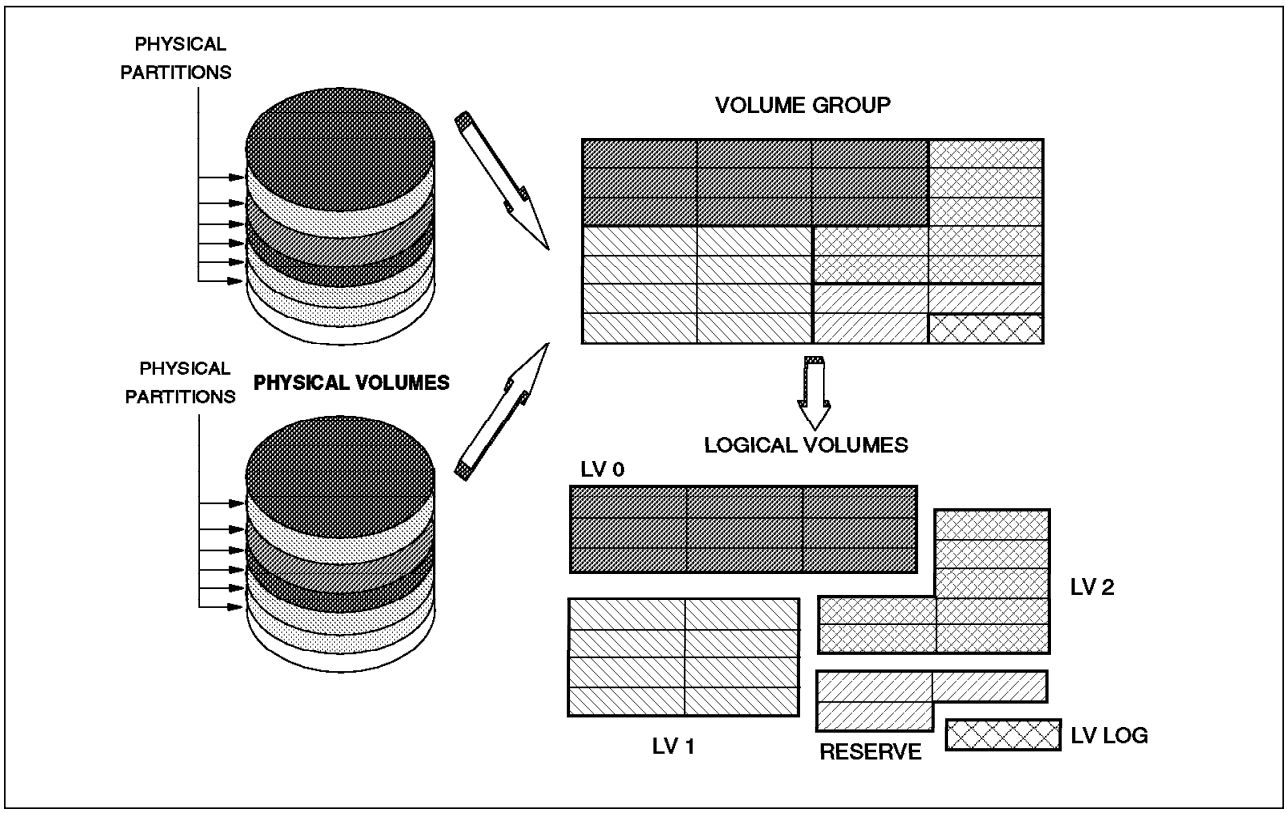


Figure 12. Logical Volume Storage

Logical volume storage provides a level of flexibility to configure the disk subsystem that does not exist in the base UNIX system. The components of logical volume storage are:

- Logical volume manager
- Physical volumes
- Volume groups
- Physical partitions
- Logical volumes
- Logical partitions.

2.4.1 Logical Volume Manager

The logical volume manager (LVM) provides tools and commands that allow you to establish and control logical volume storage. The LVM is responsible for mapping physical partitions to logical volumes. The LVM consists of the logical volume device driver (LVDD), the LVM daemon, and the LVM subroutine interface library.

The LVDD is a pseudo device driver that manages access to logical volumes. The LVM daemon provides services to the LVDD and the system management subroutines. The LVM subroutine interface library contains routines that facilitate communication between system management applications, including the operating system commands, and the LVDD.

Data on the logical volumes appears to the user to be contiguous, but it may not be contiguous on the physical volume. This mapping allows file systems, page spaces, and other logical volumes to change size, be relocated, span multiple physical volumes, and have their contents replicated for greater availability in the storage of data.

2.4.2 Physical Volumes, Groups, and Partitions

A physical volume is nothing more than a disk, connected to the computer system, with certain configuration and identification information written to it. This information includes a systemwide unique physical volume identifier.

Once a physical volume is created it must be added to a volume group. A volume group is a collection of 1 to 32 physical volumes of varying size and type.

When you add a physical volume to a volume group, the physical volume is partitioned into contiguous, equal sized units of space called physical partitions. A physical partition is the smallest unit of disk space allocation.

2.4.3 Logical Volumes and Partitions

After you create a volume group, you can create logical volumes within that volume group. A logical volume is a collection of logical partitions, and it is where a file system resides.

You can define either logical volumes (without a file system that resides in the logical volume) or a file system. For more information refer to the *AIX Systems Management Guide*.

When you create a logical volume, you specify the number of logical partitions for the logical volume. A logical partition is one, two, or three physical partitions, depending on the number of copies you specify for the logical volume. Therefore, if you specify only one copy of the logical volume, there is a direct mapping of logical partitions to physical partitions. Various flags on the **mklv** command used to create the logical volume determine which physical partitions get selected for the logical partitions.

All available physical volumes can be divided into one or more volume groups. Therefore users can separate a logical volume for special purposes, such as page space, a file system, a journal log, boot data, or dump storage. Because a logical volume is a collection of physical partitions within a volume group, the number of copies, the location, and the size of a logical volume can be dynamically changed once the logical volume is created.

2.5 File Systems

Logical volume storage controls allocation of disk space down to the physical partition level. Finer levels of data management are accomplished by higher level software components such as the virtual memory manager or the file system. Therefore, the final step in the configuration of a disk is the creation of

a file system. You can create one file system per logical volume. To create a file system, use the **crfs** command. You do not need to create a logical volume first.

A file system is a hierarchical structure (a file tree) of files and directories. This type of structure resembles an inverted tree with the root at the top of the structure and the branches at the bottom. Figure 13 shows the AIX version 3 hierarchical file structure.

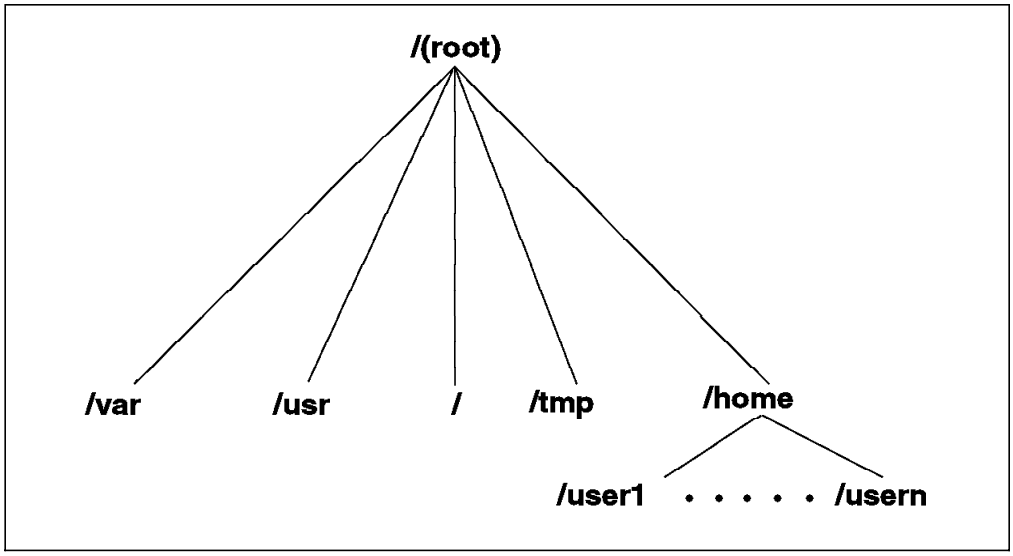


Figure 13. AIX Version 3 File Structure

This file tree uses directories to organize data and programs into groups, allowing the management of several directories and files at one time. The file system must be mounted to the system so that data, files, and programs can be accessible. When multiple file systems are mounted, a directory structure is created that presents the image of a single file system.

2.5.1 File System Types

AIX version 3 provides support for multiple file system types. These include the following:

- Journaled file system (JFS)

  JFS is the native file system type provided by AIX version 3. This file system uses database journaling techniques to maintain its structural consistency.

- Network File System (NFS)

  NFS permits files residing on remote machines to be accessed as if they reside on the local machines.

- CD-ROM

  This file system type allows the contents of a CD-ROM to be accessed through the normal system interface (open, read, and close).

- Transarc's Andrew File System (AFS)

  AFS provides the ability to see a single image of the file system even though parts of the file system may be scattered across many machines.

- Database systems

  Database systems are extensions to file systems, such as Oracle**, INFORMIX-Online**, Sybase**, and DB2/6000*, that have functions to control data integrity, allow data sharing, and provide device and platform independence.

The file systems listed above can be used with ADSM. Database systems have additional considerations for backup and recovery that are not covered in this book (see *Using ADSM to Back Up Databases*, GG24-4335).

2.5.2 Files and Directories

A file is a collection of data in a format that can be read or written. Files are typically grouped in a unique type of file called a directory. Directories contain files, subdirectories, or a combination of both. Every file and directory within a file system has a unique name.

The AIX file system contains many different kinds of files. In fact, everything that is stored on disk and is accessible to the user is a file, including:

- Text files that are human-readable using the American National Standard Code for Information Interchange (ASCII) character set
- Binary files such as those created by a compiler
- Directories, a special type of file that points to a group of files
- Device drivers, such as those found in the **/dev** directory.

Files can contain several different types of data. Some of the different data types that are in an AIX system are:

- Operating system data
- Configuration files
- Application system data
- User data (shared or nonshared)
- Print files.

The data types that you should back up or archive are described in 4.1, “Running the ADSM Client” on page 83.

2.6 AIX Extensions to UNIX

AIX adds unique features that extend the basic UNIX structure. Some of those features include extensions to the kernel, such as the LVM and the system resource controller (SRC). Other features, such as the object data manager (ODM) and the software vital product data (SWVPD), provide system management applications that facilitate the management and maintenance of the AIX system. These features are briefly described below.

2.6.1 Logical Volume Manager

The LVM is an extension to the kernel file system, discussed in 2.4.1, “Logical Volume Manager” on page 26. It enhances data storage from the fixed physical limits of physical volumes to a more flexible system by allowing the size of a logical volume to span multiple physical volumes.

2.6.2 System Resource Controller

The SRC extends the process controller function of the UNIX operating system to provide a set of commands and subroutines that make it easy to create and control system resources. The SRC is designed to minimize the need for operator intervention in system processing. It provides a common way of starting, stopping, and collecting status information on processes.

2.6.3 Object Data Manager

The ODM is a data manager for the storage of system data. Many system management functions use the ODM database. System data that the ODM manages includes:

- Device configuration information
- Display information for SMIT
- Vital product data for installation and update procedures
- Communications configuration information
- System resource information.

2.6.4 Software Vital Product Data

Information about a software product and its installable options is maintained in the SWVPD database. The SWVPD consists of a set of commands and ODM object classes for the maintenance of software product information. You can use **lslpp** and **lppvk** commands to list and verify the installed software products.

2.7 File Security

For AIX you need to know which files and directories you own and how they can be accessed.

2.7.1 Ownership

Every file and directory has an owner. Initially a file's owner is the userid of the person who created the file. The owner of a file sets the permissions, which determine who may read, write (alter), or execute the file. Only the root user can change the owner of a file.

2.7.2 Access

Access to files in the AIX environment is controlled by permissions. Three levels of permissions can be specified for files and directories:

- User
- Group (user's group)
- Other groups.

Permissions can be controlled at the user or group level. Group permissions are useful if users work together in teams, or if many users need the same permissions. By default the user's group and other groups have read permission to the file unless the owner specifically changes the permissions. The root user of the system has access to all files.

Figure 14 shows the output of an **ls -la** command that you can use to list the permission settings of files.

```
aixterm
5:root@yellow:/home # ls -la
total 160
drwxr-xr-x  20 bin      bin          512 Feb 16 17:20 ./
drwxr-xr-x  24 bin      bin         1536 Feb 18 10:28 ../
drwxr-xr-x   6 adsm     staff        512 Jan 31 12:02 adsm/
drwxr-xr-x  11 aixcase1 system      1536 Dec 17 16:38 aixcase1/
lrwxrwxrwx   1 root     system        25 Aug  4 1993  aixcase3@ -> /nfs/bering/h
ome/aixcase3/
drwxrwxr-x   2 root     system       512 Jan 22 1970  caseproj/
drwxr-xr-x  10 lrconas  staff       1024 Aug 20 1993  conas/
drwxr-xr-x   2 cvh      staff        512 Feb 18 08:57 cvh/
drwxr-xr-x   4 db2      sysadm       512 Aug 13 1993  db2/
drwxr-xr-x   4 root     staff        512 Jan 22 1970  delilah/
drwxr-xr-x   2 guest    usr          512 Jul  9 1993  guest/
drwxr-xr-x   3 root     staff        512 Jan 22 1970  guest1/
drwxr-xr-x   2 root     staff        512 Jan 22 1970  guest2/
drwxr-xr-x   4 lrconas  staff       1536 Aug 13 1993  lrconas/
drwxr-xr-x   2 mark     staff        512 Jan 25 14:04 mark/
drwxr-xr-x   2 root     staff        512 Jan 22 1970  oracle/
drwxr-xr-x   3 richard  staff        512 Jan 25 14:05 richard/
drwxr-xr-x   2 sally    staff        512 Jan 25 14:05 sally/
drwxr-xr-x   2 user1    project      512 Jan 25 17:07 user1/
drwxr-xr-x   3 user2    project      512 Jan 25 17:14 user2/
drwxr-sr-x   2 walter   staff        512 Jan 28 14:20 walter/
5:root@yellow:/home #
```

Figure 14. Listing of File Permissions

As you can see in the listing, each file and directory has a set of permissions, a user, and the user's group associated with it. For example, the fourth line from the bottom shows a directory for **user1** that has an owner of **user** in the group **project**.

The first ten characters of this line describe the file type (first character) and the permissions. Characters 2 through 4 indicate the permissions for the user, characters 5 through 7 indicate the permissions for the user's group, and characters 8 through 10 indicate the permissions for the other groups.

In this example, the file type is a directory, d, where the owner, user1, has read, write, and execute (rwx) access, while the project and all other groups have only read and execute (r-x) access.

Write-only access to a file does not imply that you also have read access. You must specify both in order to have read and write access. A user with root privilege can change the owner of a file or directory by using the **chown** command. You can change the permissions for a file or directory by using the **chmod** command. For more information about file and directory ownership and permission refer to the *AIX Systems Management Guide.*

2.8 Communication Services

The IBM RISC System/6000 system can communicate with different systems over a variety of networks. In this section we describe the communication hardware and protocols of the RISC System/6000.

2.8.1 Hardware

The RISC System/6000 system unit can communicate with other systems using the following type of connections:

- Ethernet version 2 LAN
- IEEE 802.3 LAN
- IEEE 802.5 LAN
- IBM token-ring LAN
- X.25 wide area network (WAN)
- Synchronous data link control (SDLC) WAN
- Block multiplexer channel connection
- Control unit terminal (CUT) coaxial connection
- Distributed function terminal (DFT) coaxial connection
- 5088 or 6098 graphics control unit coaxial connection
- Asynchronous connection
- Fiber distributed data interface (FDDI) LAN
- Enterprise Systems Connection Architecture (ESCON)
- Serial optical channel
- High-performance parallel interface (HIPPI).

2.8.2 Communication Protocols

The RISC System/6000 supports many protocols. However, not all of those protocols support all of the connections described above. The most popular protocols used in the RISC System/6000 are TCP/IP and APPC.

2.8.2.1 TCP/IP

TCP/IP provides facilities that make the computer system an Internet** host that can attach to a network and communicate with other Internet hosts. TCP/IP is a standard feature of the AIX operating system. It includes commands and facilities that allow you to:

- Transfer files between systems
- Log in to remote systems
- Print files on remote systems
- Run commands on remote systems
- Send electronic mail to remote users
- Converse interactively with remote users
- Manage a network.

2.8.2.2 SNA and APPC

SNA provides a highly reliable and high-performance communications protocol between various network nodes running SNA products. The AIX product that provides SNA services for the RISC System/6000 environment is AIX SNA Server/6000 version 2.1. This is an additional product that would be installed along with AIX version 3.

AIX SNA Server/6000 is designed to provide a full set of SNA functions to communicate with other applications or systems using IBM′s SNA as the communication protocol. AIX SNA Server/6000 supports the following functions:

- Advanced Peer-to-Peer Networking (APPN) network nodes and end nodes
- Low-entry networking (LEN) nodes either connected to an APPN network or in a network using independent LU type 6.2 for peer communications
- Dependent communication with a host in a subarea network using dependent LU types 0, 1, 2, 3 and 6.2
- SNA gateway connectivity through a RISC System/6000 workstation supporting dependent communication between multiple hosts and workstations using the SNA Gateway/6000.

ADSM uses independent LU type 6.2 and APPC for its SNA connection between ADSM servers and an ADSM AIX client. APPC allows two partner programs to communicate with each other as peers.

2.9 AIX User Interfaces

IBM AIX provides user interfaces to help manage and install the system. In this section we introduce two of these user interfaces.

2.9.1 System Management Interface Tool

SMIT is the primary interface available for managing the system. Many system management tasks that you perform with commands can be quickly performed by using SMIT. The SMIT facility provides a task-oriented interface that steps you through menus and dialogs to accomplish complex system management tasks.

With SMIT, you can:

- Install, update, and maintain software
- Configure devices
- Make and extend file systems and paging space
- Manage users and groups
- Configure networks and communications applications
- Print jobs
- Perform problem determination
- Schedule jobs
- Manage system environments.

SMIT is a menu-driven, command-building facility. As you make menu selections or are prompted for parameters, SMIT builds and runs the appropriate command. SMIT also builds shell scripts in a Korn shell format. The file **smit.script** in the user **$HOME** directory is used to tailor the SMIT menus.

There are two interfaces to SMIT, GUI and text. The GUI interface is based on AIXwindows* and can be viewed only on a graphics display. The text interface can be viewed on a variety of text displays (also known as ASCII terminals), such as the IBM 3151 and many non-IBM displays. Figure 15 on page 35 shows an example of the SMIT GUI as viewed on a graphics display.

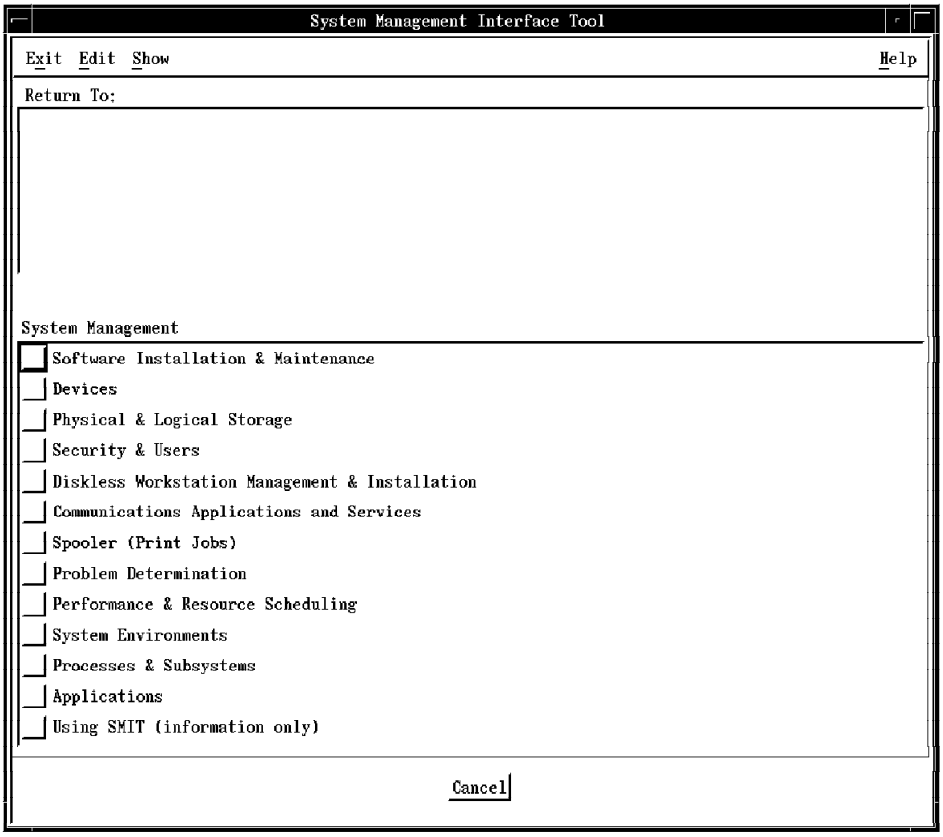


Figure 15. SMIT GUI

Figure 16 shows the general SMIT text interface viewed in an AIXwindow display.

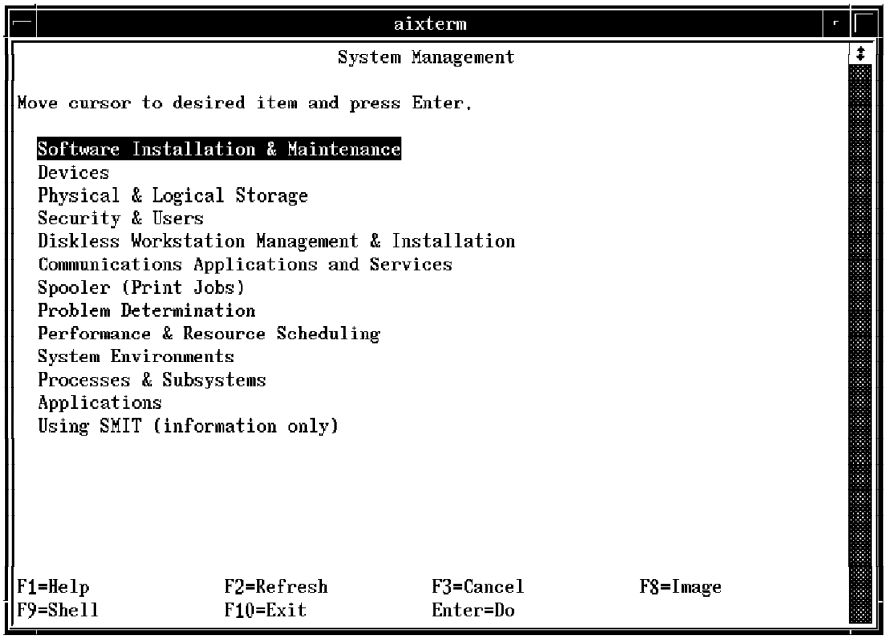


Figure 16. SMIT Text Interface

2.9.2 AIXwindows

The AIXwindows interface provides features that help you manage the windows on your AIX system. The AIXwindows interface provides functions for opening, closing, moving, and resizing windows. AIXwindows allows you to run several programs simultaneously on a single screen, create multiple windows to meet your specific needs, and personalize your environment to suit your preferences.

AIXwindows allows you to cut and paste text between windows, move between windows with the mouse, and represent programs on the screen with icons. The AIXwindows provides the GUI support for the ADSM/6000 client.

Chapter 3. Implementing the ADSM AIX Client

In this chapter we cover the implementation of the ADSM AIX client. We explain how to install the client code, tailor the basic client options, and set up the various connectivity options available between the ADSM AIX client and an ADSM server.

3.1 Installing the ADSM Client

This discussion assumes that the ADSM server and the communications protocols to be used are installed and operational.

3.1.1 Hardware Requirements

The RISC System/6000 requires the following hardware resources to run the ADSM AIX client and perform adequately:

- System processor

  Requires any RISC System/6000 POWERserver* or POWERstation* (see *RISC/6000 System Overview and Planning* for additional information).

- Disk capacity

  Requires approximately 10MB of additional disk space.

- Memory

  Requires no additional memory, but you should have a well-tuned AIX system.

- CLI

  Requires an ASCII terminal with a keyboard, like the IBM 3151, attached through the workstation′s serial interface.

- GUI

  Requires a graphic terminal, like the IBM POWERdisplay 20, attached through one of the workstation′s available graphic adapters. The workstation must have a mouse in addition to its keyboard.

- Communications

  Requires a communications adapter. You can use the communications adapter that already supports host connection.

3.1.2 Software Requirements

To implement the ADSM AIX client on the RISC System/6000 you should have the following software installed:

- AIX version 3.2 or later

  AIX version 3.1.5 is supported but not recommended.

© Copyright IBM Corp. 1994

- ADSM AIX client code
- AIXwindows

  This product is required if you want the GUI for either the backup/archive or administrative clients (it is not required for the CLI). See the *AIX Installation Guide*.
- TCP/IP or APPC
- AIX SNA Server/6000 version 2.1 or later if APPC is used

  AIX SNA Server/6000 version 1.2 is supported but not recommended.

3.1.3 Installation

The ADSM AIX client is supplied on 3.5-inch diskettes. The diskettes contain all of the software needed for installation. The software installation is straightforward and takes a short period of time for a single workstation.

Two versions of SMIT are available in the AIX version 3 operating system (ASCII and AIXwindows interfaces). You can use either one to install the ADSM AIX client. As you install the ADSM backup/archive client code, the ADSM administrative client code is also installed; **dsmadm** for the GUI and **dsmadmc** for the CLI.

The example below describes how to install the ADSM AIX client using the ASCII version of SMIT. For a detailed discussion of installation with the GUI, refer to *ADSTAR Distributed Storage Manager User's Guide and Reference for UNIX*.

To install your ADSM AIX client perform the following actions:

1. Enter **smit install_latest** on the command line.
2. Press F4.
3. Enter the installation media for your install.

   You now see the panel shown in Figure 17 on page 39.

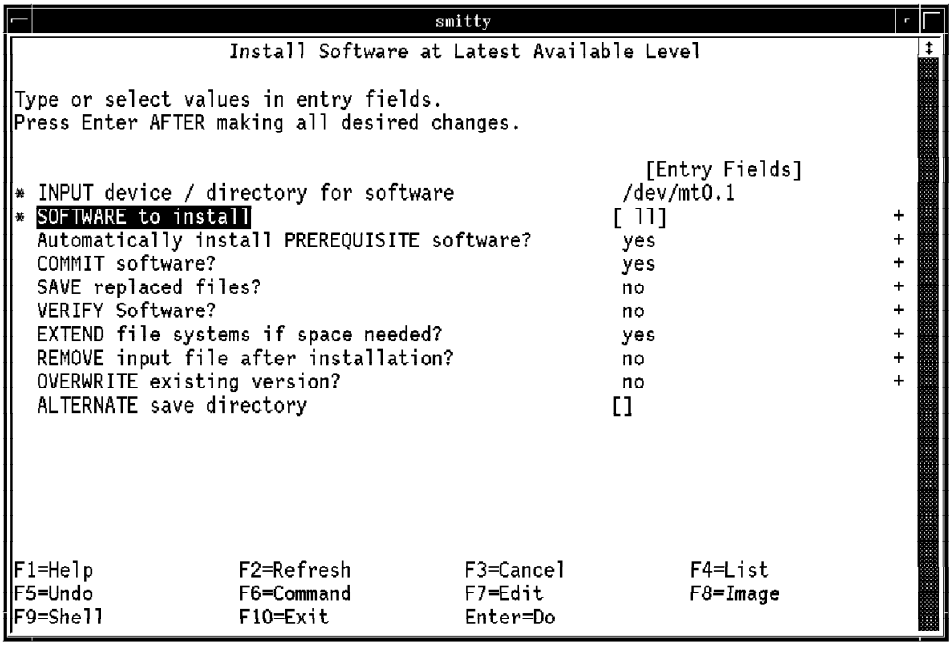


Figure 17. Installing the ADSM AIX Client: Install Software at Latest Available Level

4. Move the cursor to **SOFTWARE to install**.
5. Press F4.

   You now see the panel shown in Figure 18.

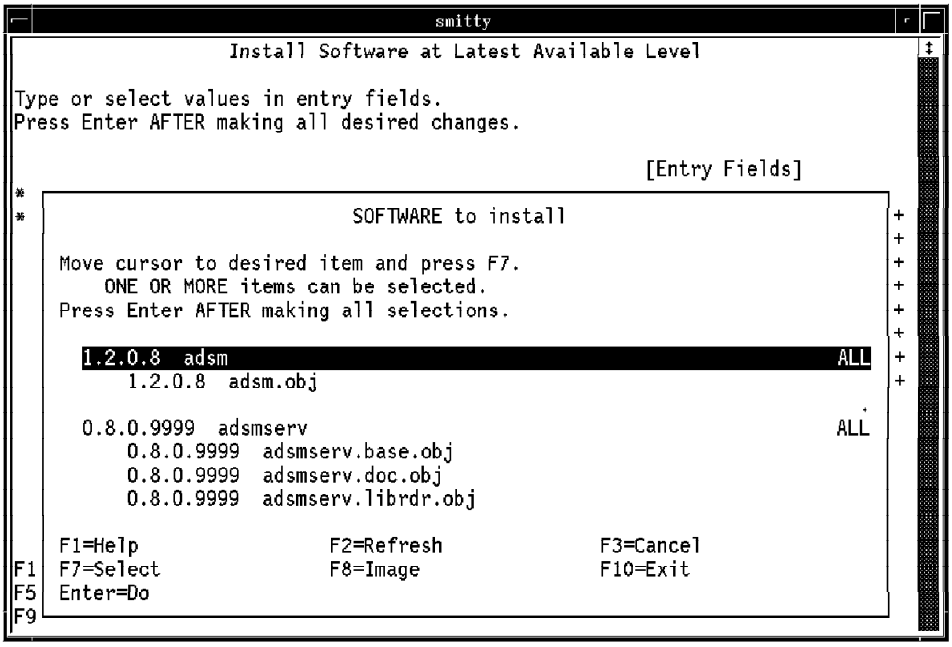


Figure 18. Installing the ADSM AIX Client: Software to Install

6. Move the cursor to **adsm**.

7. Press F7.
8. Press Enter twice.

   This starts the installation of ADSM.
9. Check for **OK**.

   You must have an **OK** at the top of the window. **OK** indicates that the installation of the ADSM AIX client code is complete.

3.2 Tailoring the ADSM Client

Two options files need to be tailored in the ADSM AIX client. The client system options file, **dsm.sys**, controls the client/server communication, backup and archive management, authorization, and schedule options. The client user options file, **dsm.opt**, is used to control processing for sessions with the ADSM server and the ADSM client′s user interface.

You must be a root user or have equivalent privilege to tailor the **dsm.sys** file. Any one who has access authority in ADSM can modify the **dsm.opt** file or create their own client user options file. A root user or a user with equivalent privilege can create an include/exclude file to specify which files can be backed up or archived and which files are excluded from backup or archive.

3.2.1 Updating the Client System Options File

To create and edit **dsm.sys**, you copy the sample client system options file, **dsm.sys.smp**, from the **/usr/lpp/adsm/bin** directory (the directory where the ADSM client typically is installed). You need to modify the required options in this file. Four groups of options can be modified:

- Communications options
- Authorization options
- Backup and archive options
- Scheduling options.

These options customize the ADSM client for communication with the ADSM server, provide access authorization for ADSM services, determine backup and archive services for the AIX files, and determine scheduling options for automatic ADSM functions. These options cannot be overridden from the command line, and the file must reside in the ADSM installation directory, **/usr/lpp/adsm/bin**. A complete example of a **dsm.sys** file can be found in Appendix A, “Sample ADSM Client Options Files” on page 111.

3.2.1.1 Communication Options

The ADSM AIX client currently provides two communication protocols, TCP/IP and APPC. Regardless of which protocol you use, you must first provide a name for your ADSM server:

- **servername**

This parameter specifies the name you want to use to identify an ADSM server to which you want to connect.

Next you configure the communication options for either TCP/IP or APPC. For each protocol, respectively, you specify the following additional options:

- **commmethod tcpip**
  - **tcpport**

    Specifies the TCP/IP port address used to communicate with an ADSM server. The default for this option is 1500.
  - **tcpserveraddress**

    Specifies the TCP/IP Internet address for the ADSM server. The value you enter can be either a TCP/IP Internet domain name, for example, **blue.sanjose.ibm.com**, or a dotted decimal address, for example, 9.113.36.100.
  - **tcpbuffsize**

    Specifies the size you want to use, in kilobytes, for the ADSM internal TCP/IP communication buffer. The default is 8KB.
  - **tcpwindowsize**

    Specifies the size, in kilobytes, for the TCP sliding window for your ADSM client. The default is 16KB.
- **commmethod snalu6.2**

  You can specify the additional APPC parameters in the **dsm.sys** file or you can specify a single parameter in **dsm.sys** that identifies an APPC side information profile where these additional APPC parameters are defined. The definition of the APPC side information profile can be found in 3.4.2.6, “Define the APPC Side Information Profile” on page 73. In either case you can also optionally include the buffer size parameter.

  Thus, if you specify all of the APPC parameters in the **dsm.sys** file, you use the following:
  - **tpname**

    Specifies the transaction program name for the ADSM server.
  - **partnerluname**

    Specifies a logical unit name used to identify the ADSM server.
  - **cpicmodename**

    Specifies the mode name or mode table name for CPIC, which is used in the SNA connection to the gateway and the ADSM server’s logical unit.
  - **cpicbuffersize**

    Specifies the CPIC buffer size that is used to transfer data between the client node and the server. The default is 15KB.

  If you use only a single parameter in the **dsm.sys** file that points to a side information profile, you use the following:
  - **symbolicdestinationname**

    Specifies a symbolic destination name for the ADSM server to which you want to connect. This name is also used as the name of the side information profile.

– **cpicbuffersize**

  Specifies the CPIC buffer size that is used to transfer data between the client node and the server. The default is 15KB.

3.2.1.2 Authorization Options

You need to configure the following authorization options to identify which users can access a particular ADSM server and to define how you want ADSM to handle passwords:

- **groups**

  Lists the groups using the AIX system that are authorized to request ADSM services. If you do not specify this option, all groups using the AIX system can access ADSM services.

- **users**

  Lists the users on the AIX system that you want to authorize to request ADSM services. If you do not specify this option, all AIX users can request ADSM services.

- **passwordaccess**

  Sets how ADSM handles passwords. An ADSM password is required for your workstation only when your administrator enables the ADSM authentication feature. Once authentication is enabled, you can set the **passwordaccess** option to either **prompt** or **generate**. Choose **prompt** when you want ADSM to prompt users for their ADSM password each time they request ADSM services. Choose **generate** when you want ADSM to store the ADSM password locally and generate a new password when the old one expires. The default is **prompt**.

- **mailprog**

  Specifies the program and userid to which you want ADSM to send the newly generated password when the old password expires. You use this option if you specified **generate** for the **passwordaccess** option.

3.2.1.3 Backup and Archive Options

Use the following options to control aspects of the backup and archive services:

- **changingretries**

  Specifies how many times you want ADSM to attempt to backup or archive a file that is currently in use. The default is four retries. This option is needed only when the serialization in the management class is shared static or shared dynamic.

- **compression**

  Specifies whether to compress files before sending them to the ADSM server. This option does not work if the ADSM administrator specifies the **never** option in the ADSM server.

- **virtualmountpoint**

  Defines a virtual mount point for a file system where ADSM can have a direct path to the files you want to back up.

- **inclexcl**

  Specifies the name of your include/exclude file if you choose to use one. Enter the **include** and **exclude** statements in this file to include or exclude files from ADSM backup and archive services and to assign a particular management class to files or group of files.

- **dirmc**

  Specifies a management class for directories if the default management class does not meet your requirements.

3.2.1.4 Scheduling Options

ADSM uses scheduling options only when the **dsmc schedule** command is running. You can use the following scheduling options:

- **maxcmdretries**

  Specifies the maximum number of times you want the client scheduler to attempt to process a scheduled command that fails. This option can be overridden by an ADSM server setting.

- **schedlogname**

  Specifies the path and file name where you want ADSM to log schedule information.

- **schedmode**

  Selects a schedule mode for scheduled work. Two modes are available in the ADSM server, **polling** and **prompted**. Use **polling** to have your ADSM client query the server for scheduled work at time intervals set by the **queryschedperiod** option. Use **prompted** to wait for the server to contact your client when scheduled work needs to be done. Note that **prompted** mode is only supported in the TCP/IP environment.

  If **schedmode** is **prompted**, you can also supply values for the following options:

  – **tcpclientaddress**

    Specifies a TCP/IP address if the client node has more than one address and you want the server to contact an address different from the address used to make initial contact with the server.

  – **tcpclientport**

    Specifies a TCP/IP port number if you want the server to contact a port different from the port used to make initial contact with the server.

  – **queryschedperiod**

    Specifies the number of hours you want the client scheduler to wait between attempts to contact the server for scheduled work. The default is 12 hours. It can be overridden by an ADSM server setting.

- **retryperiod**

  Specifies the number of minutes you want the client scheduler to wait between attempts to process a schedule command that fails or between unsuccessful attempts to report results to the server. The default is 20 minutes.

3.2.2 Updating the Client User Options File

You use the **dsm.opt** file to specify which ADSM server to contact for services and to control processing of sessions with the ADSM server. You can use a default user options file set up by the AIX server administrator, or you can choose to create your own. The **DSM_CONFIG** environment variable can be set to indicate where your client user options file is located.

You can override the options in the **dsm.opt** file, except for the **domain** option, by adding the option to the appropriate **dsmc** command. The **domain** option adds to what is specified in the client user options file instead of overriding it.

The client user options file can be divided into four basic groups of options.

3.2.2.1 Server and Node Options

You can use the following options to specify which server to contact for services and the client node for which you want to request services:

- **servername**

  Specifies which server you want to contact for services if more than one ADSM server is specified in the client system options file.

- **nodename**

  Specifies a node so you can restore, retrieve, or delete backup and archive data on a node other than the node on which you are currently working.

  Note: When you use the **nodename** option, ADSM prompts you for the ADSM password assigned to the node even if **passwordaccess** is **generate**. If you enter the correct password, you have read access to all backup and archive data on the ADSM server for the specified node. This may be an unacceptable security arrangement.

3.2.2.2 Date, Time, and Number Format and Language Options

You can use the following options to set the formats that ADSM uses to display date, time, numbers, and the language in which messages are displayed:

- **dateformat**

  Specifies the date format you want ADSM to display. The default is MM/DD/YYYY.

- **timeformat**

  Specifies the time format you want to use. The default is 00:00:00.

- **numberformat**

  Specifies the number format you want to use. The default is 1,000.00.

- **language**

  Specifies the language used for presenting ADSM messages. Currently, only American English is supported.

3.2.2.3 Command Processing Options

You can use these options to specify whether you want to display the processing information on your screen and, if so, how you want ADSM to display lists of information:

- **quiet**

  Specifies that there is no processing information to be displayed on the screen.

- **verbose**

  Specifies that you want processing information to display on the screen.

- **scrolllines**

  Specifies the number of lines that can appear at one time when ADSM displays a list of information on the screen. The default number is 20. This option is used in conjunction with VERBOSE.

- **scrollprompt**

  Specifies whether you want ADSM to stop after displaying the number of lines you specify with **scrolllines** and wait for you to scroll to the next group of lines or to scroll through all lines and stop at the end of the list. The default is to stop at the end of the list.

3.2.2.4 Backup, Restore, Archive, and Retrieve Options

You can use the following options to tailor backup processing and to determine whether you use the GUI or CLI.

- **domain**

  Specifies the default client domain. A client domain is the group of file systems for which you want ADSM to provide incremental backup services. If you do not specify this option, the default domain is all locally mounted file systems except **/tmp**.

  You can use the **domain** option with the **dsmc incremental** command to add file systems to the default client domain. You can also use the **filesystem** parameter of the **dsmc incremental** command to override your default client domain.

- **replace**

  Specifies whether you want ADSM to overwrite an existing file when you issue a **dsmc restore** or **dsmc retrieve** command. The default is for ADSM to prompt you for your choice.

- **subdir**

  Specifies whether you want ADSM to process files in all subdirectories of a directory when you issue a **dsmc selective**, **dsmc restore**, **dsmc archive**, **dsmc retrieve**, or **query backup** command. The directories themselves are backed up and restored, but they are not processed by archive at this time. The default is not to process subdirectories. Note that incremental backup always processes subdirectories.

Note: The **subdir** support for archive and retrieve was added to ADSM release 2 by PTFs, but the support is not yet included in the ADSM documentation.

- **tapeprompt**

  Specifies whether you want ADSM to wait for a tape to be mounted when required to back up, restore, archive, or retrieve a file or prompt you for your choice. This option does not apply to scheduled backups. The default is for ADSM to prompt you for your choice.

  Note: The **tapeprompt** support for backup and archive was added to ADSM release 2 by PTFs, but the support is not yet included in the ADSM documentation.

3.3 TCP/IP Connectivity

TCP/IP is the most common ADSM connectivity method. The ADSM AIX client supports TCP/IP connectivity from any supported AIX system to any ADSM server.

3.3.1 System Requirements

The implementation of TCP/IP on an AIX system is easy. TCP/IP is provided as part of the AIX operating system, so no additional products are required; TCP/IP just needs to be configured.

The requirements for the ADSM server vary and depend on the server platform:

- ADSM/6000 for AIX

  TCP/IP is included as part of the base AIX operating system.

- ADSM/2 for OS/2

  Use TCP/IP for OS/2 version 1.2 or later.

- ADSM Release 1 for MVS

  Use TCP/IP for MVS version 2.2 or later.

- ADSM Release 1 for VM

  Use TCP/IP for VM version 2.2 or later.

Note: There are alternative TCP/IP products for MVS and VM. These do not currently work with ADSM. ADSM on MVS and VM uses IUCV as the underlying communications method between TCP/IP and the ADSM server. Only those TCP/IP products on MVS and VM that support IUCV will work with ADSM.

3.3.2 Configuration

Configuration of TCP/IP consists of two tasks: configuring AIX to use TCP/IP and updating the ADSM AIX client user options file to use TCP/IP for its communication with the server.

3.3.2.1 Configuring TCP/IP

Configuration of TCP/IP is accomplished through the SMIT facility with the following steps:

1. Enter **smit tcpip** on the command line.

   You now see the TCP/IP panel shown in Figure 19 (background window).

2. Move the cursor to **Minimum Configuration & Startup**.

3. Press Enter.

   You now see the **Available Network Interfaces** subpanel shown in Figure 19.

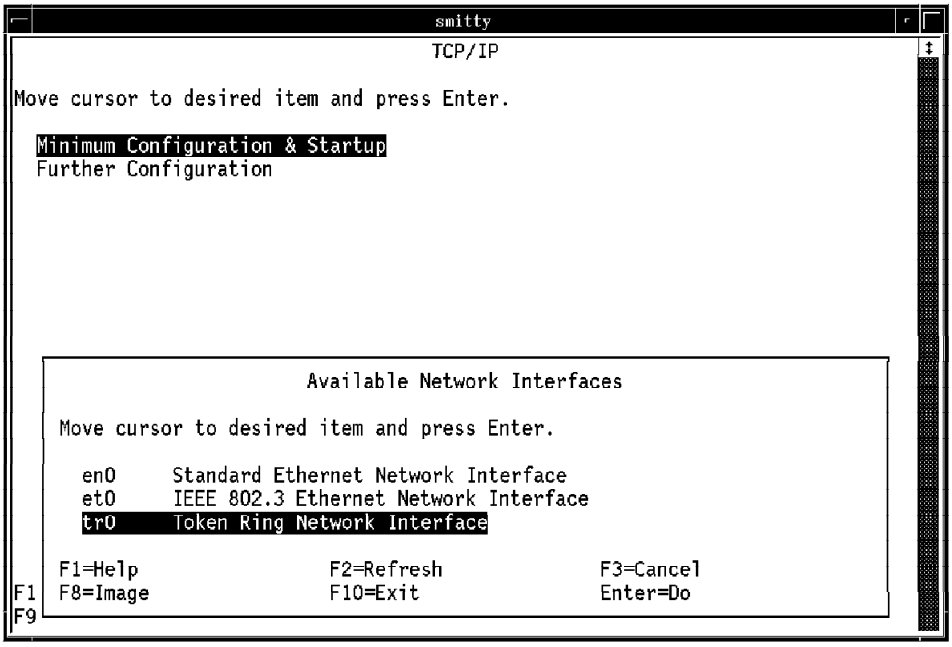


Figure 19. TCP/IP Configuration: Available Network Interfaces

4. Move the cursor to **tr0 Token Ring Network Interface**.

5. Press Enter.

   You now see the **Minimum Configuration & Startup** panel shown in Figure 20 on page 48.

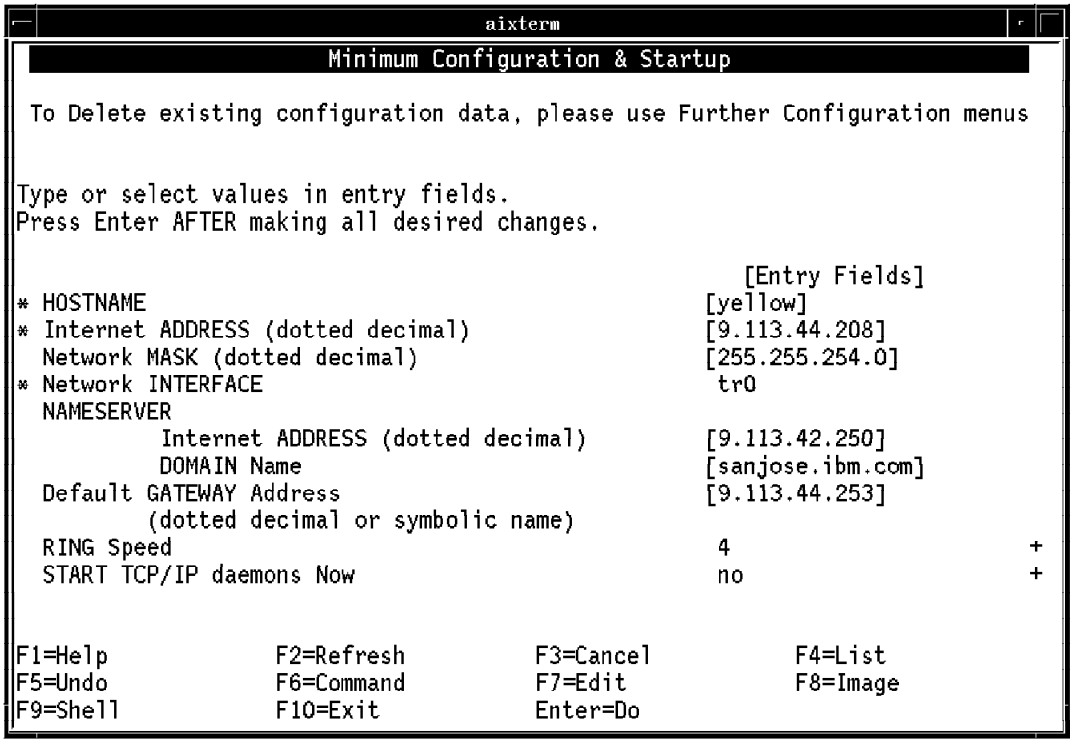


Figure 20. TCP/IP Configuration: Minimum Configuration & Startup

6. Ask your network administrator for detailed information to complete this panel.
7. Enter the following network definitions to complete your TCP/IP configuration:

   HOSTNAME your local TCP/IP host name for the AIX system. The ADSM server refers to this parameter as the ADSM client's **nodename**.

   Internet ADDRESS your TCP/IP address. You must have a unique address in the network environment. It must be in dotted decimal format, such as 9.113.44.208.

   Network MASK the network mask used by your configuration. Again it must be in dotted decimal format.

   NAMESERVER if your configuration uses a name server to resolve network addresses, you need to include the following:

   - **Internet ADDRESS** the Internet address for the name server in dotted decimal format.
   - **DOMAIN Name** the domain name from the name server.

   Default GATEWAY Address the address of the gateway, if used in your configuration, in dotted decimal format.

   RING Speed 4 or 16

   START Now yes.

3.3.2.2 Updating the Client User Options File (DSM.OPT)

The second stage of configuring ADSM is to update the **dsm.sys** file to reflect the fact that TCP/IP is being used. At a minimum you should add the following entries:

```
commmethod          tcpip
tcpport             1500
tcpserveraddress    9.113.44.100
    OR
commmethod          tcpip
tcpport             1500
tcpserveraddress    blue.sanjose.ibm.com
```

The **tcpserveraddress** is the address of the ADSM server. You get this address from your network administrator who is responsible for TCP/IP on the ADSM server. The first group of statements shown above uses the actual Internet dotted decimal address (9.113.44.100). The second group uses an address scheme that makes use of a name server (blue.sanjose.ibm.com).

3.3.3 Problem Determination

Problem determination of TCP/IP connectivity failures can be difficult if complex network configurations are involved. Most TCP/IP implementations provide an application called packet inter-network groper (PING). PING is a simple echo test where a packet is sent to a specified Internet address and the response is displayed. PING is very useful for problem determination purposes if it is unclear whether a connection has been established.

AIX provides a PING facility. After you have finished the TCP/IP configuration, we recommend that you test the connection with the PING facility as shown in Figure 21 on page 50. If you have **0% packet loss** with every command, your network connection is successful.

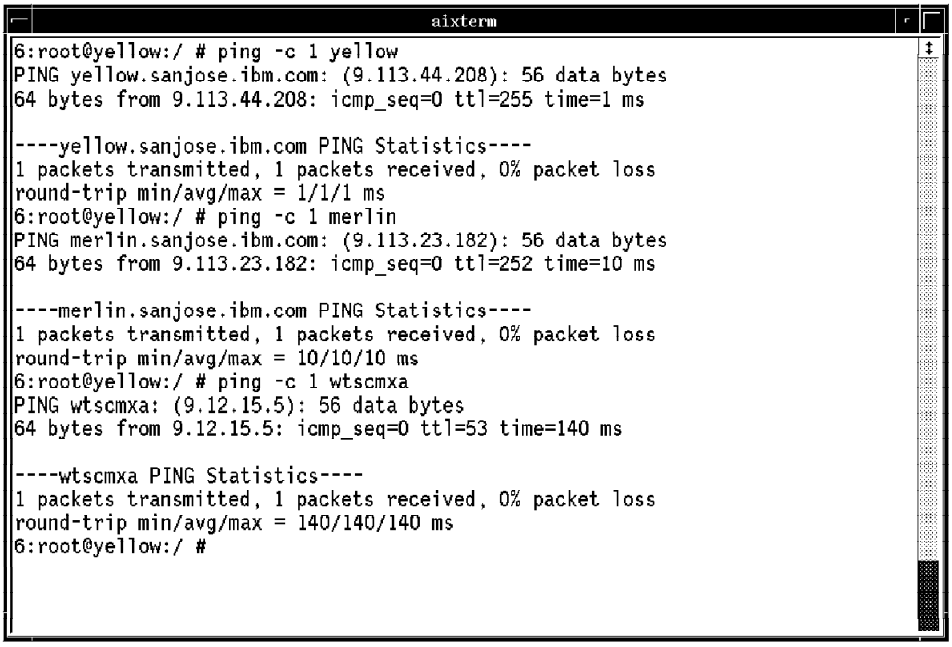


Figure 21. PING Example

3.3.4 Performance Considerations

It is beyond the scope of this document to provide comprehensive tuning guidance for TCP/IP. However there two ADSM performance options for TCP/IP, **tcpwindowsize** and **tcpbuffsize**.

TCP/IP is a connection-oriented protocol where every packet that is sent must be acknowledged before the next one is sent. The sliding window enables multiple packets to be sent without waiting for acknowledgments. Figure 22 on page 51 Illustrates how a sliding window operates.

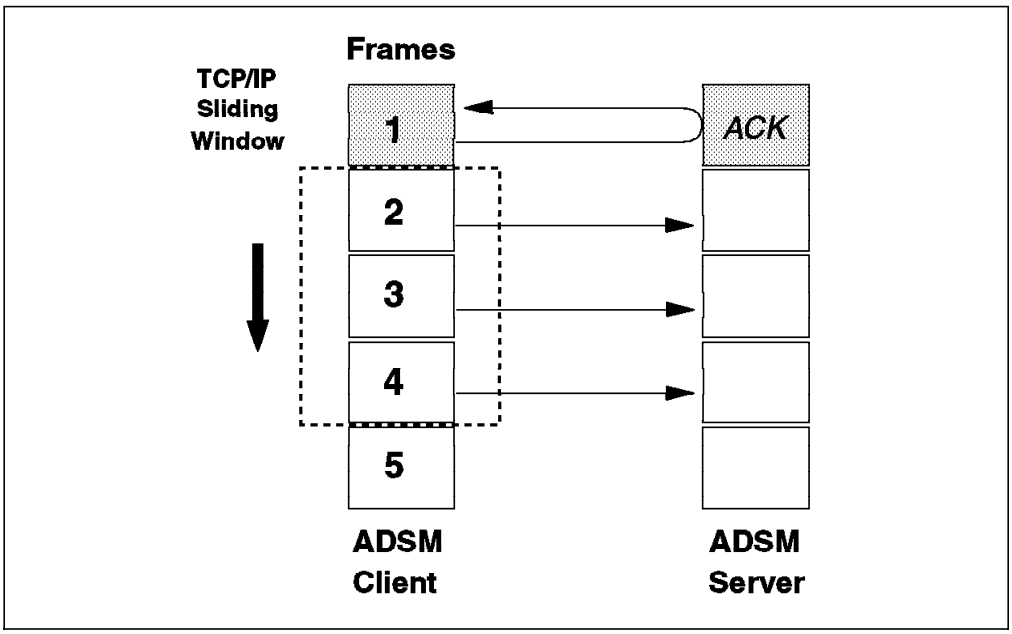


Figure 22. TCP/IP Sliding Window

The size of the sliding window is the amount of data that can be sent without waiting for an acknowledgment. When that amount of data has been sent, TCP/IP waits for the acknowledgments to start arriving. As they arrive, it slides the window down the frames waiting to be transmitted.

In Figure 22 the sliding window is large enough to contain three frames. The first three frames have been transmitted, and an acknowledgment has been received for the first frame. The window has now moved forward and frame 4 has been sent. As the acknowledgments arrive, the window moves down the frames, potentially sending multiple frames simultaneously.

In networks where long transmission delays occur, a large sliding window can improve performance. With ADSM the sliding window size, in kilobytes, is defined in the **dsm.sys** file:

```
tcpwindowsize    24
```

The default is 16KB. Increasing the size to between 16KB and 24KB is recommended.

The TCP/IP buffer size also affects performance. This parameter determines the size of the internal TCP/IP communications buffers to be used. The buffer size is defined in the **dsm.sys** file:

```
tcpbuffsize     16
```

The default is 8KB. Increasing the size to between 16KB and 32KB can improve performance, but the buffer size has less effect on performance than the sliding window size.

Although both the sliding window size and buffer sizes can improve performance, they increase the use of memory on the AIX system, which could cause other problems. A balance must be achieved between the use of AIX system memory and communications performance.

The above general recommendations affect the TCP/IP performance of the AIX client only. There are many other areas where tuning may be required: LAN gateways, routers, and the ADSM server. Recommendations for all of these areas are beyond the scope of this document. For further information refer to *ADSTAR Distributed Storage Manager Performance Tuning Guide*.

3.4 APPC (LU6.2) Connectivity

In this section we cover the APPC setup for ADSM AIX clients. This is a subject that causes considerable confusion and misunderstanding. Part of the problem has to do with the terminology, which we explain below.

At its simplest level APPC is a conversation between two programs. These programs could be applications running on the same system or on remote systems connected by a network. In SNA terms the applications are defined as logical units (LUs). An LU is a port that can be addressed to access an application or device such as a screen or printer. APPC implements LU type 6.2.

There are two basic types of LUs: dependent and independent. Dependent LUs rely on a host system to establish and manage sessions between the LU and the application to which it is connecting. A system service control point (SSCP) manages these sessions. The SSCP is VTAM*.

Independent LUs are just that; they can talk to each other without an SSCP establishing and managing the conversation. An independent LU can activate a session with another independent LU directly. This process is called binding.

The only independent LUs are LU type 6.2s. They can bind a session with another LU type 6.2 without assistance from VTAM. There are, in fact, two types of LU type 6.2s, dependent and independent. Dependent LU type 6.2s enable APPC conversations, but only under the control of VTAM.

ADSM implements independent LU type 6.2s. Thus it can do any-to-any APPC connectivity between any of the ADSM server and client platforms that support APPC. In the sections that follow we concentrate on APPC connectivity to MVS.

To implement APPC connectivity for the ADSM AIX client a number of pieces of information are required. Some will already be available, some will have to be defined. Figure 23 on page 53 illustrates some of the required parameters.

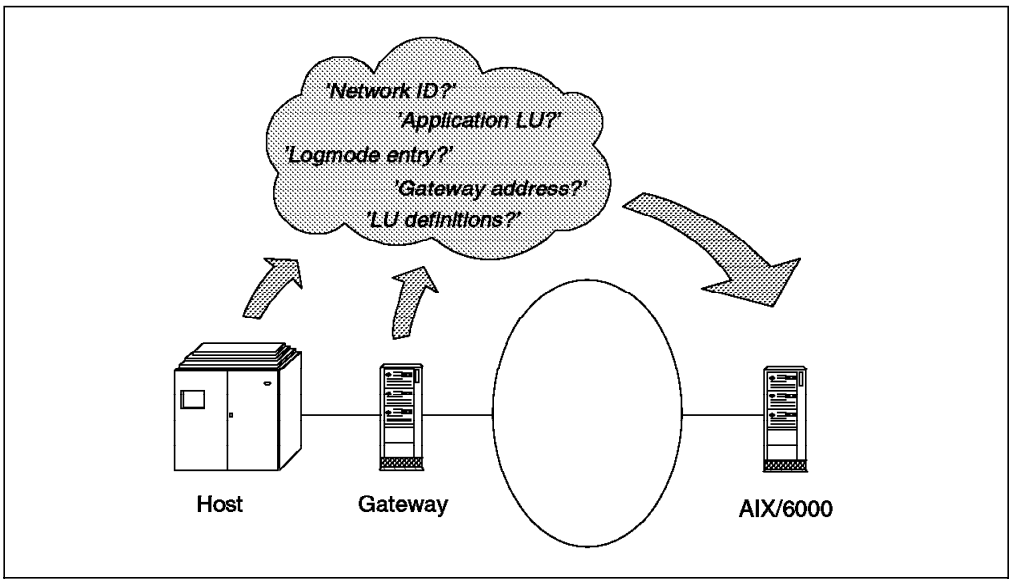


Figure 23. APPC Configuration Parameters

The following definitions are required:

- VTAM network ID

  This ID defines the VTAM network name that will be required when SNA Server/6000 is configured. The **NETID=** parameter in the VTAM ATSTRxx start list defines the network name.

- ADSM server VTAM application major node

  All resources that access VTAM must be defined. These resources include applications that communicate with other applications or terminals. Applications are defined to VTAM in a VTAM application major node definition.

  This definition defines the characteristics of the application, such as whether APPC is used, whether parallel sessions are enabled, and which logmode is to be used. Applications are defined with an LU name in the application major node definition. The ADSM server will have an LU defined, which is the partner LU that will need to be defined in SNA Server/6000.

- Name of the VTAM logmode table and entry for ADSM

  Part of the application major node definition for ADSM is the logmode that will be used. A logmode is a set of parameters that govern the conversations between application LUs and other LUs. It contains parameters that determine the type of LU that can be used, network priorities, and maximum frame sizes.

  The logmode that the ADSM server uses must match the logmode that is defined by the related LU, such as SNA Server/6000. This exchange of logmode information when establishing a session is part of the bind. If there are incompatibilities in the logmodes, the bind will fail. This is one of the most common problems encountered when setting up APPC.

  Logmodes are defined in tables that contain a number of entries. The ADSM server application major node defines a logmode table and the logmode entry within it to use. SNA Server/6000 must specify the same logmode entry name as that used by the ADSM server.

- VTAM PU/LU definitions for the AIX machine

The AIX server running SNA Server/6000 must be defined to VTAM. Typically, it will be defined as a physical unit (PU). The PU defines how VTAM accesses the system and controls the flow of data. Associated with the PU definitions are one or more LU definitions. These define the sessions that will be used with the PU.

Multiple LUs can be defined for a PU. For ADSM the PU must have an independent LU type 6.2 defined. This independent LU type 6.2 is defined by adding a LOCADDR=0 statement to the LU. Adding this statement to an LU automatically makes the PU a type 2.1 PU. A PU type 2.1 supports dependent and independent LUs. A PU type 2.0 supports only dependent LUs and cannot be used for ADSM.

- Address of host communications gateway

  The physical address of the communications gateway that will be used to access the VTAM network must be defined. This address is typically the token-ring address of a 3745, 3174, or other gateway.

A sample set of VTAM definitions can be found in Appendix B, “Sample ADSM MVS Server APPC Definitions” on page 115. These definitions are used in the sections that follow.

3.4.1 System Requirements

The APPC connectivity requirements for ADSM are quite simple. An ADSM system uses independent LU type 6.2 for communication between ADSM servers and clients. How that level of support is provided is not so simple. You need to consider three basic components when deciding how to implement APPC connectivity:

- Communications gateway
- Host software
- Workstation software.

The choice of connectivity protocol for ADSM is typically determined by the desire to utilize existing networks and investments in hardware and software. For that reason ADSM clients on AIX servers, utilizing APPC, will typically be connected to ADSM MVS servers. Figure 24 on page 55 illustrates the basic connectivity options for ADSM AIX clients connecting with APPC to an ADSM MVS server.

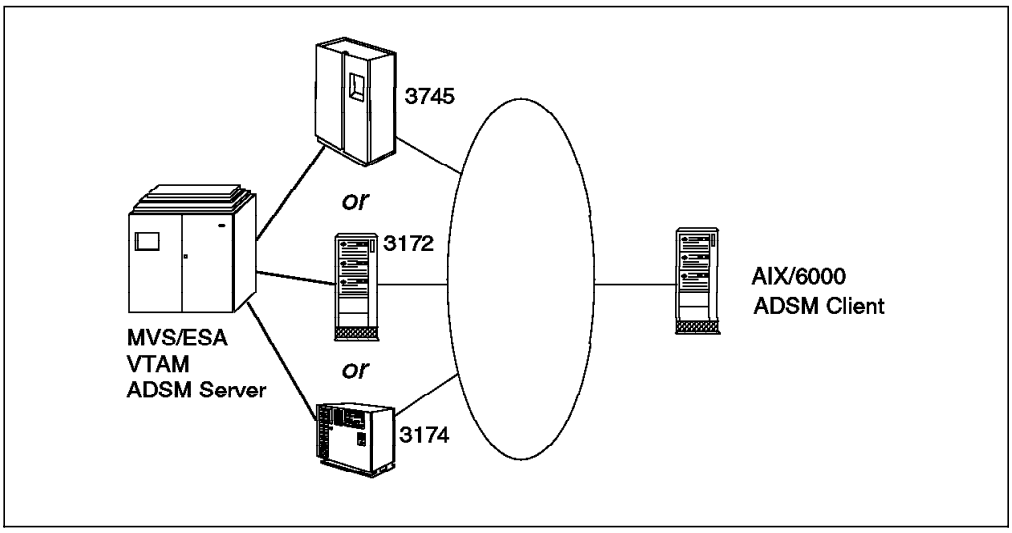


Figure 24. ADSM APPC Options for ADSM AIX Client and MVS Server

In an ADSM environment there are many different ways of providing the required APPC connectivity. The primary requirement is for PU type 2.1 support in all components of the network. Without this support, APPC does not work. Independent LU type 6.2 can be defined only with PU type 2.1 support.

In an MVS environment PU type 2.1 support is provided as a combination of communications gateway software and VTAM levels. Let us look at the PU type 2.1 support prerequisites for the possible communications gateways in turn:

- 3745 communication controllers

  NCP version 5 release 2 and VTAM version 3 release 2 (VTAM/XA) or later are required.

- 3172 interconnect controllers

  Interconnect Controller Program version 2 and VTAM version 3 release 4 (VTAM/ESA) or later are required.

- 3174 workstation controllers

  3174 Licensed Internal Code, Configuration C release 1 (recommended) or 3174 Licensed Internal Code, Configuration B with RPQ #8Q0800, Type 2.1 Passthru Function, and VTAM version 3 release 4 (VTAM/ESA) or later are required.

3.4.2 Configuration

The APPC code is included in AIX SNA Server/6000, which is a separate product. AIX SNA Server/6000 has one control point profile, **node_cp**, which is used to identify the local node to the network. You have to complete the control point profile before you can start SNA and use APPC.

After defining the control point profile, you have to configure the communications environment available in your workstation. If the token-ring adapter is already configured for your workstation, the following profiles need to be tailored to define the PU:

- A token-ring SNA DLC profile

- A token-ring link station profile.

After you define the physical environment, you need to define your local LU type 6.2 profile. The parameters in this profile indicate that the LU address you use is an independent LU and provides other related PU information. You also have to create the partner LU and link to establish a connection with the partner LU.

If this is your first use of SNA on your AIX system, you need to add token-ring data link control to the system's communications adapter. To do this use SMIT and select the following menu items in sequence: **devices**, **communications**, **token ring adapter**, **services**, **data link control**, and **add a token ring data link control**.

The APPC profiles are defined using SMIT. You will need to be a root user to define and save these APPC profiles.

In the following sections we use reverse video, **X**, to cross reference APPC information that is entered in various places. You will see the same reverse video number in the text to indicate all parameters that should have the same value.

3.4.2.1 Define the Control Point Profile

First you define the APPC control point profile. This action defines the AIX client and associates it with the SNA control point, for example, VTAM in an MVS or VM environment.

To begin configuration of the APPC communication, you proceed with the following steps to define the control point profile:

1. Enter **smit sna** on the command line.

   You now see the panel shown in Figure 25 on page 57.

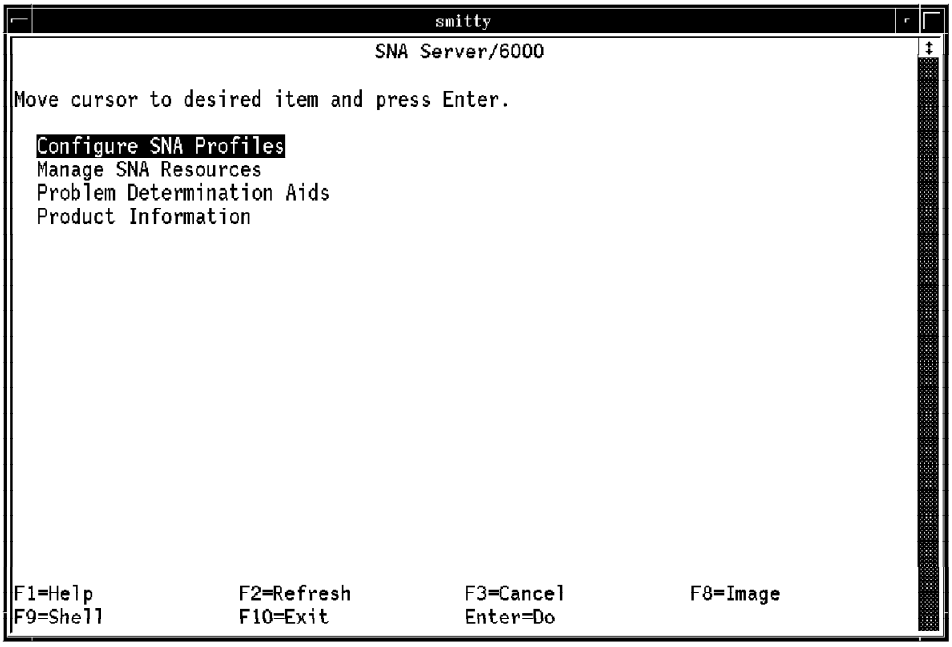


Figure 25. APPC Configuration: SNA Server/6000

2. Move the cursor to **Configure SNA Profiles**.
3. Press Enter.

   You now see the panel shown in Figure 26.

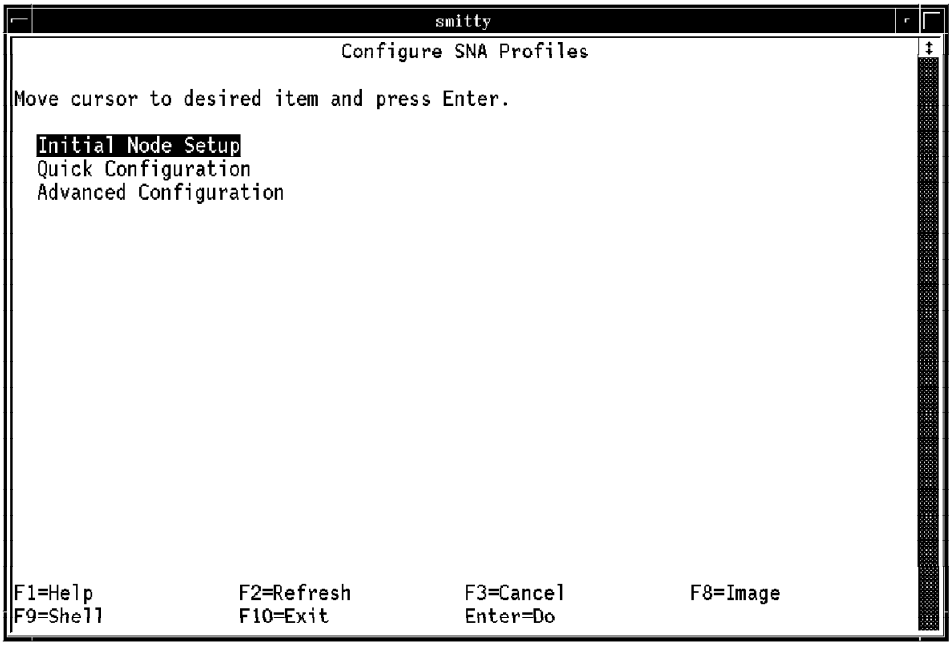


Figure 26. APPC Configuration: Configure SNA Profiles

4. Move the cursor to **Initial Node Setup**.
5. Press Enter.

   You now see the panel shown in Figure 27 on page 58.

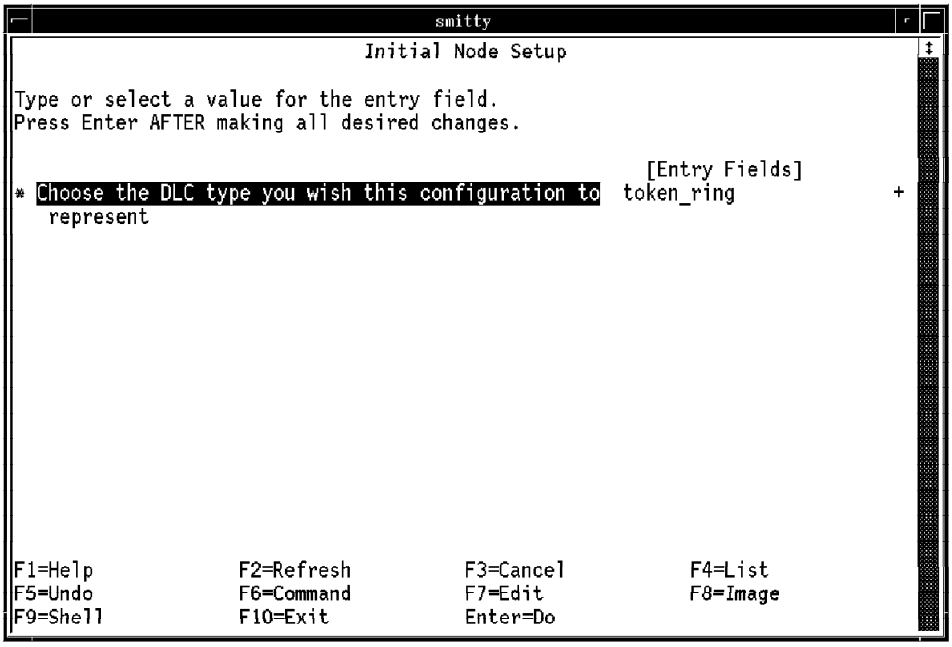


Figure 27. APPC Configuration: Initial Node Setup

6. Move the cursor to **Choose the DLC type you wish this configuration to represent**.
7. Press Enter.

   You now see the panel shown in Figure 28.

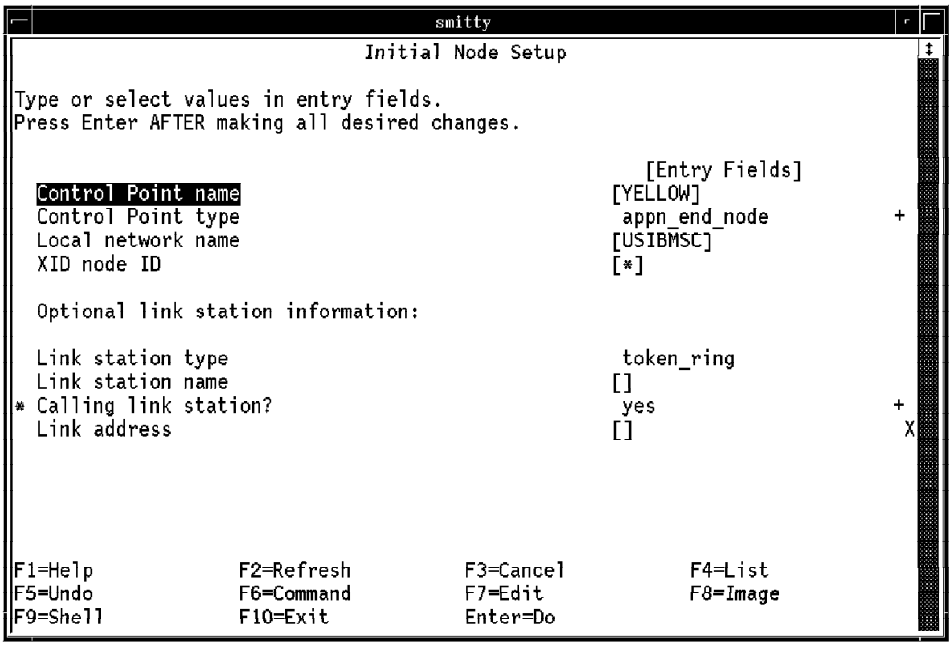


Figure 28. APPC Configuration: Initial Node Setup

8. Ask your network administrator for detailed information to complete this panel.
9. Enter the following network parameters to complete the definition of the control point profile:

Control Point name, 1 — your local APPC node name. This is the independent LU name for the ADSM client, and it must be defined in the ADSM server. For an MVS environment, it would be defined as an LU with **LOCADDR=0** in the **3745 VTAMLST**.

Control Point type — select **appn_end_node** for this field.

Local network name — ask your network administrator for the network name of the SNA network on which the AIX system is defined.

XID node ID — since the definition must be an independent LU type 6.2, you may not need a special XID node ID. If this definition is for a cross domain environment, you will need this parameter. Then enter the **IDBLK** and **IDNUM** defined in the **3745 VTAMLST** in a VTAM environment.

The other fields can be left with their defaults.

10. Press Enter.

You have finished defining the control point profile.

3.4.2.2 Define the Token-Ring SNA DLC Profile

To define the token-ring SNA DLC profile, you should continue from the **Initial Node Setup** panel as follows:

1. Press F3 twice.

   You now see the panel shown in Figure 26 on page 57.

2. Move the cursor to **Advanced Configuration**.
3. Press Enter.

   You now see the panel shown in Figure 29 on page 60.

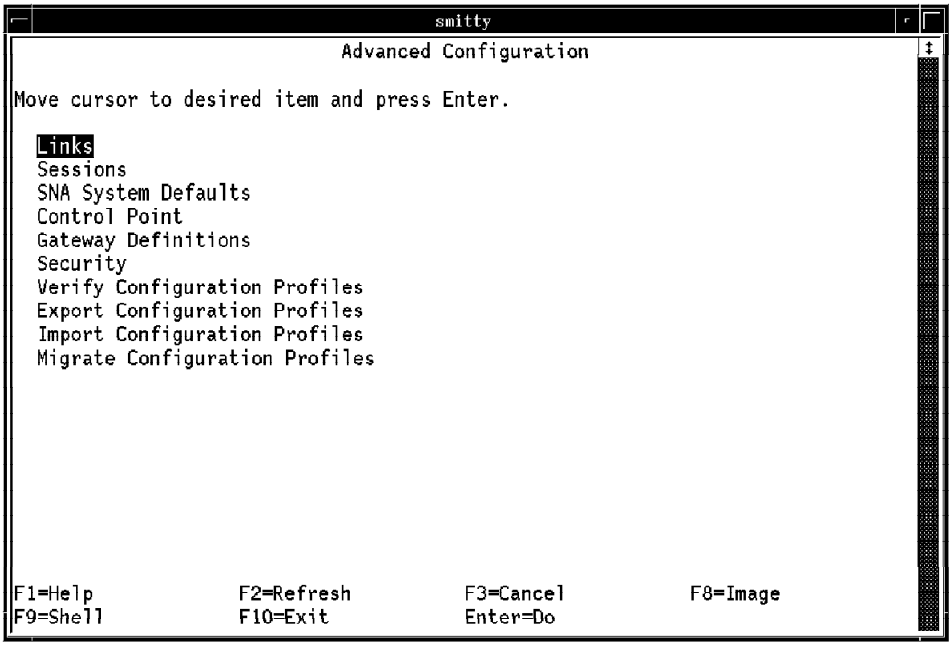


Figure 29. APPC Configuration: Advanced Configuration

4. Move the cursor to **Links**.
5. Press Enter.

   You now see the panel shown in Figure 30.

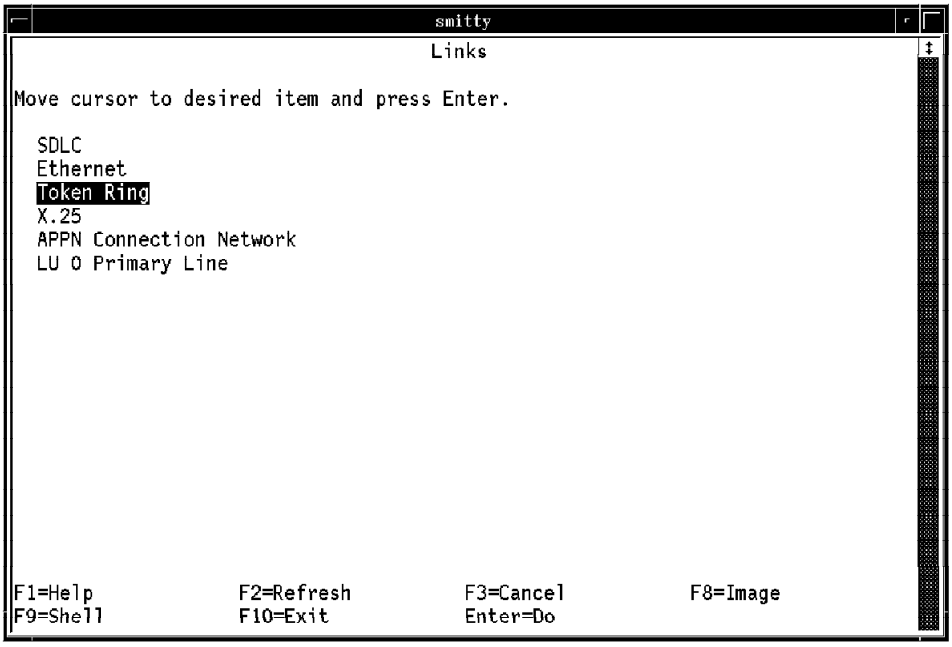


Figure 30. APPC Configuration: Links

6. Move the cursor to **Token Ring**.
7. Press Enter.

   You now see the panel shown in Figure 31 on page 61.

Figure 31. APPC Configuration: Token Ring Physical Units

8. Move the cursor to **Token Ring SNA DLC**.
9. Press Enter.

   You now see the panel shown in Figure 32.

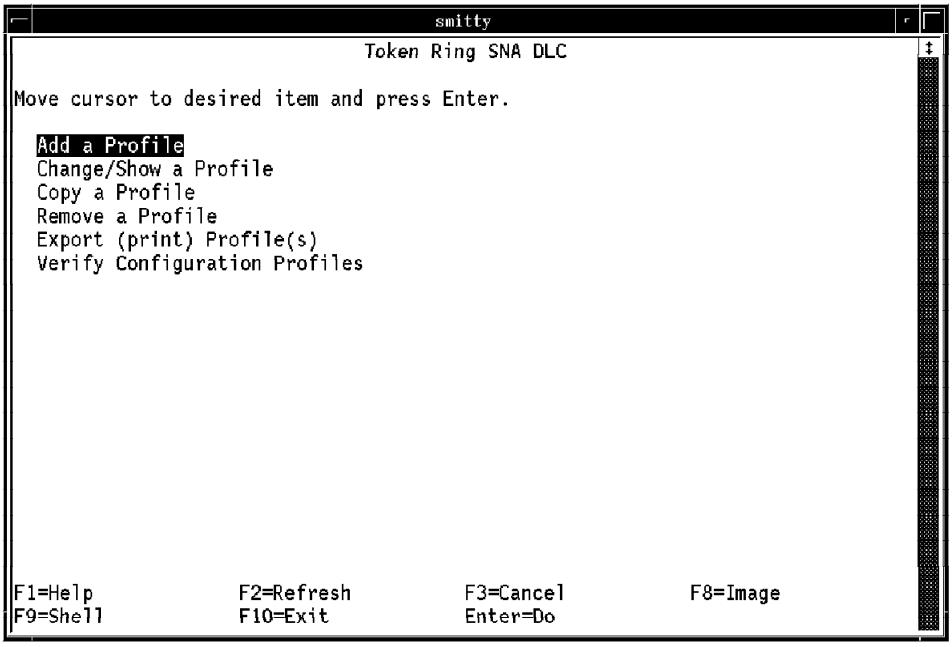


Figure 32. APPC Configuration: Token Ring SNA DLC

10. Move the cursor to **Add a Profile**.
11. Press Enter.

    You now see the panels shown in Figure 33 on page 62.

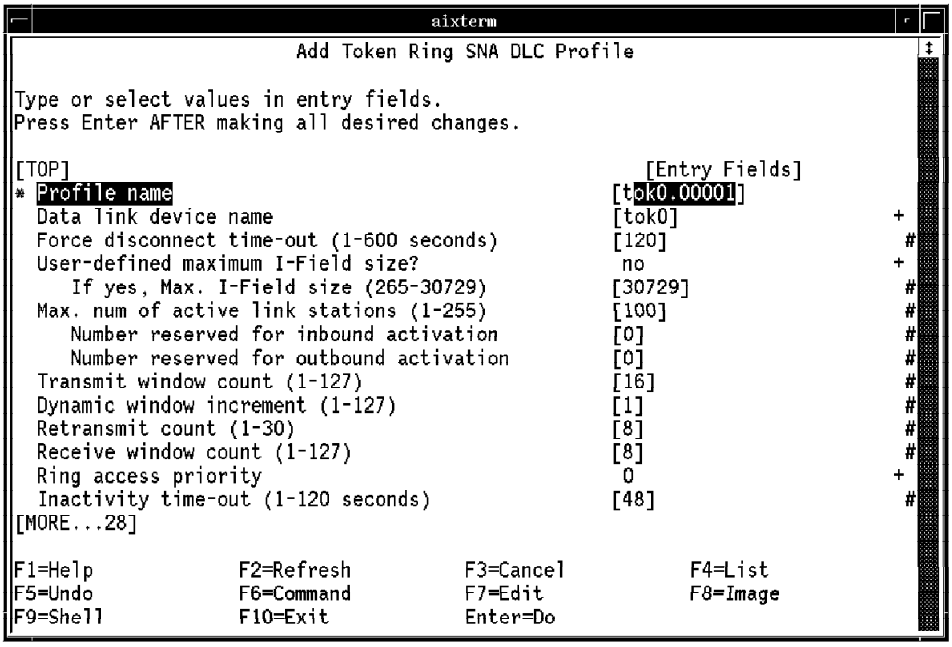


Figure 33 (Part 1 of 3). APPC Configuration: Add Token Ring SNA DLC Profile

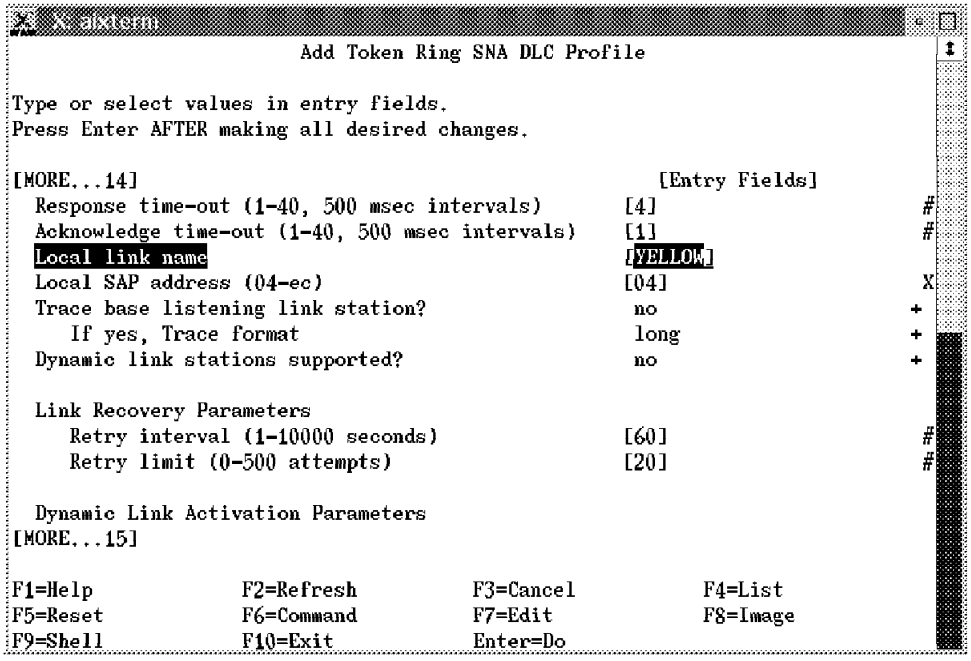


Figure 33 (Part 2 of 3). APPC Configuration: Add Token Ring SNA DLC Profile

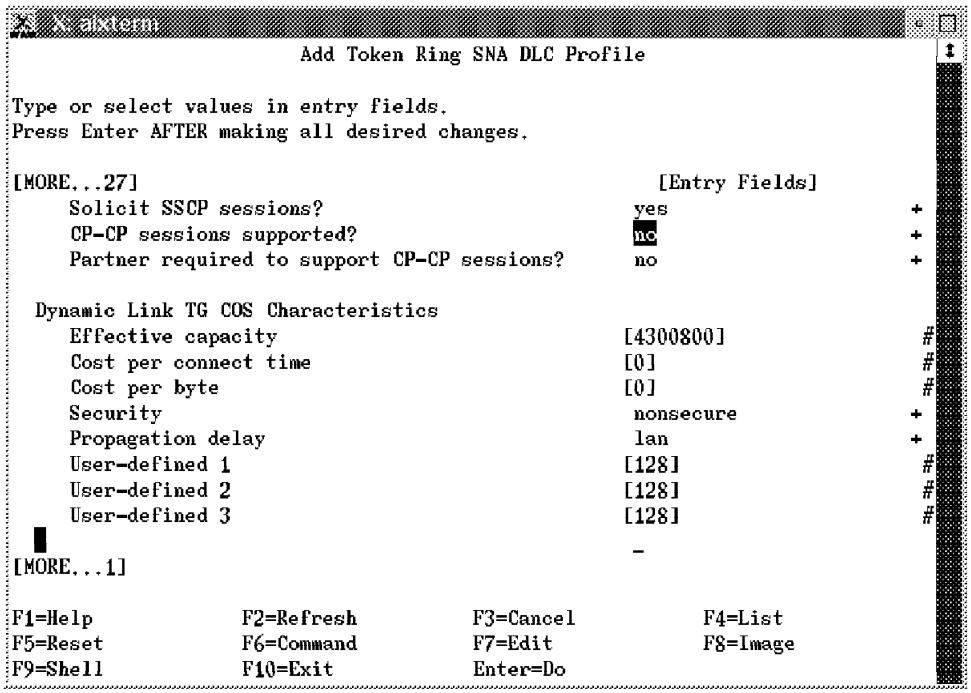


Figure 33 (Part 3 of 3). APPC Configuration: Add Token Ring SNA DLC Profile

12. Ask your network administrator for detailed information to complete these panels.
13. Enter the following network definitions to complete the definition of the token-ring SNA DLC profile:

    Profile name, 2 whatever name you want to use.

    Local link name, 1 your local APPC node name. This is the LU name for the ADSM client previously defined.

    Dynamic Link Activation Parameters Solicit SSCP sessions? yes

    Dynamic Link Activation Parameters CP-CP sessions supported? no

    The other fields can be left with their defaults.
14. Press Enter.

You have finished defining the token-ring SNA DLC profile.

3.4.2.3 Define the Token Ring Link Station Profile

You now need to define a token ring link station profile for each ADSM server that you plan to access. Continue from the **Add Token Ring SNA DLC Profile** panel as follows:

1. Press F3 three times.

   You now see the panel shown in Figure 34 on page 64.

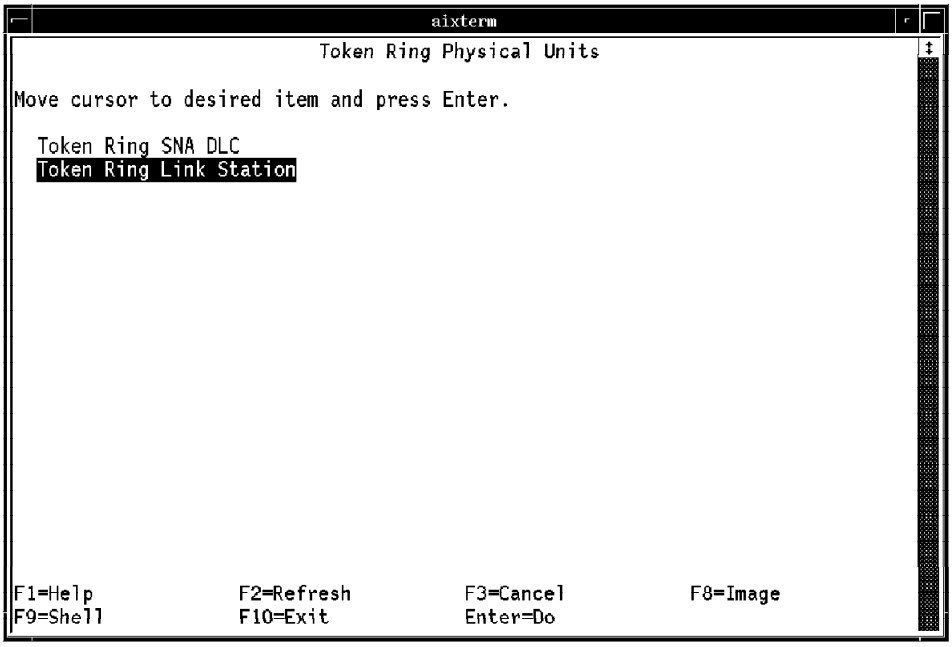


Figure 34. APPC Configuration: Token Ring Physical Units

2. Move the cursor to **Token Ring Link Station**.
3. Press Enter.

   You now see the panel shown in Figure 35.

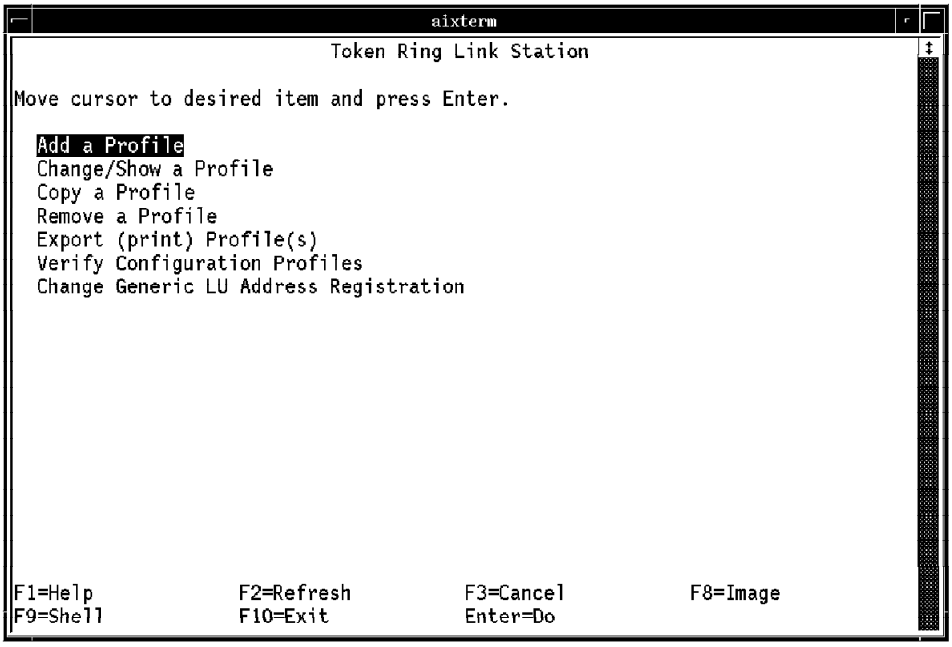


Figure 35. APPC Configuration: Token Ring Link Station

4. Move the cursor to **Add a Profile**.
5. Press Enter.

   You now see the panels shown in Figure 36 on page 65.

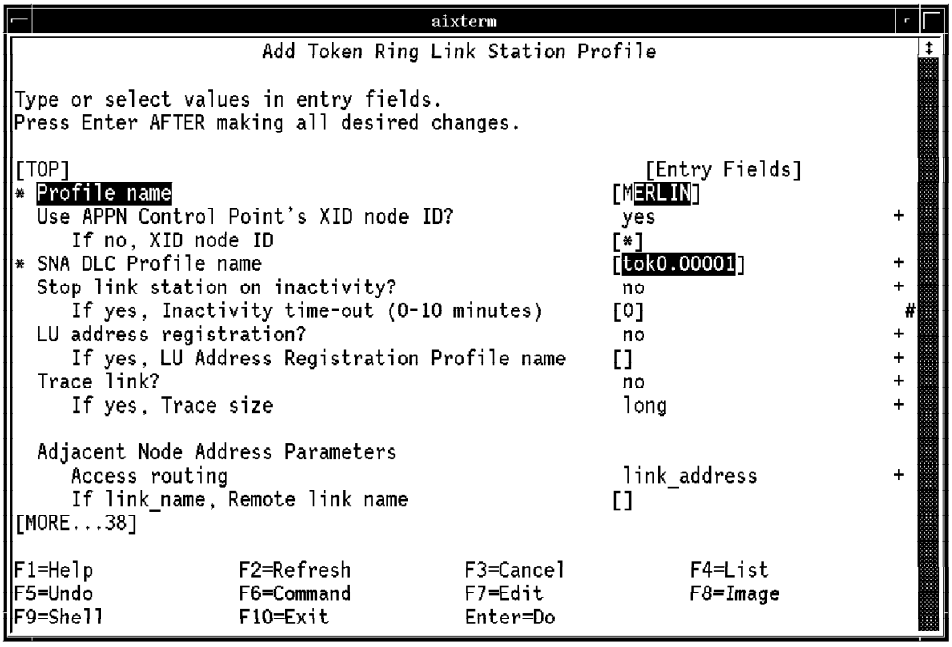


Figure 36 (Part 1 of 4). APPC Configuration: Add Token Ring Link Station Profile

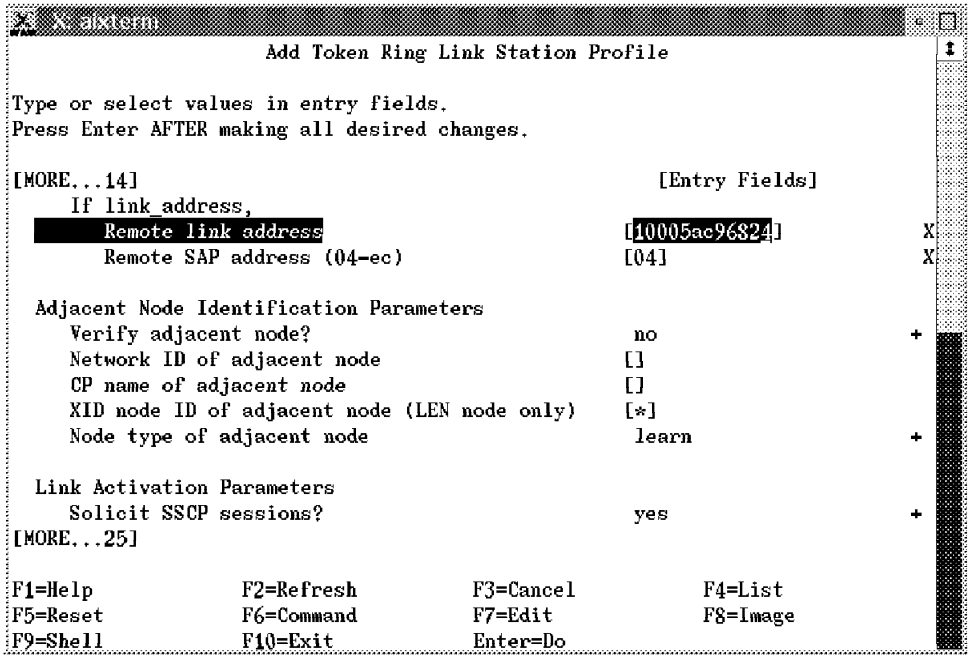


Figure 36 (Part 2 of 4). APPC Configuration: Add Token Ring Link Station Profile

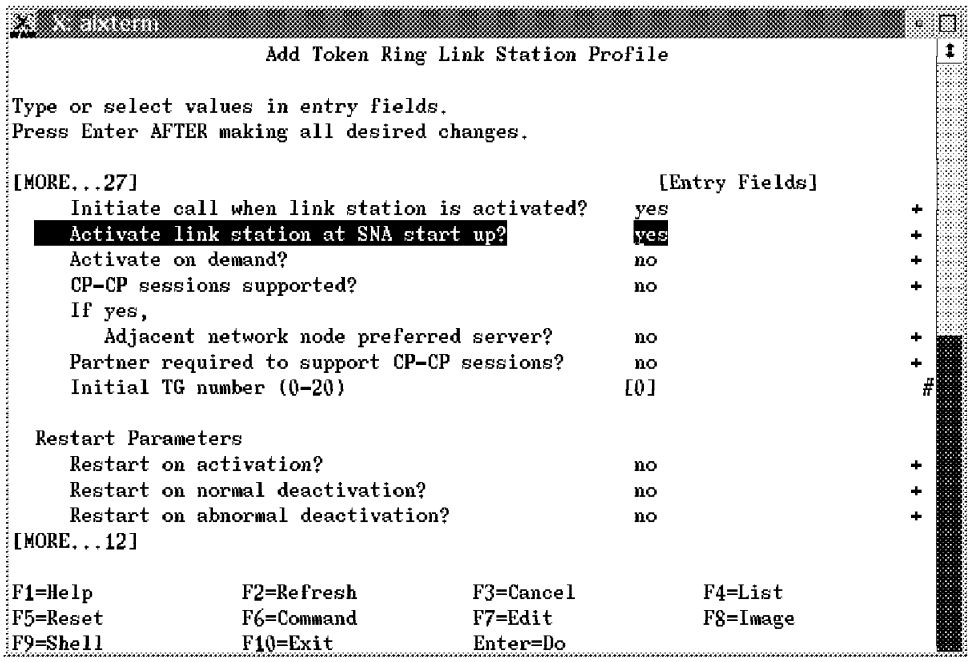


Figure 36 (Part 3 of 4). APPC Configuration: Add Token Ring Link Station Profile

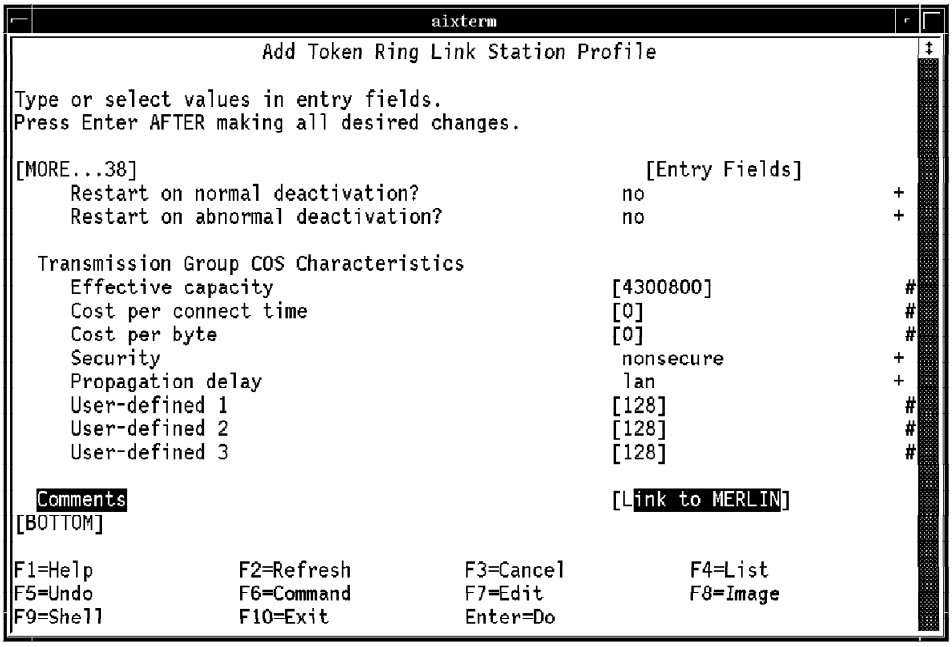


Figure 36 (Part 4 of 4). APPC Configuration: Add Token Ring Link Station Profile

6. Ask your network administrator for detailed information to complete these panels.
7. Enter the following network definitions to complete the definition of the token ring link station profile:

   Profile name, 3 this can be any name you like. You may want to associate it with the ADSM server's name.

   SNA DLC Profile name, 2 your defined token-ring SNA DLC profile.

Remote link address the link address of the APPC server. In an MVS environment this would be the token ring adapter address of the MVS 3745 or other gateway. Ask your network administrator for this information.

Solicit SSCP sessions? yes.

Initiate call when link station is activated? yes.

Activate link station at SNA start up? yes.

CP-CP sessions supported? no.

The other fields can be left with their defaults.

8. Press Enter.

You have finished defining the token ring link station profile.

3.4.2.4 Define the Partner APPC Profile

Now you need to define a partner LU type 6.2 profile for each ADSM server you plan to access. This is the definition of the ADSM server node. It must be coordinated with the definitions in the ADSM server.

Continue from the **Add Token Ring Link Station Profile** panel as follows:

1. Press F3 five times.

   You now see the panel shown in Figure 29 on page 60.

2. Move the cursor to **Sessions**.
3. Press Enter.

   You now see the panel shown in Figure 37.

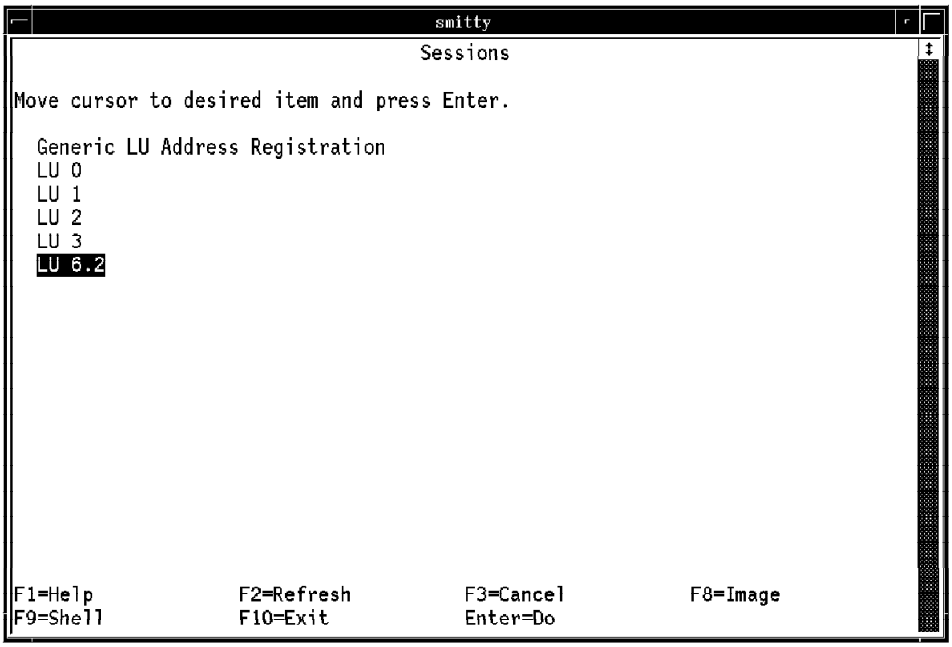


Figure 37. APPC Configuration: Sessions

4. Move the cursor to **LU 6.2**.

5. Press Enter.
6. Press F3 three times.

   You now see the panel shown in Figure 38.

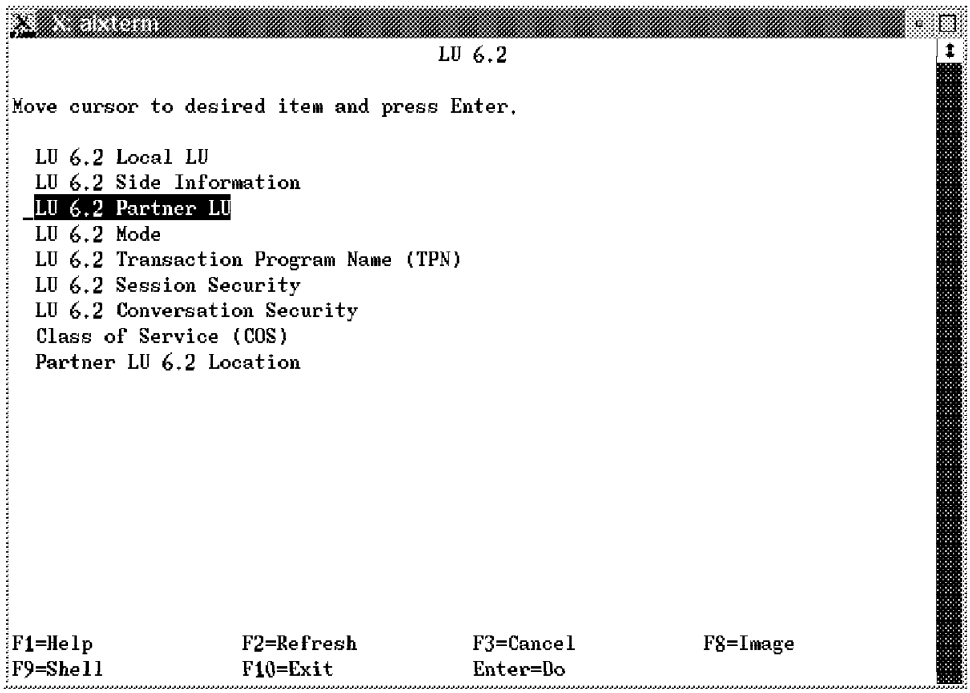


Figure 38. LU 6.2

7. Move the cursor to **LU 6.2 Partner LU**.
8. Press Enter.

   You now see the panel shown in Figure 39 on page 69.

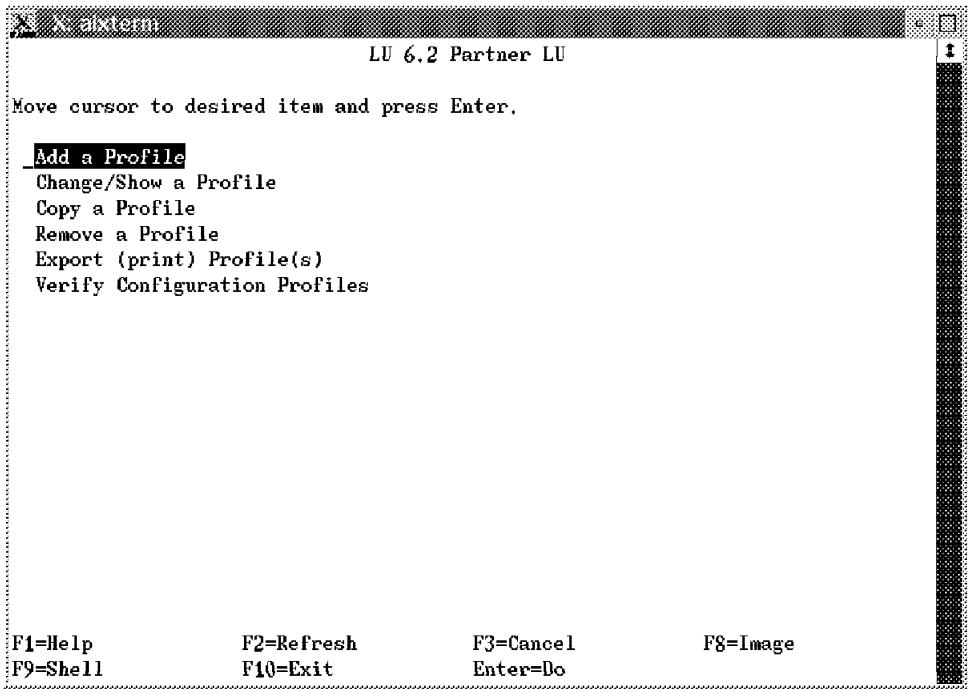


Figure 39. LU 6.2 Partner LU

9. Move the cursor to **Add a Profile**.
10. Press Enter.

    You now see the panel shown in Figure 40.

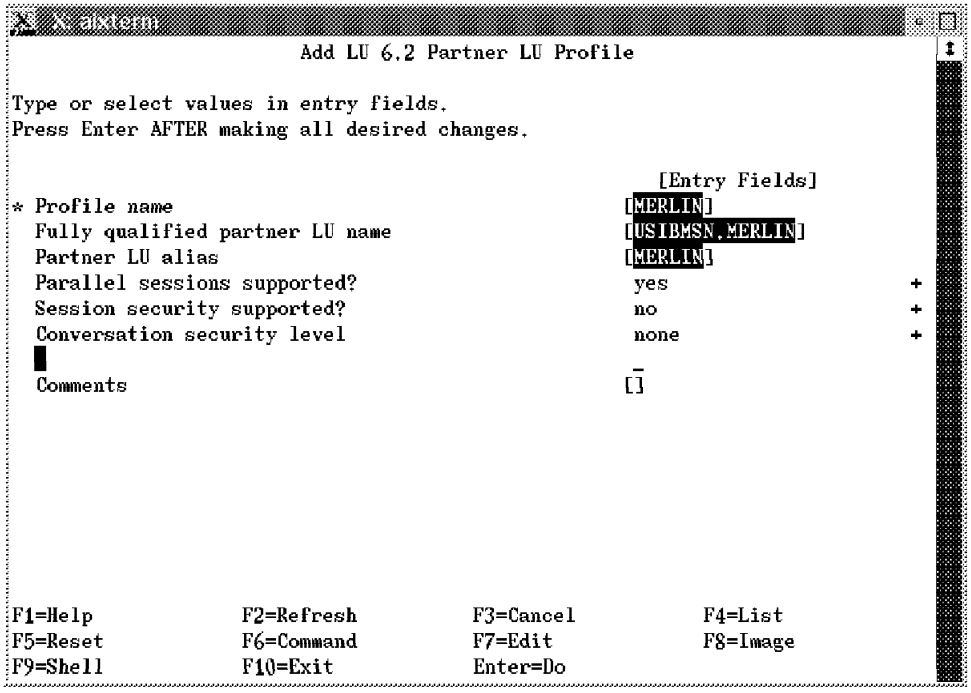


Figure 40. Add LU 6.2 Partner LU Profile

11. Ask your network administrator for detailed information to complete this panel.

12. Enter the following network definitions to complete the definition of the partner LU 6.2 profile:

    Profile name, **3** in this example we tie this to the other server profiles.

    Fully qualified partner LU name, **4** remote network name and profile name. The first part is the ADSM server's network ID. The second part is the LU name of the ADSM client as defined at the ADSM server. In an MVS environment, this is the **ACBNAME** in the **APPL** statement in VTAM for the ADSM server. Ask your network administrator for this information.

    Partner LU alias, **3** this can be the node name of the ADSM server.

    The other fields can be left with their defaults.

13. Press Enter.
14. Skip to the end of this section unless you have a cross domain network connection between the ADSM client and server.
15. If you have a cross domain network connection, press F3 twice.
16. Move the cursor to **Partner LU 6.2 Location**.
17. Press Enter.

    You now see the panel shown in Figure 41.

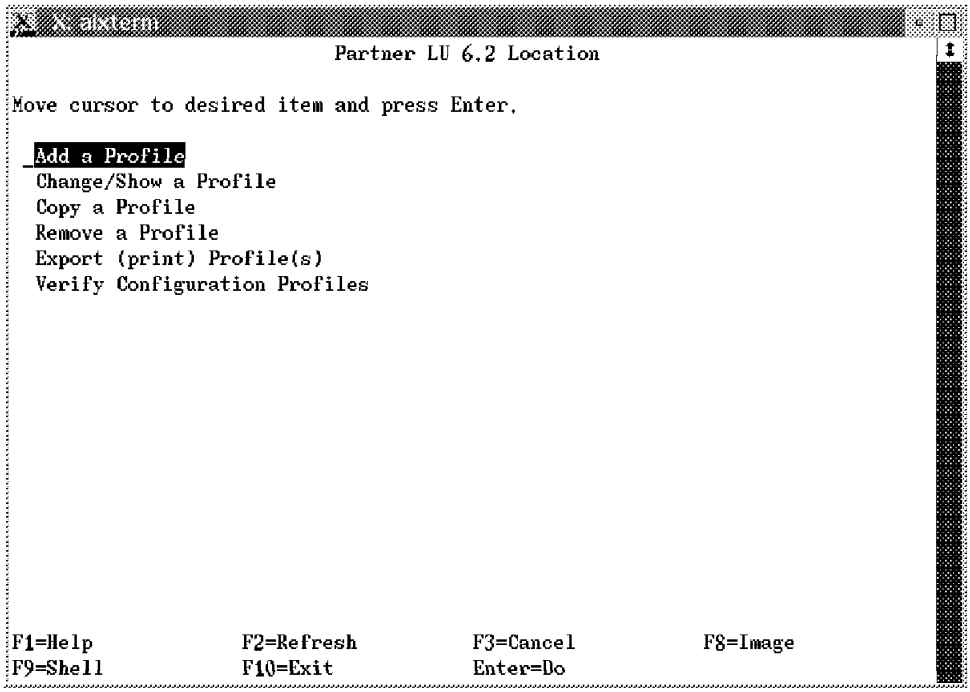


Figure 41. Partner LU 6.2 Location Profile

18. Move the cursor to **Add a Profile**.
19. Press Enter.

    You now see the panel shown in Figure 42 on page 71.

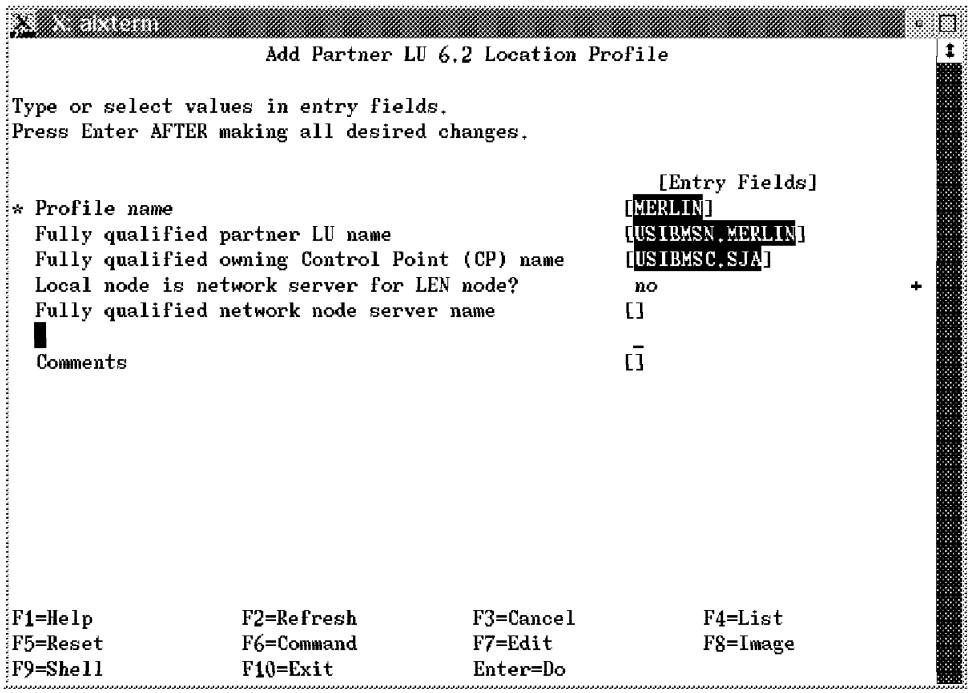


Figure 42. Add Partner LU 6.2 Location Profile

20. Ask your network administrator for detailed information to complete this panel.
21. Enter the following network definitions to complete the definition when using a cross domain environment:

    Profile name, **3** in this example we tie this to the other server profiles.

    Fully qualified partner LU name, **4** remote network name and profile name. The first part is the ADSM server's network ID. The second part is the LU name of the ADSM client as defined at the ADSM server. In an MVS environment, this is the **ACBNAME** in the **APPL** statement in VTAM for the ADSM server. Ask your network administrator for this information.

    Fully qualified owning Control Point (CP) name, the local network name and the SSCP name for the ADSM client network.

    The other fields can be left with their defaults.
22. Press Enter.

You have finished defining the partner APPC profile.

3.4.2.5 Define the APPC Mode Information

Now you need to define the mode name that refers to a table of values that determine the APPC session's run-time parameters.

Continue from the **Add Partner LU 6.2 Location Profile** panel as follows:

1. Press F3 three times.

You now see the panel shown in Figure 43 on page 72.

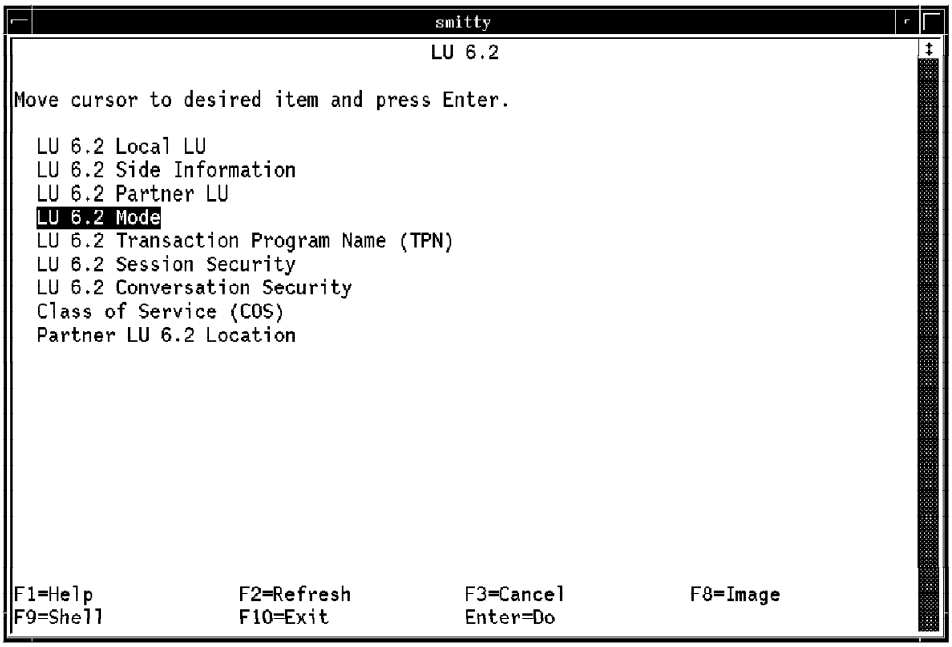


Figure 43. APPC Configuration: LU 6.2

2. Move the cursor to **LU 6.2 Mode**.
3. Press Enter.

   You now see the panel shown in Figure 44.

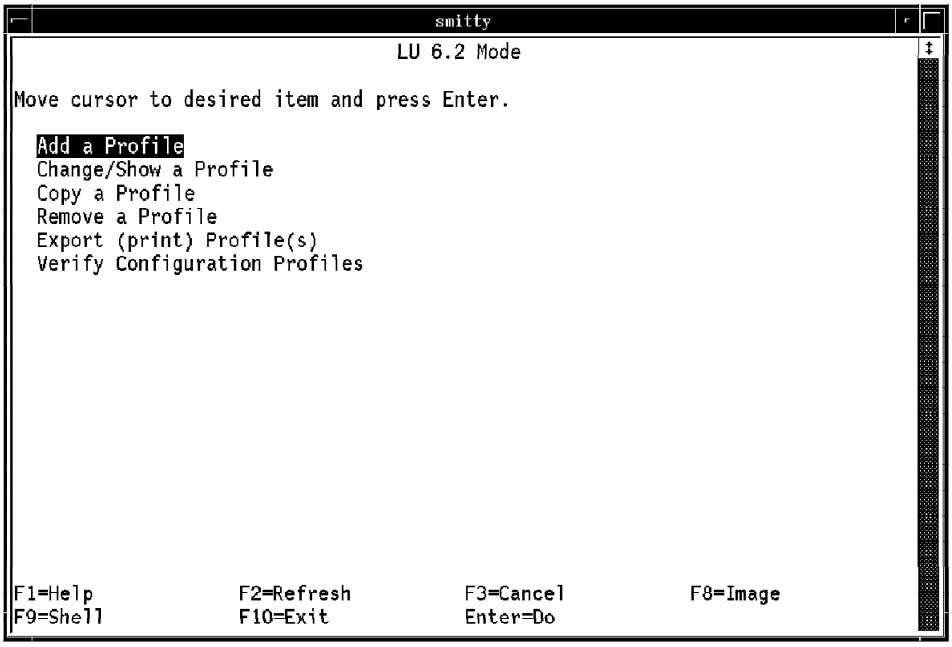


Figure 44. APPC Configuration: LU 6.2 Mode

4. Move the cursor to **Add a Profile**.
5. Press Enter.

   You now see the panel shown in Figure 45 on page 73.

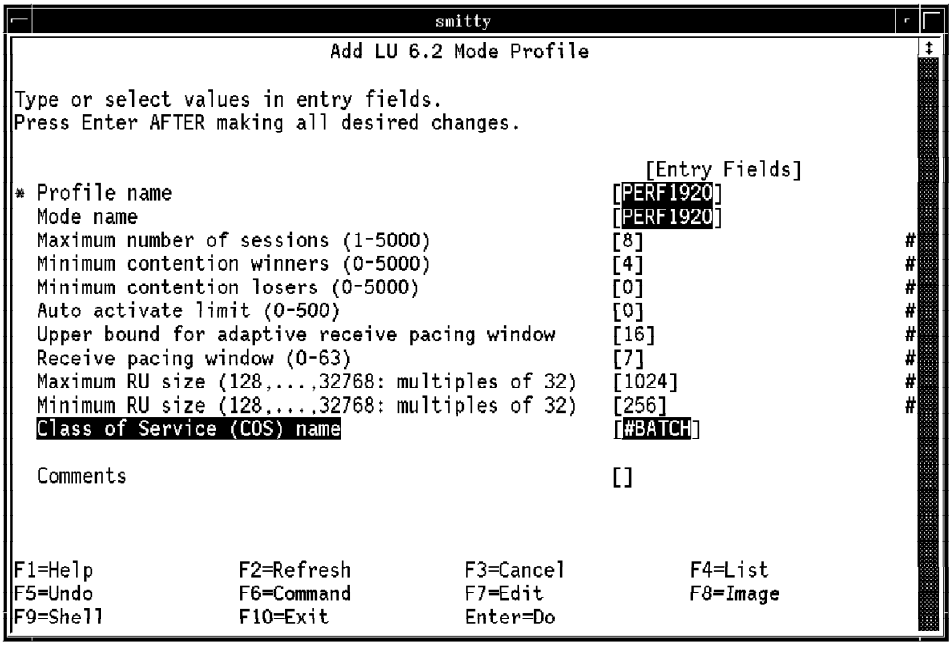


Figure 45. APPC Configuration: Add LU 6.2 Mode Profile

6. Ask your network administrator for detailed information to complete this panel.
7. Enter the following network definitions to complete the definition of the APPC mode information:

   Profile name, 5 make this the same as the mode name.

   Mode name, 5 define the local mode name. It has to be the same as the remote mode name. In MVS this is the logmode entry name in VTAM's logmode table used for the session between the ADSM client and server.

   Class of Service (COS) name #BATCH. This is optional.

   The other fields can be left with their defaults.
8. Press Enter.

You have finished defining the APPC mode information.

3.4.2.6 Define the APPC Side Information Profile

You can optionally define a side information profile before starting the APPC session. The parameters in the side information profile are used to indicate with which partner LU and transaction program you want to communicate. You can define the modes used between AIX and the ADSM server host. This step is optional because this information can be dynamically created by APPC.

Continue from the **Add LU 6.2 Mode Profile** panel as follows:

1. Press F3 three times.

   You now see the panel shown in Figure 46 on page 74.

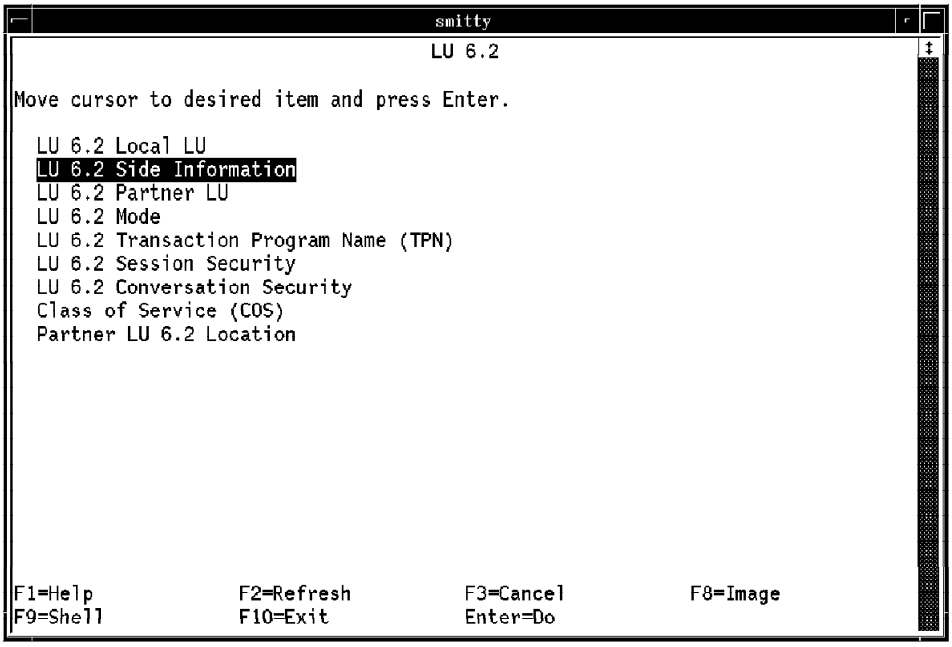


Figure 46. APPC Configuration: LU 6.2

2. Move the cursor to **LU 6.2 Side Information**.
3. Press Enter.

   You now see the panel shown in Figure 47.

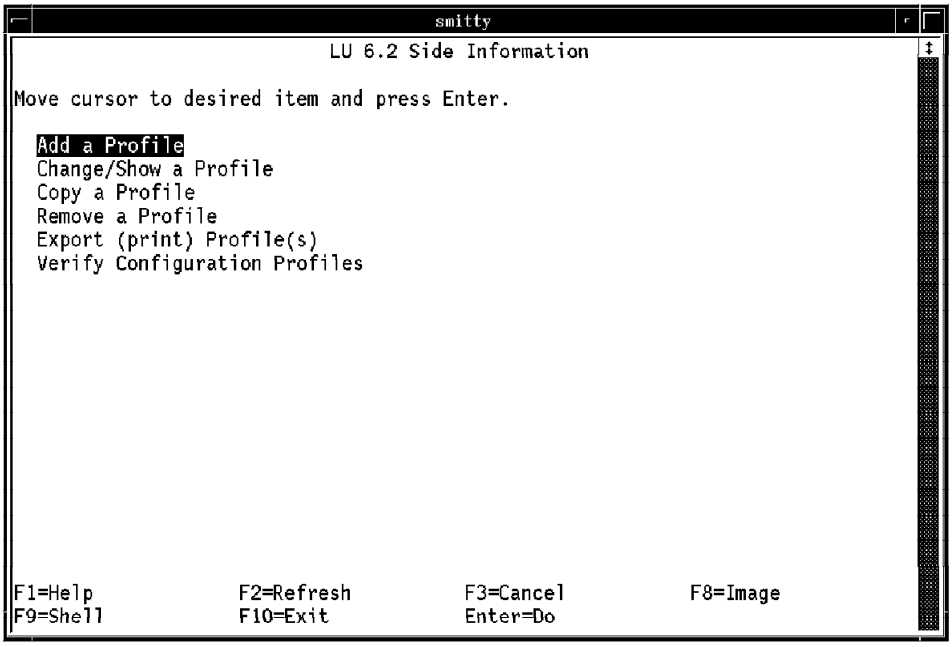


Figure 47. APPC Configuration: LU 6.2 Side Information

4. Move the cursor to **Add a Profile**.
5. Press Enter.

   You now see the panel shown in Figure 48 on page 75.

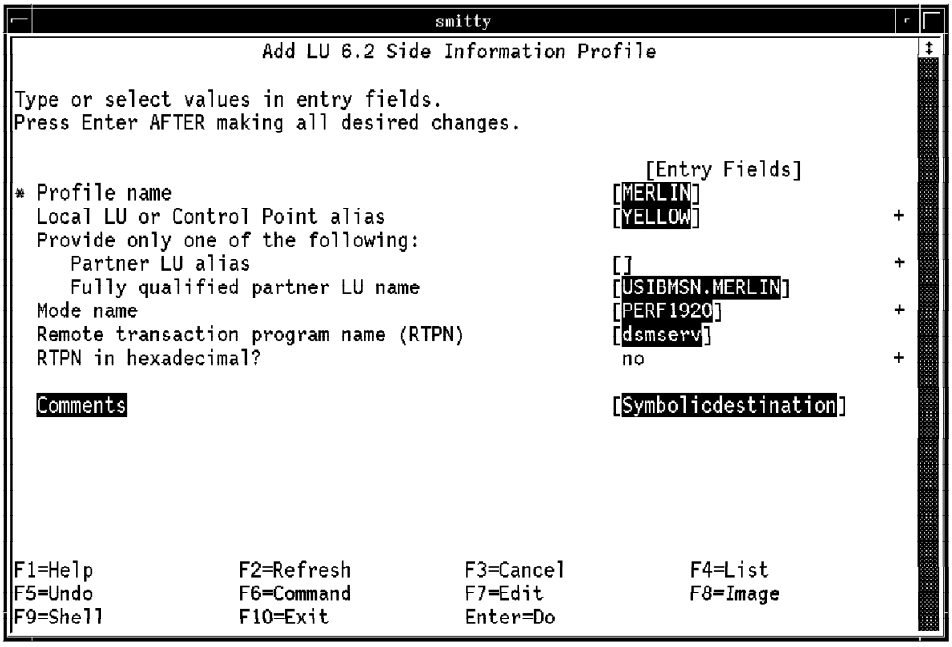


Figure 48. APPC Configuration: Add LU 6.2 Side Information Profile

6. Ask your network administrator for detailed information to complete these panels.
7. Enter the following network definitions to complete the definition of the APPC side information profile:

   Profile name, 3 this can be used to associate the side information with the ADSM server.

   Local LU or Control Point alias, 1 your defined local LU name of the ADSM client.

   Fully qualified partner LU name, 4 remote network name and profile name. The first part is the ADSM server's network ID. The second part is the LU name of the ADSM client as defined at the ADSM server. In an MVS environment, this is the **ACBNAME** in the **APPL** statement in VTAM for the ADSM server. Ask your network administrator for this information.

   Mode name, 5 the local mode name that has to be the same as the remote mode name at the ADSM server. In an MVS environment this is the logmode entry name in VTAM's logmode table that is to be used for the session between the ADSM client and server. Ask your network administrator for this information.

   Remote transaction program name (RTPN) this can be any name you like. You can relate it to the client ADSM program.

The other fields can be left with their defaults.

8. Press Enter.

You have finished defining the APPC side information profile. To repeat, this definition is optional.

3.4.2.7 Verify Configuration

After finishing the configuration for APPC connectivity, AIX SNA Server/6000 provides a utility for verification. Verification ensures that the configuration is correct and that no profiles are in conflict with each other.

Continue from either the **Add LU 6.2 Mode Profile** or **LU 6.2 Side Information** panel as follows:

1. Press F3 five times.

   You now see the panel shown in Figure 49.

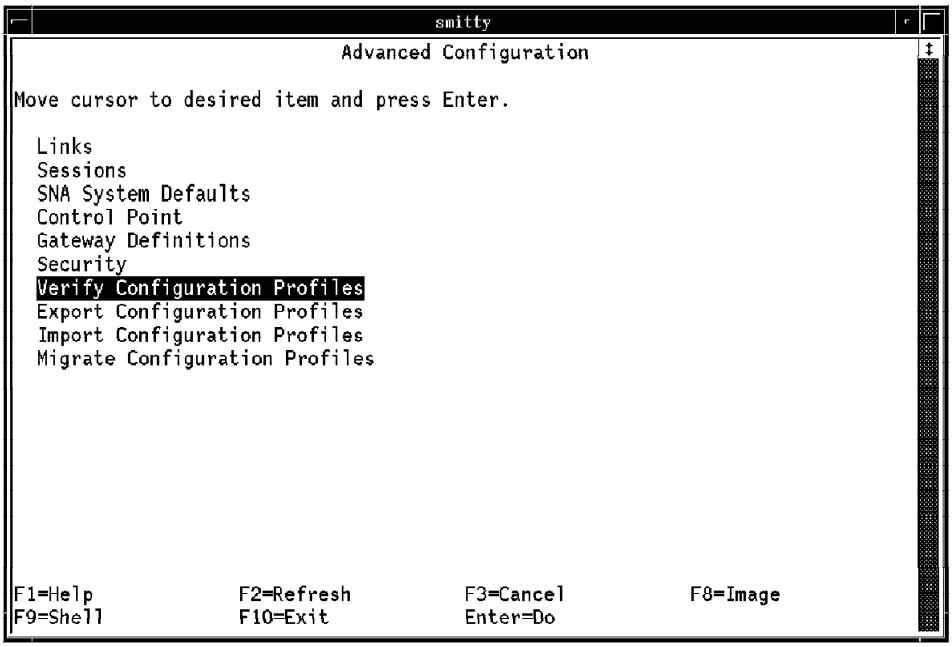


Figure 49. APPC Configuration: Advanced Configuration

2. Move the cursor to **Verify Configuration Profiles**.
3. Press Enter.

   You now see the panel shown in Figure 50 on page 77.

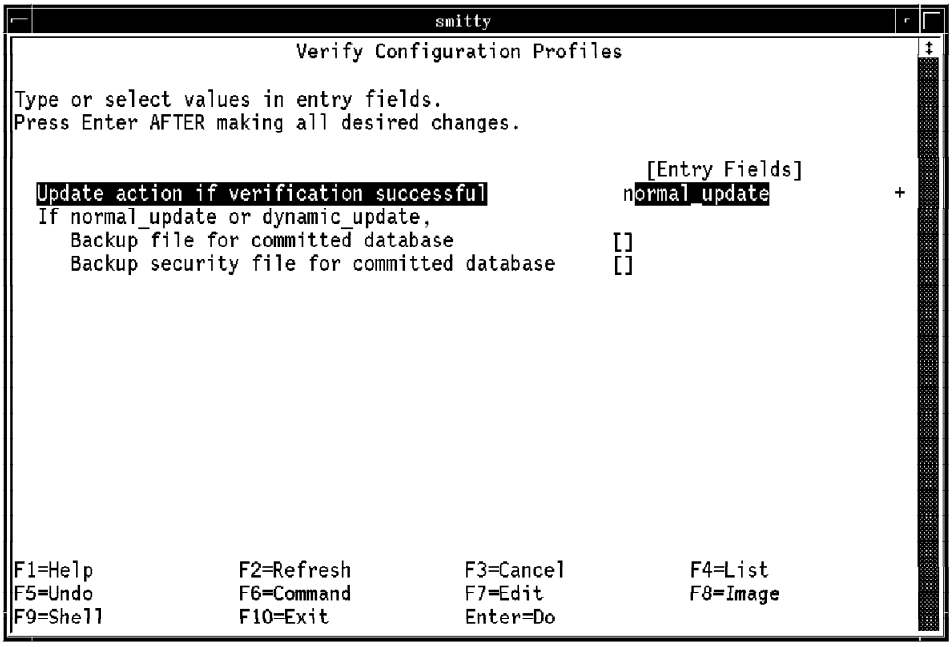


Figure 50. APPC Configuration: Verify Configuration Profiles

4. Move the cursor to **Update action if verification successful**.
5. Select the **normal_update** option in the **Entry Fields**.
6. Press Enter.

You have finished verifying the configuration.

3.4.2.8 Save the Configuration

After you have verifyied the APPC configuration you need to save it. To save your APPC configuration you have to export the configuration profiles.

Continue from the **Verify Configuration Profiles** panel as follows:

1. Enter F3 twice.

   You now see the panel shown in Figure 51 on page 78.

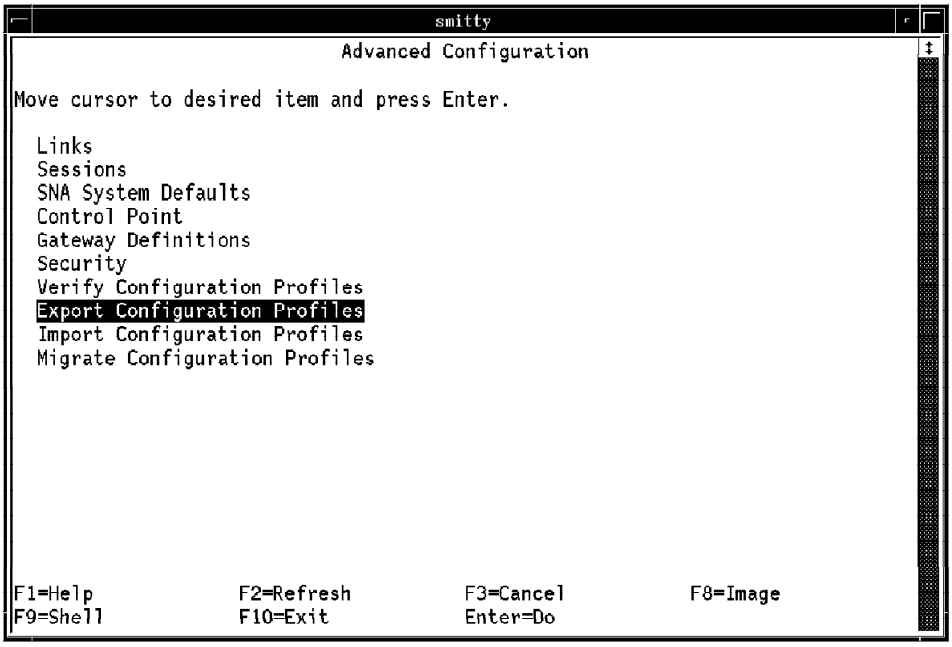


Figure 51. Export SNA Profiles: Advanced Configuration

2. Move the cursor to **Export Configuration Profiles**.
3. Press Enter.

   You now see the panel shown in Figure 52.

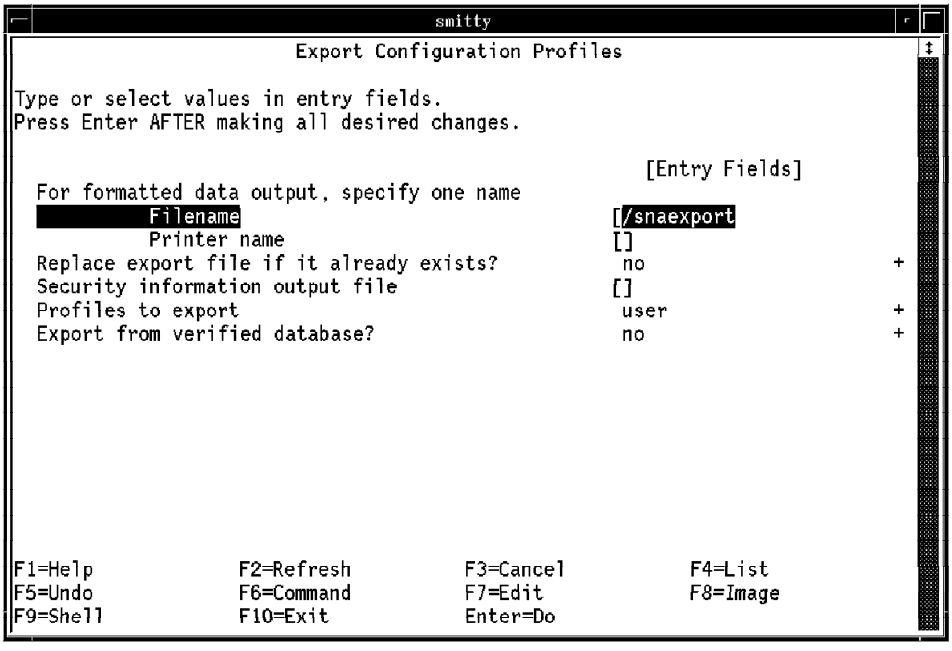


Figure 52. Export SNA Profiles: Export Configuration Profiles

4. Enter a file name in the **Entry Fields** on the **Filename** line.
5. Press Enter.

Note that on the **Advanced Configuration** panel (Figure 51) you can also import the configuration profiles for modification at a later time.

You have finished all work with the configuration. You can start the APPC session to see whether the definitions are correct. To start SNA/6000 Services enter the **sna -start** command as shown in Figure 53 on page 79.

```
aixterm
5:root@yellow:/ # sna -start
0513-059 The sna Subsystem has been started. Subsystem PID is 3592.
5:root@yellow:/ # lssrc -ls sna
    Link           Adjacent       Node    Device             Number of
   station         CP name        type     name      State    sessions
-------------- ----------------- ----- --------- ---------- ----------
@tok0                                    tok0      Starting           0
MERLIN         USIBMSN.MERLIN    NN     tok0      Active             2
SEATTLE        USIBMSN.SNC6011I  EN     tok0      Active             0
WTSCMXA                                  tok0      Starting           0
5:root@yellow:/ #
```

Figure 53. Start and Check SNA/6000 Services

3.4.2.9 Update the DSM.SYS File

You can update the **dsm.sys** file in one of two ways. You can specify either the symbolic destination ID or the full names of the transaction program and partner LU names. We recommend that you specify the symbolic destination ID. Add the following entries to the **dsm.sys** file:

```
commmethod              snalu6.2

symbolicdestination     merlin
```

This completes the setup of APPC connectivity for the AIX ADSM client.

3.4.3 Problem Determination

Two scenarios are likely to require problem determination. The first and most common is when an APPC session cannot be established. The second is when an APPC session is established but does not perform adequately.

Determining why an APPC session does not work is not easy. It typically requires running a trace to ascertain the cause of the failure. The first things to check are the token-ring link station profile, the partner APPC profile, and the APPC mode information profile. These definitions must be correct and correlate with the ADSM server's definitions. If not, APPC will not work, and you will have to run a trace.

Tracing is simple to perform, but difficult to analyze. There are two ways to run a trace to analyze APPC problems:

- Run a VTAM line trace from the host
- Run **aping** at the AIX server.

Running a VTAM trace from the host is not covered here, because it is beyond the scope of this book. You should get your MVS VTAM systems programmer involved to execute and analyze this trace.

The **aping** command can be used to test the LU type 6.2 connection. The command can be found in the **/usr/lpp/sna/samples/bin** directory. Figure 54 shows the result of testing the configuration with the **aping** command.

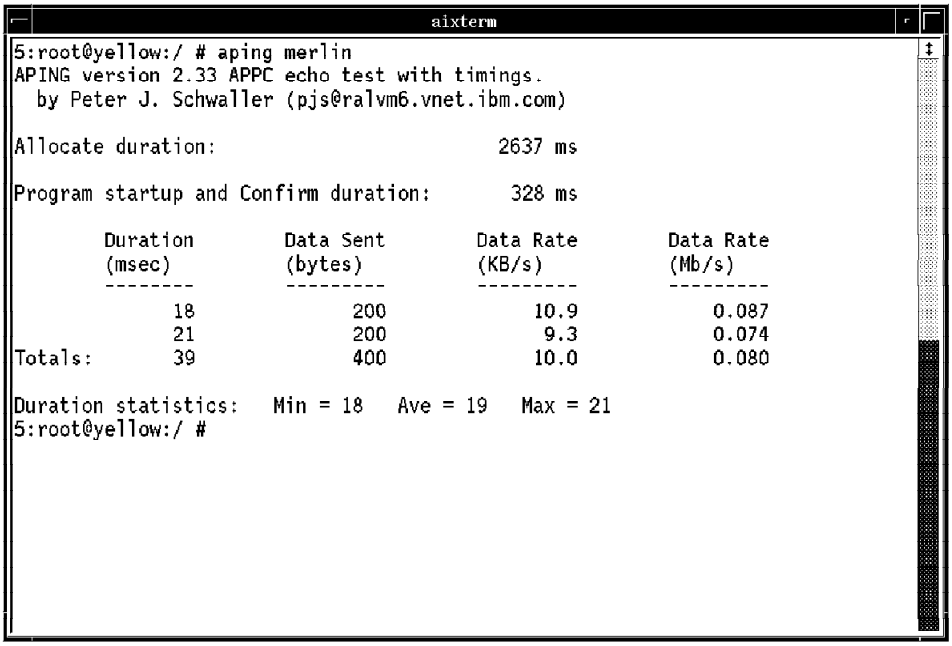


Figure 54. Aping Command

3.4.4 Performance Considerations

Tuning APPC is a complex task. Many parameters in VTAM and NCP affect APPC performance. Most of these are beyond the scope of this book. We consider below three parameters that affect performance: two are specified in SNA Server/6000 and one is an ADSM option:

- RU size
- RU pacing
- CPIC (APPC) buffer size.

For bulk data transfer products like ADSM, a large RU size is desirable for performance. The RU size is negotiated as part of the bind process at the beginning of each session. The RU size used is the minimum value allowed by each node in the transmission path.

Increasing the RU size increases the amount of memory needed. A good starting point for ADSM is a maximum RU size of 4096 bytes and a minimum RU size of 256 bytes.

The RU size for the SNA Server/6000 is defined in the APPC mode information. The RU size should be coordinated between the ADSM client and server. The RU size is set in the VTAM logmode entry for an MVS ADSM server.

RU pacing controls the number of RUs a machine can send before stopping data transmission and waiting to receive an acknowledgment. If a small window is specified, data transfer may intermittently stop in order to wait for acknowledgments.

Efficient memory usage is most important in small machines. To balance better performance with efficient memory use, a maximum pacing window may not always be desirable. RU pacing should be matched to the power of the ADSM client workstation. A value of 8 is recommended for an 80386-based machine and 63 for an 80486-based machine.

RU pacing is set in the APPC mode information for SNA Server/6000. It is also defined with the APPC parameters for the ADSM server.

The **cpicbuffersize** option of the **dsm.sys** file sets the size of the APPC buffer. The larger this buffer is, the better communications performance will be unless the AIX system is short on memory. In this case continue to use the default of 15KB. If the machine has ample memory, increase this option to the maximum of 31KB.

APPC also needs to be tuned in the ADSM server. Parameters like the RU size should be coordinated between the ADSM client, the ADSM server, and any intermediate nodes for optimal performance.

A detailed discussion of APPC at the ADSM server is beyond the scope of this book. The type of ADSM server parameters to consider when MVS is the ADSM server include the following VTAM parameters:

- RUSIZES - RU maximum and minimum sizes
- PACING and VPACING - RU pacing
- IOBUF - the amount of buffering.

The key parameters within NCP include:

- MAXBUFRU - number of RU buffers
- UNITSZ - RU buffer size
- RCVBUFC - DLC frame size
- T2TIMER - DLC pacing.

Chapter 4. Using the ADSM AIX Client

In this chapter we present an overview of using the ADSM AIX client. For detailed examples of using the ADSM backup/archive client services see the *ADSM User's Guide and Reference for UNIX*.

We also cover tailoring of backup and archive services through the use of management classes, controlling which files are to be processed through the include/exclude process, and automatically scheduling and executing ADSM backup and archive processing.

The GUI is used in the examples in this chapter. The CLI commands are identified after the GUI examples. Both the GUI and CLI for all ADSM AIX client functions are covered in detail in the *ADSM User's Guide and Reference for UNIX*.

4.1 Running the ADSM Client

After customizing the options files and setting up the communications protocol environment, you can run the ADSM client to request backup and archive services. To allow the AIX system to begin ADSM service, the system needs to be authorized to access the ADSM server. Once authorized, you can bring up the ADSM client at an AIX workstation and begin ADSM services.

4.1.1 Authorization and Security

An ADSM server uses the client's node name to authorize access to ADSM services. Thus, nodes registered with an ADSM server have permission to use the ADSM server. You must be an ADSM administrator with system privilege to register nodes with the server.

Once an ADSM AIX client is registered in an ADSM server, AIX users can obtain ADSM backup and archive services. You can tailor the client system options file to prevent access to ADSM services for selected users or groups of users.

When you request backup service from the ADSM client, you can only back up and restore your files to the ADSM server. However, you can archive any files for which you have access permission. In AIX, you can control your files to determine who can share them. The same is true of the ADSM client. You can authorize other users, on other nodes, to restore your backup files.

4.1.2 Starting the ADSM Client

To start ADSM issue the **dsm** command with AIXwindows or enter the **dsmc** command in an ASCII environment. If AIXwindows has not been started, you should enter **xinit**.

If you do not use the **passwordaccess** option in the client system options file, ADSM displays a login panel on which you can enter your password. Once an

© Copyright IBM Corp. 1994

ADSM AIX client node is registered, users of that client can obtain services from the ADSM server by entering the correct password. Ask your ADSM administrator or AIX administrator for the server's password.

After the authentication process, you can begin with ADSM services. When you use the GUI, ADSM displays the **ADSTAR Distributed Storage Manager** panel as a window that includes an action bar and two lists of the file systems available to you, one for backup and archive processing and the other for restore and retrieve processing. On this window you should select the file systems that you want to process. You can then use the menu bar to choose services, such as **Backup**, **Restore**, **Archive**, **Retrieve**, **Utilities**, **View**, and **Help**.

The ADSM functions discussed in this chapter are selected through the GUI, but they also can be selected through the CLI. The advantage of using the GUI is that it is more user friendly. The CLI offers more flexibility, however.

The ADSM AIX client also supports online help documentation. If you have a usage problem, type **help** if using the CLI or select the **Help** button in the GUI to get help information.

The ADSM AIX client does not support backup or archive of special operating system data types. Thus, you need to recover the following files using AIX system utilities:

- Character special files, for example, device drivers
- Block special files, for example, files in the **/dev** directory
- Named pipe files.

4.2 Using ADSM Functions

In the sections that follow we describe the ADSM AIX client backup, restore, archive, and retrieve services through the GUI. For information on how to use the CLI or for more detailed examples of the GUI refer to the *ADSM User's Guide and Reference for UNIX*.

4.2.1 Incremental Backup

Incremental backup should be used for your daily work to prevent data loss. You can start incremental backup by request, or you can use the ADSM scheduler to back up your files automatically. Usually, it is the responsibility of the root user to run incremental backup.

To run incremental backup by request, select **Backup** from the action bar on the ADSM main window and then select **incremental backup** from the pull-down menu. The files eligible for incremental backup are determined by the **include** and **exclude** options defined. During the backup process, status information on each file backed up is displayed. Figure 55 on page 85 shows an example of incremental backup service at completion.

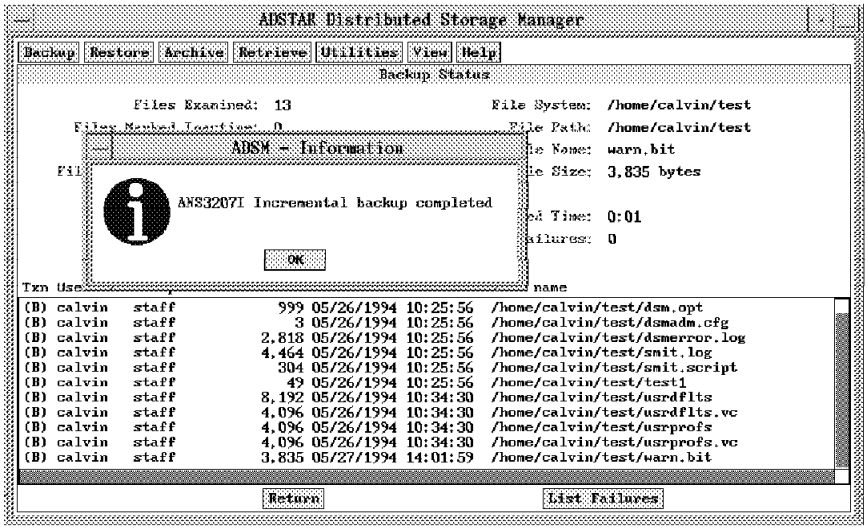


Figure 55. ADSM Incremental Backup

To request an incremental backup using the CLI you would enter the **dsmc incremental** command followed by the file system that you want to incrementally back up.

4.2.2 Management Classes

ADSM uses management classes to determine whether a file or group of files is eligible for backup or archive services. Below we describe how to define a management class and how to use management classes with ADSM backup and archive services.

4.2.2.1 Definition

As an ADSM administrator, you can define storage management policies based on user requirements for backup or archive services. Policy domains provide a logical way of managing a group of client nodes. For example, you can establish policy domains by:

- Functional organization, such as payroll, application programming, or customer service
- Physical location, such as building 70B or building 51
- LAN, such as all client nodes associated with file server B.

Each policy domain can hold numerous policy sets, which contain one or more management classes. Policy sets can be used to implement different policies based on business and user requirements. Only one policy set can be active at a time. A management class contains a backup or an archive copy group. These copy groups are used to establish backup and archive services for groups of files.

ADSM uses management classes to determine whether files can be backed up or archived and how to manage the backup versions and archived copies of files

in the ADSM server. If the management class you assign to files contains no backup copy group, you cannot back up files.

4.2.2.2 Contents

A management class contains a backup copy group or archive copy group or both. A backup copy group contains attributes that ADSM uses during backup processing. It also contains attributes to manage the backup versions of your files on a server. The attributes determine:

- Whether a file is to be backed up
- How many days must elapse before a file can be backed up again
- How a file is processed during backup if it is in use
- Where the server stores backup versions of your files and directories
- How many backup versions of your files ADSM keeps
- How long the ADSM server keeps the backup versions of your files.

An archive copy group contains attributes that control:

- Whether a file is archived if it is in use
- Where the ADSM server stores archived copies of your files
- How long the ADSM server keeps archived copies of your files.

To define a management class, you must be an ADSM administrator with policy privilege. For more detailed information about defining management classes, refer to the administrator′s guide for the ADSM server you are using.

4.2.3 Creating an Include/Exclude File

As an AIX administrator of ADSM services, you can determine which file or files users can or cannot back up or archive by creating an include/exclude file. This file controls whether ADSM should consider a file for backup and which management class is to be assigned to the file.

4.2.3.1 Consider a File for Backup

To use an include/exclude file, you must specify the file name in the **inclexcl** option statement of the client system options file. The include/exclude file must reside in a directory to which all users of the ADSM client have read access. If you do not create an include/exclude file, ADSM considers all files in the ADSM client′s domain to be eligible for backup and archive.

Before creating an include/exclude file, you need to:

- Determine which files should not be considered for backup. Define these files with an **exclude** option statement.
- Determine whether there are any exceptions to the **exclude** statements. If so, define specific **include** statements for those exceptions.
- Discuss the list with users to determine whether any additional **include** or **exclude** statements are required.

- Determine whether files should be assigned to a specific management class instead of the default management class.

The following statements might appear in an include/exclude file:

```
exclude /home/proj2/test/*
include /home/proj2/test/chp4
```

The processing flow of the **include** and **exclude** statements is from the bottom up. Therefore, in this example the **chp4** file is included for backup service, and all other files in the **test** directory are excluded.

If the order of the **include**/**exclude** statements were reversed, you would have different files backed up:

```
include /home/proj2/test/chp4
exclude /home/proj2/test/*
```

Here, as the statements are processed in a bottom up order, all files in the **test** directory are excluded and cannot be considered for backup or archive services. Thus the **chp4** file is not processed with this reversed order.

When ADSM backup and archive services are requested, all files in the default client domain go through include and exclude processing. Be sure to use the minimum number of **include** and **exclude** statements to produce the results you want and to minimize processing time. Note that you cannot exclude a directory because ADSM backup and archive services always store the directory information.

When you request the ADSM archive service, ADSM does not check the include/exclude file to determine whether files are eligible for archive. ADSM only checks whether the files are associated with a specific management class. You can archive any files to which you have read permission.

4.2.3.2 Assign Management Class to Files

Each of the files you back up or archive must be associated with a management class. The management class contains attributes that ADSM uses to determine whether a file is qualified for backup or archive. ADSM also uses the attributes to determine how to manage the backup versions and archive copies of your files on ADSM storage. If you do not assign a management class for files, ADSM uses the default management class identified by the ADSM administrator.

To assign a management class other than the default to a file or group of files, you use an **include** statement in the include/exclude file. For example, to associate all files in the **test** directory with a management class of **finance** you can use the following statement:

```
include /home/proj2/test/*    finance
```

When you archive a file or group of files, you can choose to override the assigned management class for those files. If you use the GUI, ADSM presents a window that allows you to select a different management class. With the CLI you can use the **archmc** option of the **dsmc archive** command. You can use the **dirmc** option in the client system options file to assign a specific management class to directories.

4.2.4 Selective Backup

Use ADSM selective backup if you want to back up only a specific subset of your files. ADSM supports selective backup by file specification and by directory tree.

Select **Backup** from the action bar on the ADSM main window and then select the **Backup by file specification** from the pull-down menu. You now see the panel shown in Figure 56. Enter the name of the file that you want to back up. The name can include wildcard characters. After entering the file name, select **List files**.

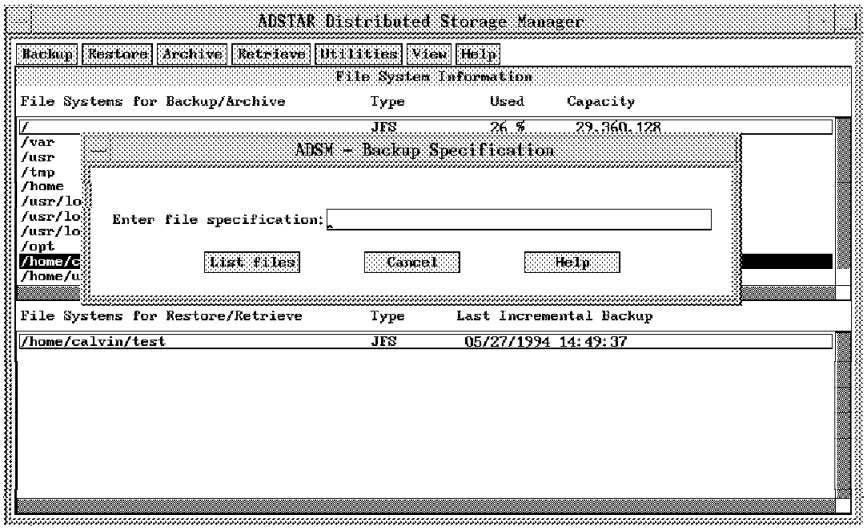


Figure 56. ADSM Selective Backup by File Specification

You now see the list of files that you have selected for backup. You can select individual files from the list or you can use the **Select All** option to back up all the files in the list.

If instead you want to back up an entire directory tree, select the **Backup by directory tree** option. For each file system, ADSM shows the directory tree. Select the directory name, and all files in the directory will be shown as in Figure 57 on page 89. ADSM waits for you to select which files in which directories you want to back up.

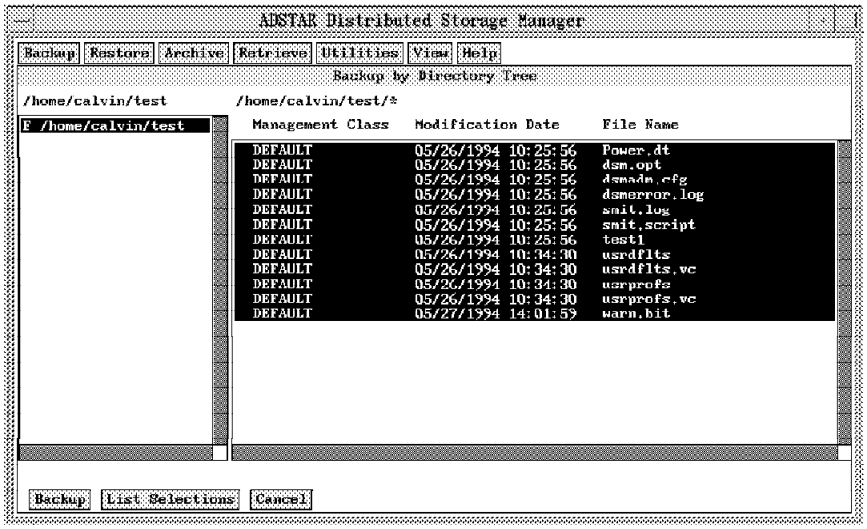


Figure 57. ADSM Selective Backup by Directory Tree

To request a selective backup using the CLI you would enter the **dsmc selective** command followed by the file system that you want to selectively back up.

4.2.5 Restore

Use the restore function to return backup files to the workstation when data has been lost. As with backup, select the file systems to be processed. Then select **Restore** from the action bar, and you see three ways of restoring your backup files:

- Restore by file specification
- Restore by directory tree
- Restore by subdirectory path.

To restore backup files by file specification, select the **Restore by file specification** option in the **Restore** pull-down menu. You then can enter the file name, including wildcard characters, for the file that you want to restore. Then select the **List files** option. ADSM then shows you all of the qualified files that can be restored (see Figure 58 on page 90). Select all or some of them and click on the **Restore** push button.

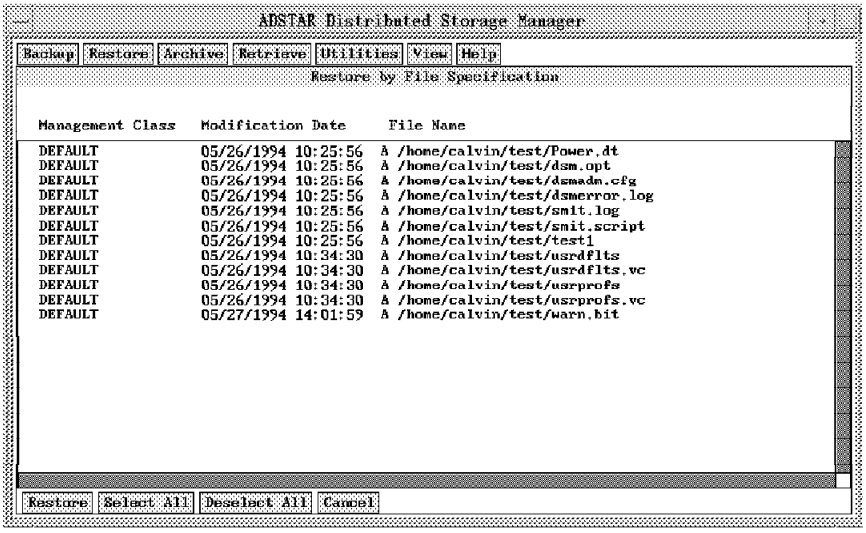


Figure 58. ADSM Restore by File Specification

ADSM present you with a window in which you can select how you want the files to be restored. You can restore the file to its original location or to a new destination.

You can also select the **Restore by directory tree** option from the **Restore** pull-down menu to restore one or more directories. The directory tree for each file system you want to process is displayed. Select the directory in which you are interested, and the files available for restore are listed as shown in Figure 59.

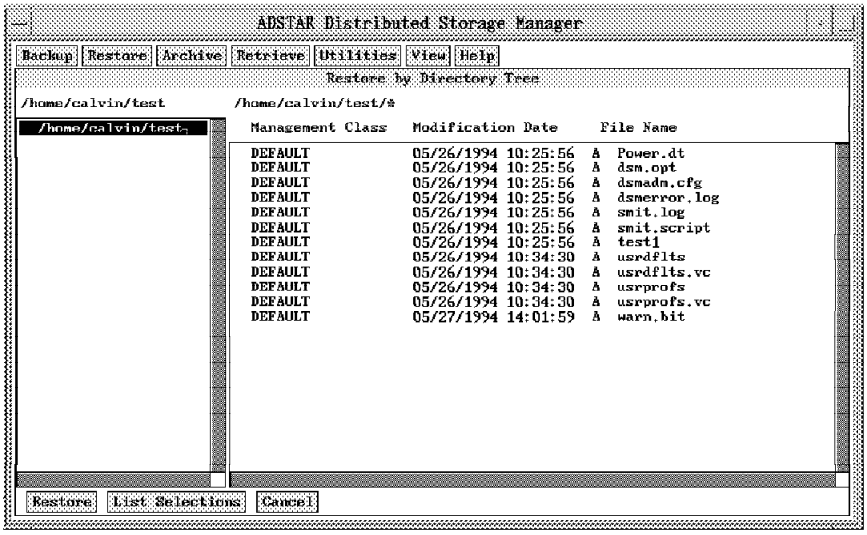


Figure 59. ADSM Restore by Directory Tree

Select the files you want to restore from the list and click on the **Restore** push button. A window is displayed in which you can select the restore destination.

To restore by subdirectory path, select **Restore subdirectory path** from the **Restore** pull-down menu. The window shown in Figure 60 on page 91 is displayed. Enter the source and destination path for the file you want to restore and click on **OK**.

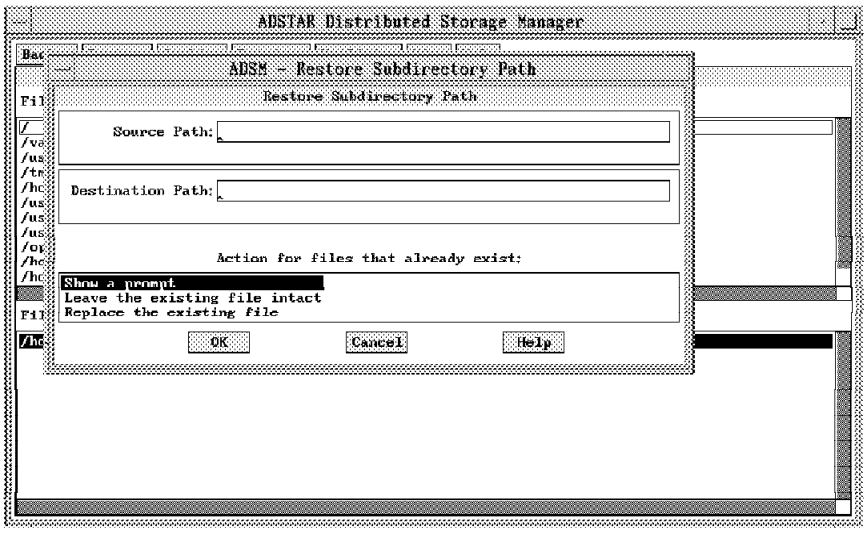


Figure 60. ADSM Restore by Subdirectory Path

To request a restore using the CLI you would enter the **dsmc restore** command followed by the file system that you want to restore.

4.2.6 Archive

You can use the ADSM archive service to save files at a specific point in time, or when you want to place copies of files on the ADSM server and erase them from your workstation. ADSM provides two ways for you to archive files, by file specification and by directory.

To archive files by file specification, select **Archive** from the ADSM main window after selecting the file systems you want to process. Then select **Archive by file specification** from the pull-down menu.

Enter the specific file name, optionally using wildcard characters. Click on the **List files** push button. The window shown in Figure 61 on page 92 is displayed showing a list of those files that match your specifications.

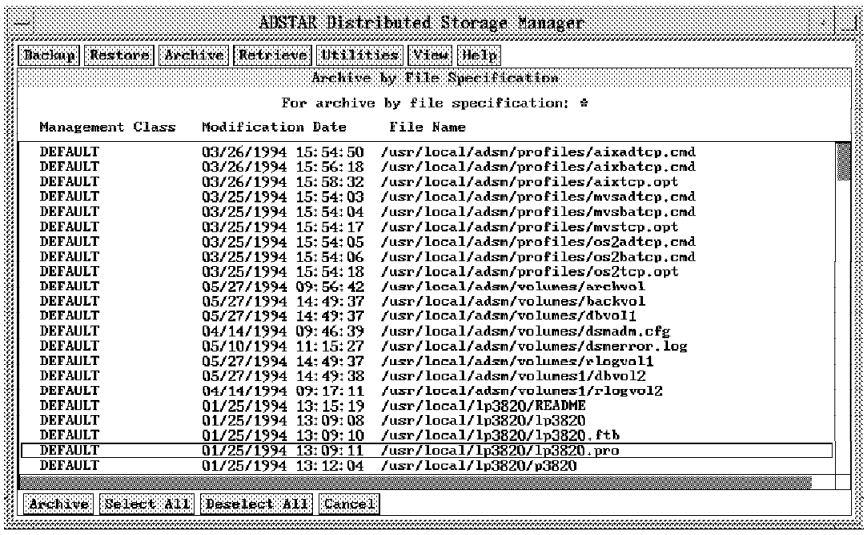


Figure 61. ADSM Archive by File Specification

Select the files that you want to archive and then click on the **Archive** push button. You now see a window for each file you selected in the list. This window allows you to enter descriptive text that is stored with the archive and can be used later to help you retrieve the correct copy of the file.

The alternative way for you to archive files is to archive the files by directory tree. Select **Archive by directory tree** from the **Archive** pull-down menu. This action displays the directory tree for each file system you want to process. Select the directory you want to use with archive. The screen shown in Figure 62 is displayed.

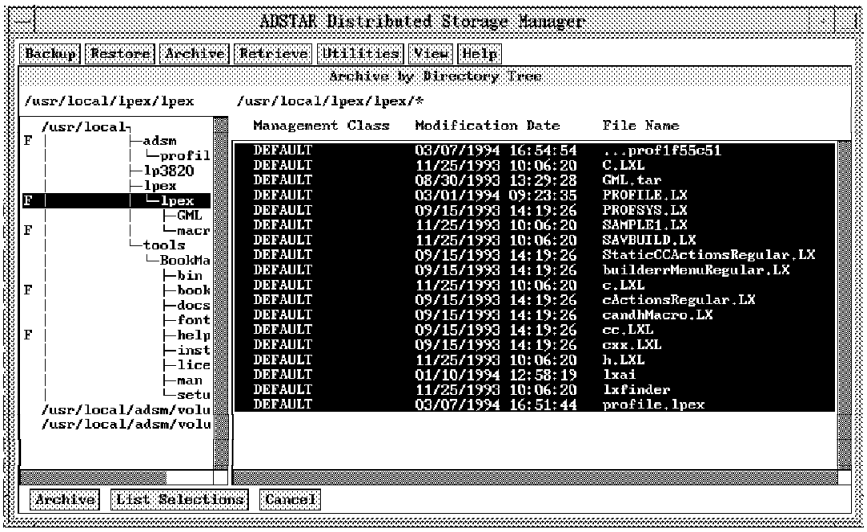


Figure 62. ADSM Archive by Directory Tree

Select the files within the directory that you want to archive. You can then either verify the list you have selected by clicking on the **List Selections** push button or go straight to archive by clicking on the **Archive** push button. A window for each file you have selected for archive is displayed where you can enter descriptive text that you can use when you retrieve the archived file.

To request an archive using the CLI enter the **dsmc archive** command followed by the file system that you want to archive.

4.2.7 Retrieve

If you find that you need the archived files at your workstation, you can retrieve the files from the ADSM server. You can retrieve files only by file specification. Select **Retrieve** from the ADSM main window action bar after selecting the file systems you want to process. Select **Retrieve by file specification** from the **Retrieve** pull-down menu. You now see the window shown in Figure 63.

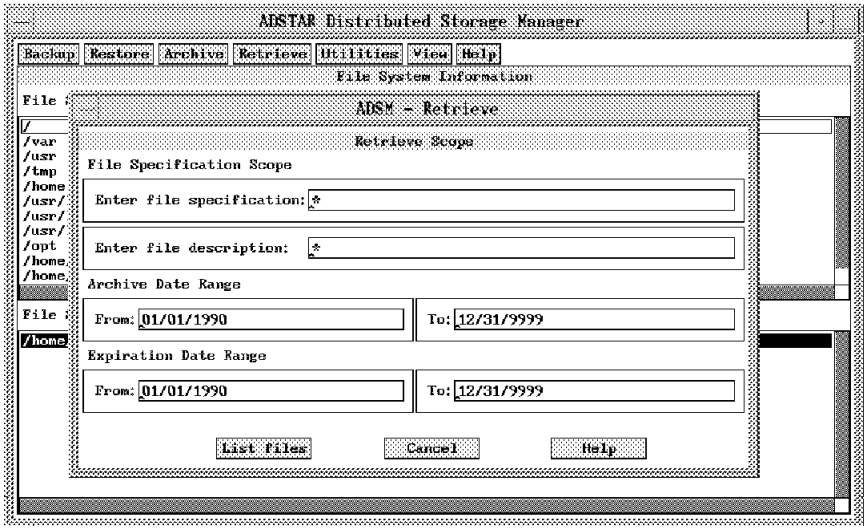


Figure 63. ADSM Retrieve by File Specification

Enter the file name, description, archive date, or expiration date of the file you want to retrieve. You can use wildcard characters in the file name and description. All of these fields are optional, so you could enter only the file description. Click on the **List files** push button.

You now see a window with a list of the files you have selected for retrieval. Select the files you want and then click on the **Retrieve** push button. You then see a window that allows you to select the destination of the retrieved file and whether you want to replace a file with the same name at your desired destination.

To request a retrieve using the CLI you would enter the **dsmc retrieve** command followed by the file system that you want to retrieve.

4.2.8 Sharing Access to Files

The files you own can be shared by granting authorization to other users. As well, the ADSM client allows other ADSM users to access your backup or archive files.

To provide shared authorization, select **Utilities** from the action bar in the ADSM main window. Select **Set Authorization** from the pull-down menu to get to the

window shown in Figure 64 on page 94 where you can authorize users to access your backup or archive files.

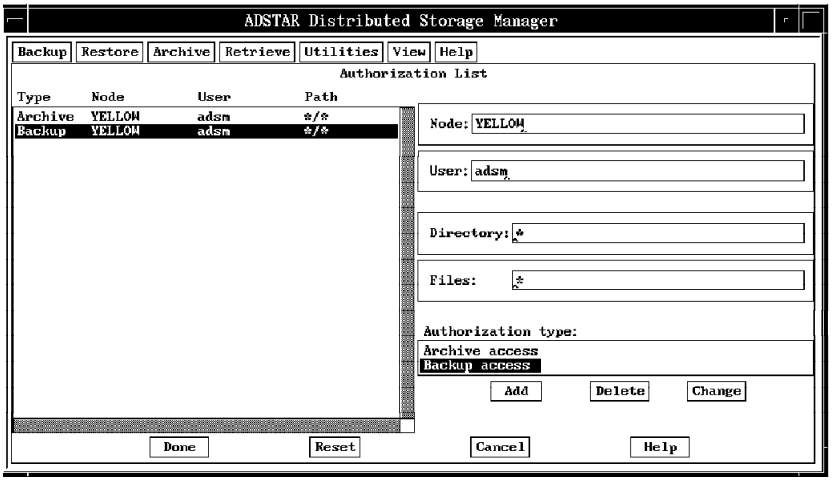


Figure 64. Set Authorization

To provide access to your files using the CLI you would enter the **dsmc set access** command followed by the file system to which you want to allow access.

4.3 Automatic Scheduling

To eliminate the routine workload for the user in backing up and archiving files on a day-to-day basis, ADSM provides automatic scheduling. With ADSM scheduling, an ADSM administrator can define schedules to run incremental backup or archive for your file systems on a regular basis. In the sections that follow we describe how to use automatic scheduling for backup and archive.

4.3.1 ADSM Server Implementation

To set up scheduling on the ADSM server, the storage administrator should do the following:

- Define one or more schedules on the ADSM server
- Associates client nodes with their schedules
- Set server parameters related to scheduling.

To define the schedule on the ADSM server, you issue a **define schedule** command along with parameters to tailor the schedule, for example, to set the date and time the schedule is to begin. There are also parameters for the ADSM server that can be used for balancing scheduled work, choosing a schedule mode, and controlling contact with the ADSM server. You can also define how long and how often the schedule should run once it begins.

The schedule specifies which file systems ADSM is to process and whether ADSM should perform incremental or selective backup or archive. The schedule can also be given a priority for execution.

Once the schedule is defined at the server, ADSM clients can be associated with the schedule. This is done at the ADSM server and can be done only by an authorized user of the ADSM administrative client.

4.3.2 ADSM Client Implementation

As the AIX root user, you need to do the following at the ADSM client to support automatic scheduling:

- Modify schedule options in the client system options file, **dsm.sys**
- Start the client scheduler on your node.

Section 3.2.1.4, “Scheduling Options” on page 43 discusses the scheduler options that need to be placed in the **dsm.sys** file. The client scheduler must be running before the scheduled work can be initiated. To start a client scheduler, issue the **dsmc schedule** command. You can start the client scheduler when you start the operating system, or at any other appropriate time. When you enter the **dsmc schedule** command, ADSM starts the client scheduler, which runs continuously until you close the window in which you entered the schedule command.

You can also issue the **query schedule** command to determine when the next schedule is to run. You are then prompted for the AIX password. After you have entered the password, you see the following panel:

```
Session established with server ADSM: AIX
  Server Version 1, Release 2, Level 0.4
    Server date/time: 11.03.1994 12:14:23   Last access: 11.03.1994 12:09:56

      Schedule Name: AIX_DAILY
        Description: daily incremental backup of netware files
             Action: Incremental
            Options:
            Objects:
           Priority: 10
     Next Execution: 2 Hours and 29 Minutes
           Duration: 20 Minutes
             Period: 1 Day
        Day of Week: Any
             Expire: Never
```

To start the scheduler, enter the **dsmc schedule** command and the ADSM scheduling session screen is displayed as follows:

```
  ADSTAR Distributed Storage Manager
  Command Line Backup Client Interface - Version 1, Release 2, Level b.8
  5648-020 (C) Copyright IBM Corporation, 1990, 1993, All Rights Reserved.

  Please enter password for node "YELLOW":
```

After you have entered the password correctly, you see status information about the schedule. In this case a schedule for incremental backup has been set up for the ADSM client **yellow**. The schedule is to start at 14:45:00 server time:

```
Session established with server ADSM: AIX
  Server Version 1, Release 2, Level 0.4
  Server date/time: 26.05.1994 11:55:50   Last access: 24.05.1994 11:04:20

Querying server for next scheduled event.
Next operation scheduled:
------------------------------------------------------------
Schedule Name:         AIX_DAILY
Action:                Incremental
Objects:
Options:
Server Window Start:   14:45:00  on 26.05.1994
------------------------------------------------------------
Command will be executed in 2 hours and 49 minutes.
```

Chapter 5. Exploiting the ADSM AIX Client

In this chapter we present examples of how you might take full advantage of the ADSM client on an AIX system. We discuss when and when not to use ADSM in the recovery of different components of the AIX system's software environment. We also briefly discuss performance and tuning of the ADSM environment.

5.1 ADSM Client with Multiple ADSM Servers

An ADSM AIX client can connect to multiple ADSM servers. This may be useful if the ADSM server is located in the same building as the AIX server. In this case you might want to attach to another ADSM server that is located outside the building for disaster recovery purposes.

You have to configure the options files to connect to different ADSM servers. The configuration for multiple ADSM servers is almost the same as configuring your ADSM client to connect to a single ADSM server. Figure 65 shows one AIX system as an ADSM client connecting to two ADSM servers. An authorized user of the ADSM client can use services from multiple ADSM servers at the same time.

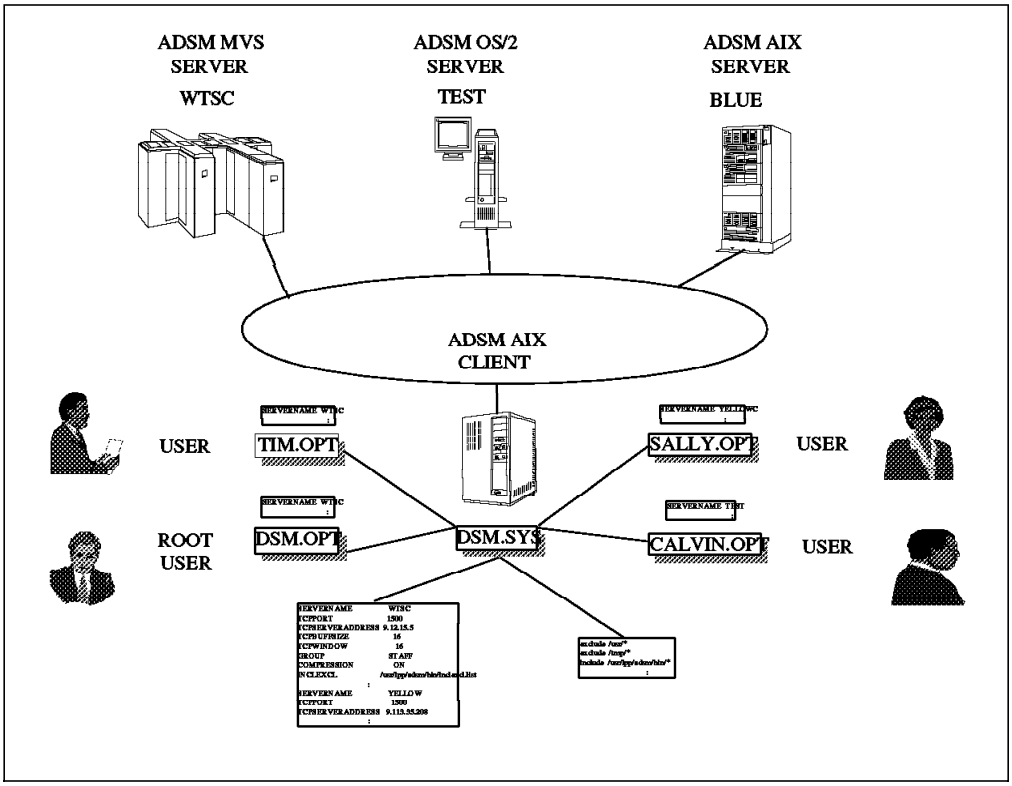


Figure 65. ADSM Client with Multiple ADSM Servers

© Copyright IBM Corp. 1994

5.1.1 Setting Up Options Files for Multiple ADSM Servers

The ADSM AIX client environment has only one client system options file, **dsm.sys**. However, you can define different client user options files, **dsm.opt**. Each client user options file can connect to a different ADSM server. You would then use the **DSM_CONFIG** environment variable to specify the directory path and file name of the client user options file you want to use.

The client system options file, **dsm.sys**, contains groups of statements that define the communications protocols between the ADSM client and each ADSM server. The group of statements for a particular server start with the **servername** option. To connect to more than one ADSM server, you need to define more than one group of these communication options, one group for each ADSM server with which the ADSM client node wants to communicate.

If the communications protocols of the multiple ADSM servers are different, the communications options you define are also different. The ADSM AIX client supports two protocols, TCP/IP and APPC. The example below shows two groups of statements in the client system options file. Both groups of statements use TCP/IP to communicate with the ADSM client.

The first group is for an ADSM AIX server, blue, with the IP address of 9.12.15.5:

```
servername              blue
   commmethod               tcpip
      tcpserveraddress        9.12.15.5
      tcpport                 1500
```

The second group is for an ADSM MVS server with a host name of **merlin**:

```
servername              merlin
   commmethod               tcpip
      tcpserveraddress        merlin
      tcpport                 1500
```

Other options, such as authorization, scheduling, and backup and archive, can be optionally added based on your ADSM environment.

You can request ADSM services from different ADSM servers by defining different client user options files. Then you create two windows with the GUI; each window would be associated with a different client user options file through the **DSM_CONFIG** variable. Thus, you can concurrently connect the AIX system to multiple ADSM servers.

You can request services from the ADSM AIX server by entering **dsmc -servername=blue** from the CLI, while using the client user options file for the ADSM AIX server.

5.1.2 Automating Use of Multiple ADSM Servers

You can automate the startup process of ADSM. This is particularly useful if you have more than one ADSM server that is used from the ADSM client system. To do this you place the startup statements in a command file along with the command to start up the ADSM client. You create a different command file for each ADSM server. Then, you bring up the ADSM client for a particular ADSM server by issuing a command for the appropriate server.

In a sample ADSM implementation on AIX we have three ADSM servers with TCP/IP connections and one server with APPC connection. Thus, we define the following four client user options files:

- **aixtcp.opt**

  contains the entry **servername server_a**.

- **os2tcp.opt**

  contains the entry **servername server_b**.

- **mvstcp.opt**

  contains the entry **servername server_c**.

- **aixappc.opt**.

  contains the entry **servername server_d**.

Here **server_a** is an ADSM/6000 server connected to our client with TCP/IP. **Server_b** is an ADSM/6000 server connected with APPC. **Server_c** is an ADSM/2 server, and **server_d** is an ADSM MVS server, both connected with TCP/IP.

These options files are located in the **/usr/local/adsm/profiles** directory. The permissions for these files are **—rw—r——r——**. The same directory contains four corresponding command files. The permissions for these files are: **—rwxr—xr—x**. The command files and their statements are as follows:

- **aixdsm.cmd**

```
export DSMOPT=/usr/local/adsm/profiles/aixtcp.opt
export DSM_CONFIG=$DSMOPT
export DSM_LOG=$HOME
export DSMG_CONFIG=$DSMOPT
export DSMG_LOG=$HOME
dsm& (for GUI) or dsmc& (for CLI)
```

- **aixdsmap.cmd**

```
export DSMOPT=/usr/local/adsm/profiles/aixappc.opt
export DSM_CONFIG=$DSMOPT
export DSM_LOG=$HOME
export DSMG_CONFIG=$DSMOPT
export DSMG_LOG=$HOME
dsm& (for GUI) or dsmc& (for CLI)
```

- **os2dsm.cmd**

```
export DSMOPT=/usr/local/adsm/profiles/os2tcp.opt
export DSM_CONFIG=$DSMOPT
export DSM_LOG=$HOME
export DSMG_CONFIG=$DSMOPT
export DSMG_LOG=$HOME
dsm& (for GUI) or dsmc& (for CLI)
```

- **mvsdsm.cmd**

```
export DSMOPT=/usr/local/adsm/profiles/mvstcp.opt
export DSM_CONFIG=$DSMOPT
export DSM_LOG=$HOME
export DSMG_CONFIG=$DSMOPT
export DSMG_LOG=$HOME
dsm& (for GUI) or dsmc& (for CLI)
```

To use these groups of commands to start up the connection to one of the ADSM servers, you run the appropriate command file. To make this easy you can link the command files to a simple and short command name:

ln -s /usr/local/adsm/profiles/aixdsm.cmd /usr/bin/aixdsm

ln -s /usr/local/adsm/profiles/aixdsmap.cmd /usr/bin/aixdsmap

ln -s /usr/local/adsm/profiles/os2dsm.cmd /usr/bin/os2dsm

ln -s /usr/local/adsm/profiles/mvsdsm.cmd /usr/bin/mvsdsm

Once these links have been created you can run them by entering:

ADSM/6000 server using TCP/IP

aixdsm

ADSM/6000 server using APPC

aixdsmap

ADSM/2 server using TCP/IP

os2dsm

ADSM MVS server using TCP/IP

mvsdsm

5.1.3 Setting Up Multiple Schedules

Once an environment to use multiple servers is established, you can set up a schedule for automatic backup and archive. You do this in the same way as for a single ADSM server. To start up the schedule from a specific ADSM server, as the root user, you should specify the desired server name in the CLI. For example, to start up the schedule with the ADSM AIX server, you need to enter:

```
dsmc schedule -servername=merlin
```

You can create different sessions to start up all schedules associated with this workstation and the multiple ADSM servers to which it is connected.

5.2 Recovery of the AIX System

System recovery is an important issue for a system administrator. Once an error occurs, system files are damaged, or the whole system crashes, and the system administrator needs to consider how to recover. You can use one of the following methods to recover the AIX system:

- Recovery from diskettes or tape

  The most common and easiest way to recover the system is to use backup diskettes or tapes. The system administrator creates a backup image of the current system environment. You can use **smit** to create a system backup image. When the system needs recovery, change the AIX machine to service mode and insert the diskette or tape to restore the system.

  How often to backup the system depends on business requirements. For critical data you should create system backups frequently to control the magnitude of the damage. Where you store the diskette or tape backups will determine the type of damage from which you will be able to recover. If the diskettes or tapes are stored at the same location as the AIX system, they may be damaged along with the system. A method of keeping both offsite and local system backup images is recommended.

- Recovery using ADSM

  You can use ADSM to recover part of the AIX system environment. Before using ADSM for recovery, you need to recover the AIX system and the ADSM client so that ADSM can be used. To recover the system, you must first install the base operating system of AIX and then install the ADSM client code. ADSM must be tailored before it can be used. The **dsm.sys** and **dsm.opt** options files must have a minimal set of statements to allow connection to the ADSM server.

  Once the ADSM client is connected to the ADSM server, you can use ADSM services to restore or retrieve application files. The advantage of using ADSM for application file recovery is that the backup and recovery time is shorter and the data can be recovered more closely to the status before the system crashed.

- Recovery by reinstallation

  In the worst case you can always recover the AIX system by reinstalling all of its components and then tailoring them to rebuild the environment that was in place before the damage.

5.3 Recovery of the ADSM Client

If application data is damaged, you can restore or retrieve it back to your system from the ADSM server. However, if the application data and the ADSM client are both damaged, you cannot use ADSM services until the ADSM client is recovered. You may want to have a backup version of the ADSM client available to rebuild the damaged ADSM system.

The ADSM client can be damaged in many ways. Thus, there are several ways that the ADSM client can be rebuilt. You could for example:

- Reinstall the ADSM client
- Use a backup image of the ADSM client
- Use multiple file systems and physical disks
- Use another ADSM AIX client
- Use diskettes or tape.

Reinstalling the ADSM client is not discussed in detail. If you have to reinstall the ADSM client, install the ADSM client code exactly as it was initially. The ADSM client and the communications environment to the ADSM server must be tailored in exactly the same way that they were tailored before the damage.

5.3.1 Using a Backup Image of the ADSM Client

The files of the ADSM client code require about 3.1MB of disk space. When you install ADSM on an AIX system, the files reside in the **/usr/lpp/adsm/bin** directory. Figure 66 shows a listing of this directory.

Figure 66. ADSM Client Executable Files

A common way to recover the ADSM client is to create backup images of all ADSM client files shown in Figure 66 to a different directory. To differentiate between these two ADSM clients, the running one is called the production version and the copied one is called the backup version of the ADSM client.

As a root user, copy the files in the default installation directory, **/usr/lpp/adsm/bin**, to the directory in which you want to put the backup ADSM client, for example, the **home/admin/adsm/backup** directory. If the original ADSM files are damaged and they cannot be used for ADSM service, you can copy the backup files of the ADSM client code back to the original directory.

You can also change the ADSM client to use a directory different from the installation directory, **/use/lpp/adsm/bin**. This needs to be done with extreme care but can allow you to use the backup images of the ADSM client directly without having to copy them to the original installation directory. To change the ADSM client to use a different directory do the following:

- Make sure the permissions of the files are not changed.

- Update the directory locations of the bit map files, which are in the ADSM AIXwindows resource file, **/usr/lpp/adsm/bin/dsmx**, to the new directory where the ADSM client backup images are stored.
- Update the symbolic links for the backup ADSM client in the **/usr/bin** directory.
- Ensure that every user of ADSM sets the **DSM_DIR** environment variable to the new backup directory.

After setting up the backup ADSM client environment, use the restore or retrieve function to recover the production version of the ADSM client back to the workstation.

After rebuilding the ADSM client, you can use the restore or retrieve function to recover other damaged application data. Figure 67 shows the environment with two copies of the ADSM client code in separate directories.

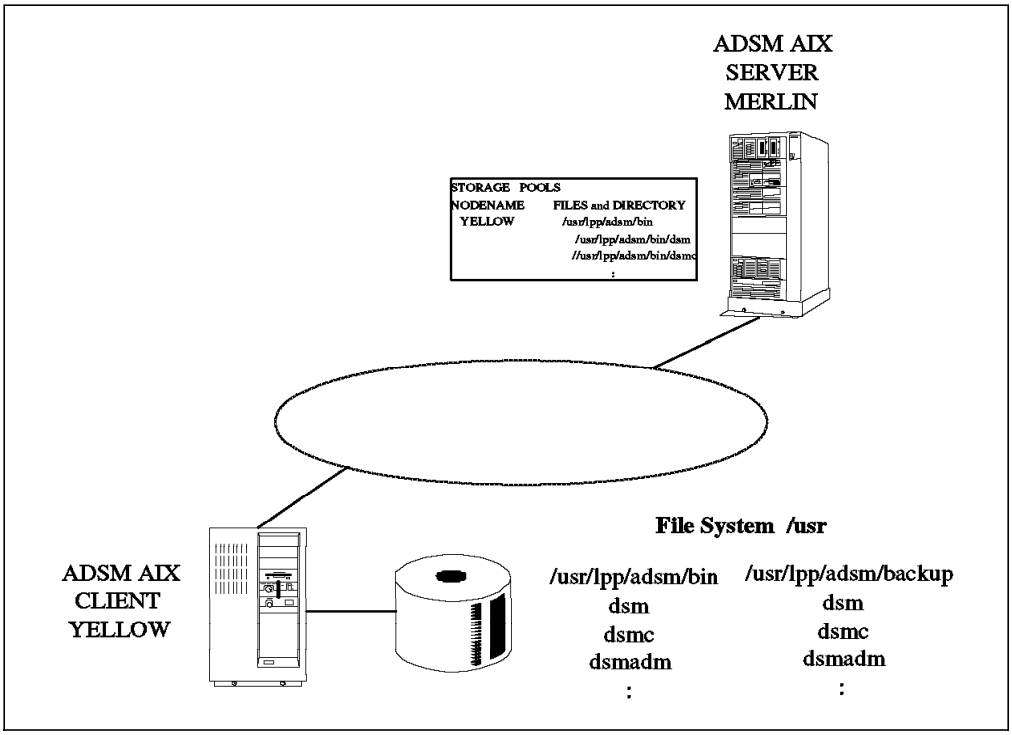


Figure 67. Two Copies of the ADSM Client on One AIX System

5.3.2 Using Multiple ADSM Clients and File Systems and Physical Disks

When the production version and backup version of the ADSM client are both installed in the same file system or hard disk and the file system is damaged, both ADSM clients cannot be used. Another way to create a backup ADSM client environment is to use a separate file system or hard disk on your AIX system, if available. This has the advantage that when the file system or the hard disk of the production version of the ADSM client is damaged, you can use the backup version of the ADSM client in the other file system or hard disk.

To rebuild the production ADSM client environment, copy the backup versions of the ADSM client files back to the production system's file system or hard disk.

Figure 68 on page 104 shows the ADSM client **YELLOW** with two file systems and hard disks.

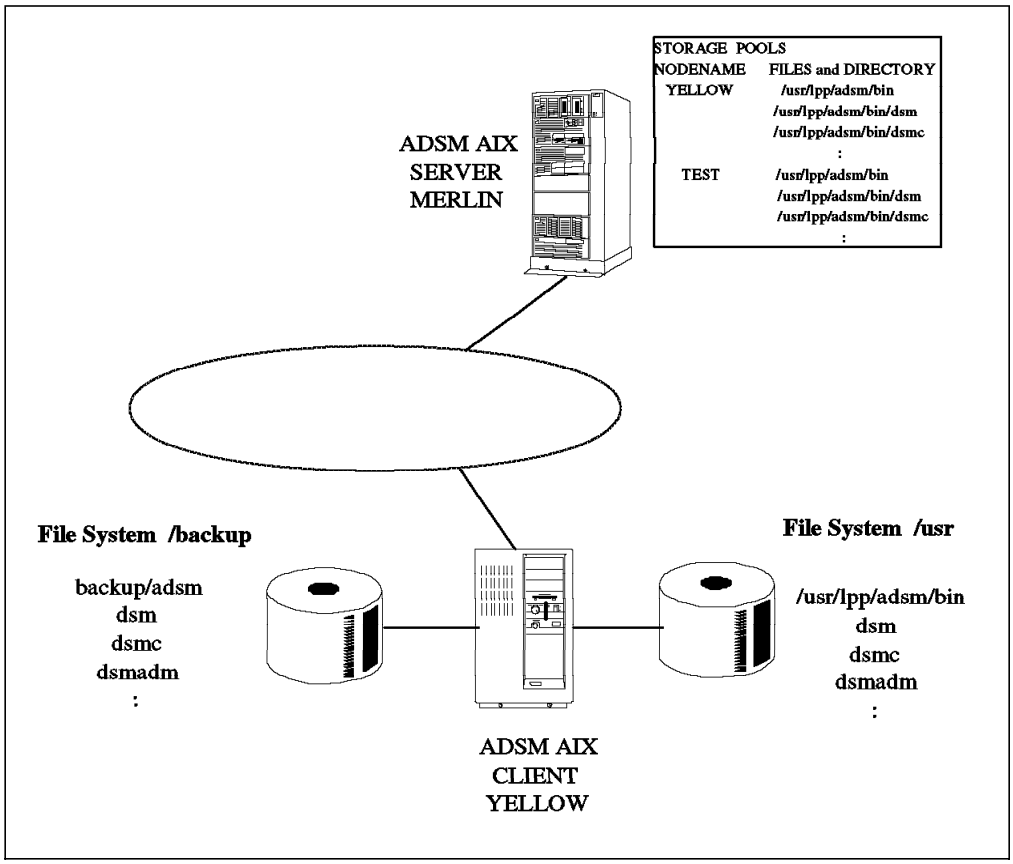


Figure 68. Two Disks on One AIX System

5.3.3 Using Other ADSM AIX Clients

If more than one AIX client node is available in the network, you can use another ADSM client associated with the same ADSM server to recover the disabled ADSM client. Figure 69 on page 105 shows two ADSM clients, **YELLOW** and **TEST**, both connected to the same ADSM server, **MERLIN**. You must ensure that the ADSM client files for **YELLOW** are backed up in the ADSM server and that you have granted access authorization for **YELLOW**′s files to the **TEST** node.

If the ADSM client in the AIX system **YELLOW** is damaged, the ADSM client in the other AIX system, **TEST**, can restore the **YELLOW**′s ADSM client environment. To do this perform the following tasks:

- Use the **TEST** node to restore the ADSM client files of **YELLOW** node.
- Transfer the files to the AIX system, **YELLOW** from **TEST**.
- Restart the ADSM client from the AIX **YELLOW** system.

You could also use the **nodename** parameter on the **TEST** system. This parameter allows the **TEST** sytem to restore **YELLOW**′s files directly. The use of **nodename** does have security implications, which are discussed in 3.2.2.1, “Server and Node Options” on page 44.

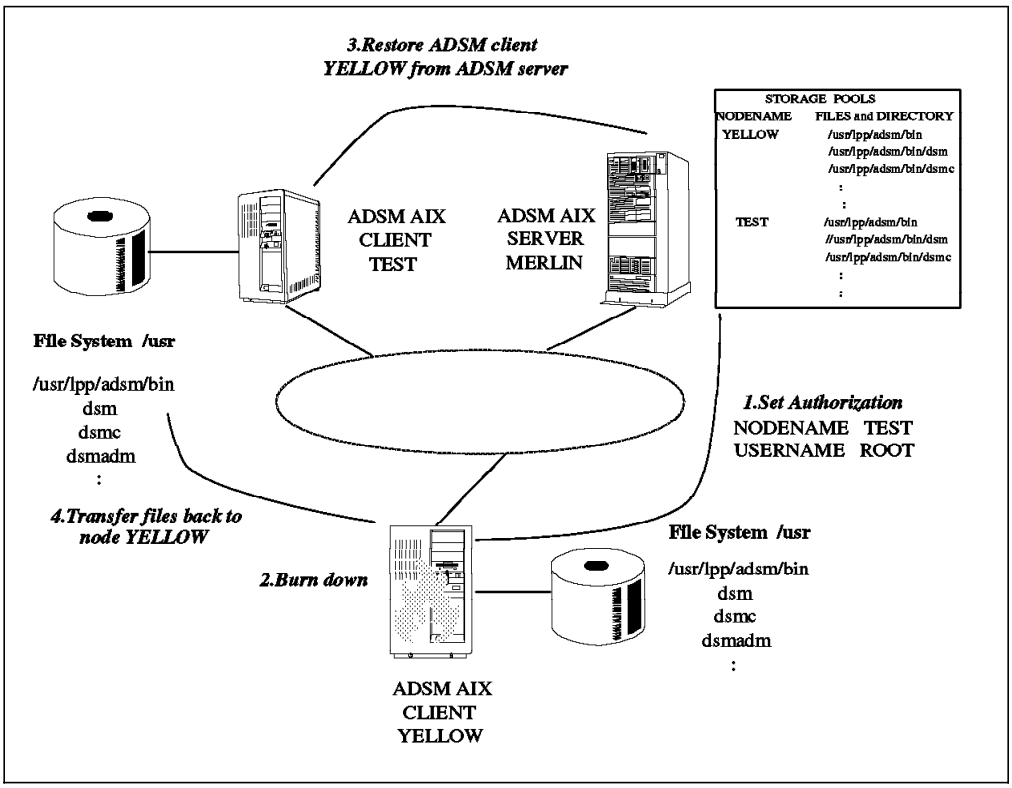


Figure 69. One ADSM Client Backs Up Another ADSM Client

5.3.4 Using Backup to Diskette or Tape

Another way of backing up the ADSM client environment is to use diskettes or tapes to back up the ADSM client files (see Figure 70 on page 106). Use AIX utilities, such as **tar** or **dd**, to back up the production version of the ADSM client files. The advantage of using diskettes or tapes is that they are portable and flexible.

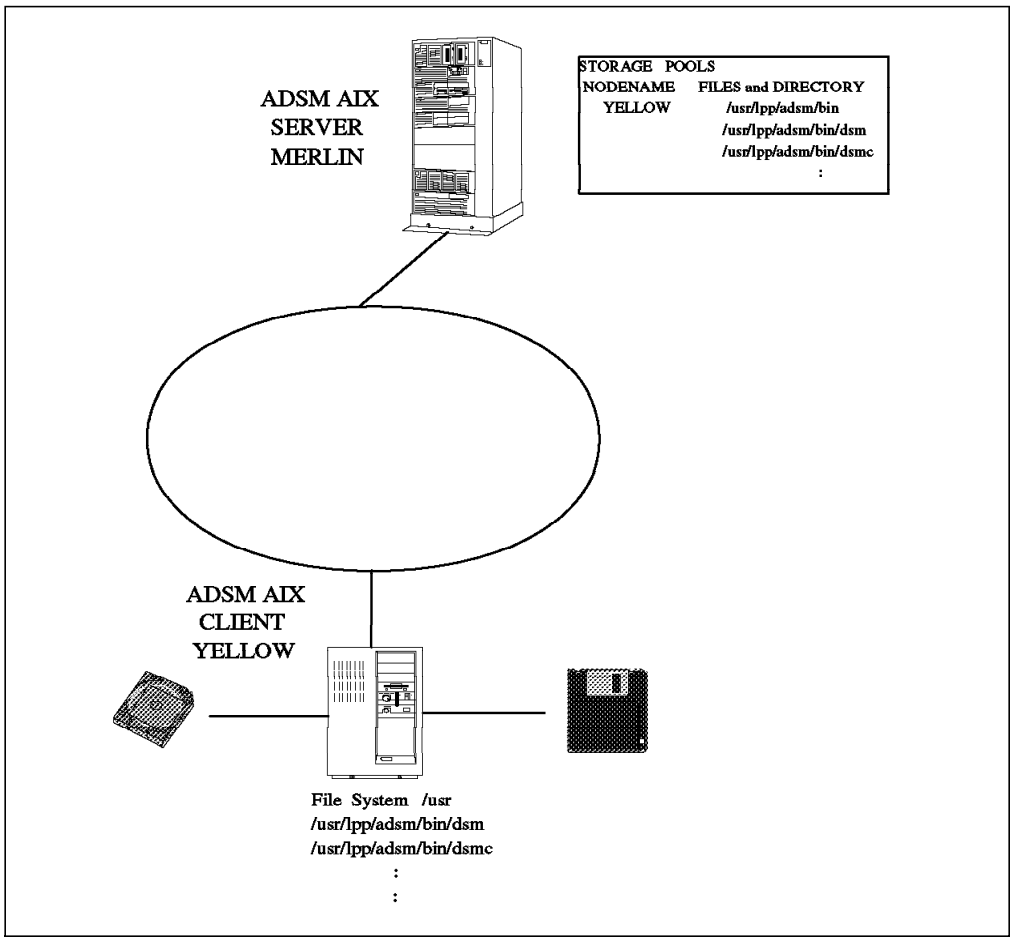


Figure 70. Diskette or Tape Backups for an AIX Client

5.4 Recovery of Applications and User Data

Not all data in the AIX system can be processed by the ADSM client. Users should not request ADSM backup and archive services for the following files because the ADSM client ignores them during backup or archive services:

- Character-specific files
- Block-specific files
- Pipe-specific files.

Also, you should be selective in terms of the data you decide to back up. The number of files and the frequency of backup should be determined carefully because the ADSM client system, the network between the ADSM client and server, and the ADSM server do not have unlimited resources. It would be very bad if every workstation user of the AIX system decided to back up the entire AIX system.

You need to consider how to recover backup and archive files when using the ADSM client. In this section we discuss the following recovery scenarios:

- Loss of files

- Loss of directory
- Loss of file system
- Loss of physical disk.

There are many ways of recovering application and user data. The key reason to use ADSM to back up application and user data is ADSM′s central control. ADSM provides data integrity for the backup version and system assistance during the recovery.

5.4.1 Recovering a File

ADSM can be used to recover a file if it is damaged on a physical disk or if you have deleted it by mistake. If you are the owner of the data, you can recover the lost file from the ADSM server. You can also retrieve the file from the ADSM server if the lost file was archived.

Whether you should use the backup or archive version of the file depends on the point in time to which you want it rebuilt. If your files change frequently, you should use ADSM backup service to back them up to the ADSM server. You should use archive when the file is no longer needed at the AIX system. You can archive the file to the ADSM server and delete it from the workstation. If you need the file again, you retrieve it from the ADSM server.

5.4.2 Recovering a Directory

When you back up a file in a directory, ADSM also backs up the directory. The directory is not backed up or recovered independently of the files in the directory.

If you delete a directory accidentally or the location of the directory is damaged, you need to restore that directory and the files in the directory from the ADSM server. When recovering, make sure you are authorized to the files in the directory and that the destination file system is mounted.

5.4.3 Recovering a File System

You can use different file systems to distinguish different data types or applications. If there is a disk failure or all information in a file system is damaged, you need to recover the entire file system. You must make sure all data is backed up to the ADSM server and that you have the permissions to restore the file system. The procedures to recover a file system are:

- Verify that physical disk space is available and create a file system with either the same or a different name as the backup version.
- Mount this file system.
- Use the ADSM restore function to recover the file system.

5.4.4 Recovering a Physical Disk

The physical disk can be damaged because of machine movement. If this happens, files on that disk are damaged. You can use ADSM services to back up all of the files on a disk. Once a failure occurs, change to another physical disk and use the proper procedures to start up the disk. After the disk is varied on, you can create file systems to restore the backup versions of application or user data from the ADSM server.

5.5 Performance Considerations

Performance of the ADSM AIX system, like all other systems, depends on many factors and variables. These factors include:

- Client hardware type and speed
- Operating system setup
- ADSM server hardware
- ADSM server operating system workload
- ADSM server disk and tape performance characteristics
- Communications controller hardware
- Communications protocol
- Network speed, activity, and reliability
- ADSM workload, including the number and size of files and their frequency of change.

All or any of the above factors can affect ADSM performance. A detailed discussion on performance or tuning for the ADSM environment is beyond the scope of this book. For more detail, consult the *ADSTAR Distributed Storage Manager: Performance Tuning Guide Release 2*.

5.5.1 General Environment

Below are some observations which we have identified during the use of ADSM:

- The more powerful the client, the higher the throughput.
- APPC tends to be faster than TCP/IP, which is much faster than 3270 emulation.
- Ethernets (10Mbit/sec) may not be slower than token rings (16Mbit/sec) because the speed is often limited by the adapter model in either the client or the controller.
- 3172-1 and 3745-210 are about the same speed for backup and restore functions, but the 3745 required much less processor time on the ADSM server.

5.5.2 Compression

Compression of ADSM data is done at the ADSM client. Compression is optional and is defined in the client system options file. The benefits of compression vary in different environments and with different types of data, but in general they are:

- Less disk space consumed: approximately two-thirds lower
- Decreased network utilization: approximately two-thirds lower
- Decreased ADSM server processor time: approximately one-third lower.

The costs for the above benefits are slower backup and restore elapsed times and higher processor utilization at the AIX system. The benefits must be weighed against the costs and, depending on where the bottleneck is in the ADSM environment, trade-offs must be made.

5.5.3 Colocation

Colocation is used in conjunction with backup and migration. The benefit of colocation is that it reserves specific tapes for an ADSM client and places only that client's backup and archive data on the reserved tapes. This minimizes tape mounts and rewinds during file system restore but requires more overall tapes at the ADSM server.

5.5.4 Incremental Backup

Incremental backup processes only files that have changed since the last backup run. The efficiency of incremental backup depends on the percentage of the file system changed. Small percentage changes are backed up incrementally much faster than full selective backups.

The number of backup versions kept also affects the performance and size of the ADSM server's files. If tape colocation is used, performance is improved at the ADSM client during recovery, because fewer tape mounts and rewinds are required for recovery of files for one particular user, but backups across the server take longer and use more tapes.

5.5.5 Migration

Migration performance of data between storage levels on the ADSM server is done at a very fast rate. DASD to DASD migration frequency is affected by space threshold levels and activity. DASD to tape migration is not affected by simultaneous backups; however, the backups are slowed down by migration activity.

5.5.6 Tuning Considerations

Performance in a client/server network is affected by many items. In an AIX environment a rule of thumb for performance for both backup and restore processing is between 512KB to 660KB per second or 1.84GB to 2.38GB per hour. If you use compression, the performance is between 390KB and 464KB per second or 1.40GB or 1.67GB per hour.

Some tuning tips to help are:

- Set packet size to 2000 bytes
  - RU size for VTAM
  - Maximum transmission unit (MTU) size for TCP/IP
- Use large window and buffer sizes
  - 16KB to 32KB
- Check packet sizes on peripheral hardware
  - Adapters for token-ring or Ethernet
  - Parameters for communication controllers
- Allocate multiple DASD volumes for storage pools
  - More than the number of simultaneous backups.

Tips for efficient execution include:

- Use central scheduling to control execution
- Use incremental backups
  - Avoid full backups where possible
- Use client compression
- Use server migration during nonbackup hours
  - Modify migration thresholds after backups are completed
- Use colocation for faster restores of file systems.

Appendix A. Sample ADSM Client Options Files

This appendix contains sample ADSM client options files.

A.1 Client Options File for TCP/IP

The following are sample statements to support TCP/IP as the communications protocol between the ADSM server and client:

```
servername  server_a  * RS/6000 ADSM-Server "blue"
   commmethod         tcpip
   tcpport            1500
   tcpserveraddress   blue.sanjose.ibm.com

servername  server_b  * OS/2    ADSM-Server "victoria"
   commmethod         tcpip
   tcpport            1500
   tcpserveraddress   victoria.sanjose.ibm.com

servername  server_c  * MVS     ADSM-Server "pokmvs"
   commmethod         tcpip
   tcpport            1500
   tcpserveraddress   pokmvs.sanjose.ibm.com
```

A.2 Client Options File for APPC

The following are sample statements to support APPC as the communications protocol between the ADSM server and client:

```
servername  server_d  * AIX     ADSM-Server "merlin"
   commmethod          snalu6.2
   symbolicdestination merlin
   cpicbuffersize      31
```

A.3 Client Options File for Authorization

The following are sample statements to support client node authorization:

```
 servername  server_a  * RS/6000 ADSM-Server "blue"
   commmethod          tcpip
   tcpport             1500
   tcpserveraddress    blue.sanjose.ibm.com
   passwordaccess      prompt
   groups              adsm
   users               sally caroline walter
```

© Copyright IBM Corp. 1994

```
servername  server_c  * MVS     ADSM-Server "pokmvs"
  commmethod          tcpip
  tcpport             1500
  tcpserveraddress    pokmvs.sanjose.ibm.com
  passwordaccess      generate
  mailprog            /usr/bin/xsend root
  groups              system adsm
```

A.4 Client Options File for Backup and Archive

The following are sample statements to support backup and archive processing:

```
servername  server_a  * RS/6000 ADSM-Server "blue"
  commmethod          tcpip
  tcpport             1500
  tcpserveraddress    blue.sanjose.ibm.com
  passwordaccess      prompt
  groups              adsm
  users               sally caroline walter
  compression         on
  incexcl             /adsm/adsm/backup.excl

servername  server_c  * MVS     ADSM-Server "pokmvs"
  commmethod          tcpip
  tcpport             1500
  tcpserveraddress    pokmvs.sanjose.ibm.com
  passwordaccess      generate
  mailprog            /usr/bin/xsend root
  groups              system adsm
  dirmc               Standard
  compression         on
  incexcl             /adsm/adsm/archive.excl
```

A.5 Client Options File for Scheduling

The following are sample statements to support scheduling.

```
servername  server_a  * RS/6000 ADSM-Server "blue"
  commmethod          tcpip
  tcpport             1500
  tcpserveraddress    blue.sanjose.ibm.com
  passwordaccess      prompt
  groups              adsm
  users               sally caroline walter
  compression         on
  incexcl             /adsm/adsm/backup.excl
  schedlogname        dsmsched.log
  queryschedperiod    12
  schedmode           polling
```

```
servername  server_c  * MVS     ADSM-Server "pokmvs"
  commmethod          tcpip
  tcpport             1500
  tcpserveraddress    pokmvs.sanjose.ibm.com
  passwordaccess      generate
  mailprog            /usr/bin/xsend root
  groups              system adsm
  dirmc               Standard
  compression         off
  incexcl             /adsm/adsm/archive.excl
  schedlogname        dsmsched.log
  queryschedperiod    12
  schedmode           prompted
```

A.6 Include File Statement

The following sample statement supports include/exclude tailoring for backup and archive processing:

```
include /home/proj2/test/* finance
```

Appendix B. Sample ADSM MVS Server APPC Definitions

This appendix lists the VTAM definitions that are required to establish an APPC connection between an ADSM AIX client and an ADSM/MVS server.

B.1 VTAM Start List

The VTAM start list on an MVS system is usually in SYS1.VTAMLST in a member call ATCSTRxx:

```
SSCPID=06,NOPROMPT,
CONFIG=00,LIST=00,MAXSUBA=31,SUPP=NOSUP,
HOSTSA=6,
SSCPNAME=SJA,
NETID=USIBMSC,                                          & 15
HOSTPU=HOST06PU,
CRPLBUF=(208,,15,,1,16),
IOBUF=(100,384,19,,1,20),
LFBUF=(104,,0,,1,1),
LPBUF=(64,,0,,1,1),
SFBUF=(163,,0,,1,1),
WPBUF=(78,,0,,1,1)
```

B.2 VTAM Application Major Node

The following is the VTAM application major node definition for the ADSM server on MVS:

```
ADSM      VBUILD TYPE=APPL
*
*-------------------------------------------------------------------*
*   ADSMLU DEFINITION FOR ADSM                                      *
*                                                                   *
*   ADSM 1.1.0                                                      *
*-------------------------------------------------------------------*
*
MERLIN   APPL  ACBNAME=SCADSMLU
               APPC=YES,
               PARSESS=YES,
               SRBEXIT=YES,
               DMINWNL=3,
               DMINWNR=3,
               DSESLIM=6,
               AUTOSES=3,
               DRESPL=NALLOW,
               DDRAINL=NALLOW,
               EAS=509,
               DLOGMOD=PERF1920
               MODETAB=MTAPPC,
               SECACPT=ALREADYV,
```

© Copyright IBM Corp. 1994

```
                VERIFY=NONE,
                VPACING=8
```

B.3 VTAM Logmode Table

Below is the JCL for the job to create the VTAM logmode entry used for ADSM. It creates a logmode entry called PERF1920 in the MTAPPC logmode table.

```
//TIM1     JOB (999,POK),'MTAPPC',CLASS=A,REGION=4096K,
//    MSGCLASS=T,MSGLEVEL=(1,1),NOTIFY=&SYSUID
//STEP1 EXEC ASMHCL,PARM.L='LIST,REUS'
//C.SYSLIB DD  DSN=SYS1.SISTMAC1,DISP=SHR
//         DD  DSN=SYS1.MACLIB,DISP=SHR
//C.SYSIN  DD  *
MTAPPC   MODETAB
*********************************************************************
*        LOGMODE TABLE ENTRY FOR APPC CONNECTION.                   *
*********************************************************************
PERF1920 MODEENT LOGMODE=PERF1920
                FMPROF=X'13',
                TSPROF=X'07',
                PRIPROT=X'B0',
                SECPROT=X'B0',
                COMPROT=X'D0B1',
                RUSIZES=X'8989',
                PSERVIC=X'060200000000000000000300'
END      MODEEND
         END
/*
//L.SYSLMOD  DD  DSN=SYS1.LOCAL.VTAMLIB(MTAPPC),DISP=SHR
```

The RUSIZES statement defines the maximum inbound and outbound RU size that can be negotiated for use with this logmode. The two bytes, 8989, are the maximum inbound and outbound RU sizes expressed as: 8 multiplied by 2 to the power of 9 (8 x 2•) for both inbound and outbound sizes. This equates to 4096 bytes inbound and outbound RU sizes.

B.4 VTAM Workstation Definitions

The sample VTAM definitions for ADSM AIX client systems attached through 3745 and 3174 gateways are presented below.

B.4.1 VTAM 3745 Switched Major Node Definition

The following 3745 switched major node definition is an example of one working configuration. This definition could also be used for a 3172 gateway.

```
SWSJ001  VBUILD  TYPE=SWNET,
               MAXGRP=1,
               MAXNO=1
*
YELLOW   PU    ADDR=01,
               CPNAME=SJA2024I,
               ANS=CONT,DISCNT=NO,
               IRETRY=NO,ISTATUS=ACTIVE,
               MAXDATA=4105,MAXOUT=7,
               MAXPATH=1,
               PUTYPE=2,SECNET=NO,
               MODETAB=MTAPPC,DLOGMOD=PERF1920,
               USSTAB=USSRDYN,
               PACING=8,VPACING=8
*
SJA2024I LU    LOCADDR=0
*
```

B.4.2 VTAM Cross Domain Definition

The above switched major node definition was defined on a VM VTAM system, separate from the MVS system where the ADSM server resided. The following cross domain resources were defined to enable the independent LU type 6.2 sessions to connect to the MVS VTAM system:

```
          VBUILD TYPE=CDRSC
          NETWORK NETID=USIBMSC
 ********************************************************************
 *                                                                  *
 *   CROSS DOMAIN RESOURCES ON WTSCPOK (LU 6.2)                     *
 *                                                                  *
 ********************************************************************
 *
 SJA2024I CDRSC CDRM=SCG20,
                ISTATUS=ACTIVE
```

B.4.3 VTAM 3174 Local Node Definitions

Another communications gateway that can be used for APPC connectivity is a 3174. A 3174 is defined in VTAM differently from a 3745. Below is an example of a 3174 local node definition for a 3174 supporting independent LU type 6.2.

This sample differs in some parameters from the previous 3745 definition. It also has different PU and LU names for ADSM's APPC sessions. The PU name of PU3174 is used rather than YELLOW. The LU name of 3174ILU1 is used rather than SJA2024I.

```
DSM3174  VBUILD  TYPE=LOCAL,
*
PU3174   PU    CUADDR=2A0,
               PUTYPE=2,
               XID=YES,
```

```
                DISCNT=NO,
                ISTATUS=ACTIVE,
                MAXBFRU=9,
                PACING=8,
                VPACING=8,
                SECNET=NO,
                USSTAB=USSTB7E,
                MODETAB=MTAPPC,
                DLOGMOD=PERF1920
*
* INDEPENDENT LUs
*
3174ILU1 LU    LOCADDR=0
*
* DEPENDENT LUs
```

Index

Numerics

3172 55, 116
3174 55, 117
3745 55, 116

A

administrative client 8, 38, 94
administrator
  See storage administrator
ADSM
  hardware requirements 37
  software requirements 37
  startup 83, 84, 99, 100
advanced program-to-program communications
  See APPC
AFS 28
AIX
  ADSM support 37
  AFS
    See AFS
  CD-ROM file system
    See CD-ROM file system
  database systems
    See database systems
  environment variable 44, 98, 102
  extensions to UNIX 29, 30
  file support 11, 84, 86
  file system 27—29, 84
  industry UNIX standards 21
  Internet address 48, 49
  JFS
    See JFS
  logical volume 27
  logical volume storage 25—27
  LVM
    See LVM
  NFS
    See NFS
  ODM
    See ODM
  partition 27
  physical volume 27
  root user 24, 31, 32, 40, 56, 84, 95, 100, 102
  security 30—32
  server
    See server
  SMIT 22, 30, 34, 38, 39, 47, 48, 56—77, 78
  system recovery 101
  system structure 21—25
  user interface 34, 36
  volume group 27
AIX SNA Server/6000
  ADSM support 33, 37
AIX SNA Server/6000 *(continued)*
  APPC mode information 71—73
  APPC parameters 53, 54
  APPC side information 73—75
  control point profile 55—59
  definition 33
  local LU type 6.2 profile 56
  partner APPC profile 67—71
  performance 80, 81
  save configuration 77, 78
  start configuration 78
  token-ring link station profile 55, 63—66
  token-ring SNA DLC profile 55, 59—63, 66
  verify configuration 76, 77
AIXwindows 34, 36, 37, 83
alternate path
  See cross-directory
Andrew File System
  See AFS
API 8
aping command 79, 80
APPC
  ADSM support 5, 37
  aping command 79, 80
  associated VTAM parameters 52—54
  client system options file 41, 79, 81, 111
  configuring for ADSM 55—75
  control point profile 55—59
  definition 5, 33, 52—54
  functions 33
  local LU type 6.2 profile 56
  mode information 71—73, 80, 81
  partner APPC profile 67—71
  performance 80, 81
  problem determination 79, 80
  sample VTAM definitions 115—117
  save configuration 77, 78
  side information 41, 73—75
  start configuration 78
  system requirements 54, 55
  token-ring link station profile 55, 63—66
  token-ring SNA DLC profile 55, 59—63, 66
  trace 79, 80
  verify configuration 76, 77
application client 8
application programming interface
  See API
archive
  client system options file 19, 42
  client user options file 45, 46, 112
  definition 2, 3
  exclude 19
  file selection 86, 87
  functions 11, 12

© Copyright IBM Corp. 1994

archive *(continued)*
include 19
usage 91, 92
authentication 9, 84
authorization 9, 42, 83, 93, 94, 111

B

backup
active versions 9
client system options file 19, 42, 87
client user options file 45, 46, 112
definition 2, 3
exclude 19
file selection 86, 87
functions 7, 9, 10, 11, 12
inactive versions 9
include 19
incremental 9, 10, 16, 17, 19, 45, 84, 85
selective 9, 10, 45, 88, 89
versions 2, 3, 9, 10, 16, 85—87
backup/archive client 7, 38, 83
bind 52, 53, 80
buffering 50, 51, 80, 81, 110

C

CD-ROM file system 28
central scheduling
See scheduling
CLI 7, 37, 83—85, 87, 89, 91, 92—94
client
definition 1, 3
dsm.opt file 18—20, 40, 44—46, 49, 83, 86, 98, 99, 104, 112
dsm.sys file 18, 19, 40—43, 50, 51, 79, 81, 87, 95, 98, 111
functions 7
installation 38, 39
multiple ADSM servers 97—100
recovery 101—103
registration 8
tailoring 40—46
client system options file
See dsm.sys file
client user options file
See dsm.opt file
client/server 1, 2, 3, 9, 33
collision 10
colocation 109, 110
command interpreter
See shell
command line interface
See CLI
communications gateway
See gateway
communications protocol
ADSM client/server 5, 6
APPC
See APPC
communications protocol *(continued)*
client system options file 19, 40, 41
client user options file 19
harware support 32
TCP/IP
See TCP/IP
compression 11, 19, 42, 109, 110
connectivity
See communications protocol
copy group
archive 15, 16, 85, 86
backup 15, 16, 85, 86
definition 14—16
DESTINATION 16
FREQUENCY 16
MODE 17
RETEXTRA 16
RETONLY 16
SERIALIZATION 17
VERDELETED 16
VEREXISTS 16
cross-directory
restore 90
retrieve 93
cross-domain network 59, 70, 71, 117
cross-platform
restore 12
retrieve 12
cross-user
restore 12
retrieve 12

D

daemon
See process
data compression
See compression
data link control 56
data security
See security
database systems 28, 29
DB2/6000
See database systems
directory 9, 10, 19, 28, 29, 31, 32, 42, 45, 86—88, 90, 92, 98, 99, 102, 107
disaster recovery 3, 97
dsm.opt file
archive options 45, 46
backup options 45, 46
commmethod 49
dateformat 44
definition 18—20
domain 19, 44, 45
inclexcl 86
language 44
nodename 44, 104
numberformat 44
passwordaccess 83

dsm.opt file *(continued)*
quiet 45
replace 45
restore options 45, 46
retrieve options 45, 46
samples 112
scrolllines 45
scrollprompt 45
servername 44, 99
subdir 45
subdirectories 19
tailoring 40
tapeprompt 46
tcpport 49
tcpserveraddress 49
timeformat 44
user interface options 44, 45
verbose 45
dsm.sys file
archive options 42
authorization options 42
backup options 42
changingretries 42
commmethod 41, 79
communications options 40, 41
compression 42
cpicbuffersize 41, 81
cpicmodename 41
definition 18, 19
dirmc 42
group 42
inclexcl 42
mailprog 42
maxcmdretries 43
partnerluname 41
passwordaccess 42
queryschedperiod 43
retryperiod 43
samples 111
schedlogname 43
schedmode 43
scheduling options 43
servername 40, 98
symbolicdestination 79
symbolicdestinationname 41
tailoring 40
tcpbuffsize 41, 50, 51
tcpclientaddress 43
tcpclientport 43
tcpport 41
tcpserveraddress 41
tcpwindowsize 41, 50, 51
tpname 41
users 42
virtualmountpoint 42

E

Ethernet 32
exclude 9, 10, 19, 42, 83, 84, 86, 87
export 3

F

file support 11, 84, 86

G

gateway 33, 48, 54, 55, 66
graphical user interface
See GUI
GUI 7, 8, 34, 37, 83, 84, 87—93

I

import 3
include 9, 10, 15, 19, 42, 83, 84, 86, 87, 113
incremental backup 9, 10, 16, 17, 19, 45
INFORMIX-Online
See database systems
Interconnect Controller Program 55
Internet address 48, 49
Internet protocol
See TCP/IP

J

JFS 28
journaled file system
See JFS

K

kernel 22, 30

L

LAN 32
local area network
See LAN
logical unit
See LU
logical volume manager
See LVM
logmode table 53, 71—75, 80, 116
LU
definition 52, 53
dependent 33, 52, 54
independent 33, 52, 54—56, 59
partner LU 53, 56, 67—79
type 6.2 33, 52, 54—56, 59, 67
LVM 26, 30

M

management class 12, 14, 15, 83, 85—87

N

NCP 55, 80, 81
Network Control Program
  See NCP
network file system
  See NFS
network name 53, 59
NFS 28
node name 2, 8, 44, 48, 58, 63, 83

O

object data manager
  See ODM
ODM 30
online documentation 84
online help 84
Oracle
  See database systems

P

pacing 80, 81
packet inter-network groper
  See PING
partner LU
  See LU
password 8, 9, 44, 83
performance
  ADSM server 108—110
  APPC 80, 81
  buffering 50, 51, 80, 81
  client 108—110
  hardware 108, 109
  network 108, 110
  TCP/IP 50, 51
  workload 109, 110
permissions 31, 32, 83, 87, 99, 102
physical unit
  See PU
PING 49
policy domain 12, 13, 14, 85
policy management 3, 10—16, 85—87
policy set 12, 14, 85
problem determination
  APPC 79, 80
  TCP/IP 49
process
  background 24
  daemon 24
  definition 22
  defunct 24
  foreground 23, 24
  parent process 23
process *(continued)*
  PID 23, 25
  zombie 24
process identification number
  See process, PID
PU 53—56
PU type 2.0
  See PU
PU type 2.1
  See PU

R

RACF 9
recall 3
recovery
  ADSM client from another remote ADSM client 104
  ADSM client from diskette or tape 105
  ADSM client using a backup copy 102, 103
  ADSM client using multiple hard disks 103
  AIX system by reinstallation 101
  AIX system from diskette or tape 101
  AIX system using ADSM 101
  client 101—103
  data 3
  directories 106, 107
  disaster 3
  disk 3
  entire physical disk 106, 108
  file selection 106
  file system 106, 107
  files by archive copies 106, 107
  files by backup versions 106, 107
registration
  closed 8
  open 8
response unit
  See RU
restore
  client user options file 19, 45, 46
  collision 10
  cross-directory 10, 90
  cross-platform 12
  cross-user 12
  definition 2
  functions 7, 9—12
  usage 89—91
retrieve
  by date 11, 93
  by description 3, 11, 92, 93
  client user options file 19, 45, 46
  cross-directory 93
  cross-platform 12
  cross-user 12
  definition 3
  functions 7, 11, 12
  usage 93

RISC System/6000 32, 37
root user
See AIX
RU 80, 81, 110, 116

S

scheduling
client polling 18
client system options file 19, 43, 95
client user options file 112
definition 12, 17, 18
multiple ADSM servers 100
query 95
server prompted 18
startup 95, 96
usage 94—96
SDLC 32
security
ADSM functions 8
client system options file 42, 83
file 30—32, 83
permissions 31, 32
selective backup 9, 10, 45
server
ADSM 1, 3, 18, 40—42, 44, 46, 49, 51—55, 58, 63—75, 80, 81, 83, 86, 94, 95, 106, 115—117
AIX 1
client system options file 44
configurations 5
definition 1, 3
functions, ADSM 6
multiple ADSM servers 97—100
shell 22, 23
sliding window 50, 51
SMIT 22, 30, 34, 38, 39, 47, 56—77, 78
SNA 5, 33, 52—75
software vital product data
See SWVPD
space management 3
spawning 23
SRC 30
storage administrator 3, 7—10, 12, 13, 18, 83, 85—87, 94
storage hierarchy 6
storage pools 6, 16
SWVPD 30
Sybase
See database systems
synchronous data link control
See SDLC
system management interface tool
See SMIT
system resource controller
See SRC
Systems Network Architecture
See SNA

T

TCP/IP
ADSM support 5, 37
client system options file 41, 43, 111
configuring for ADSM 47—49
definition 5, 33
functions 33
performance 50, 51
PING 49
problem determination 49
scheduling options 18, 43
system requirements 46
trace 49
token-ring 32, 47, 48, 54—66
trace 49, 79, 80
transmission control program
See TCP/IP

U

UNIX
See AIX
user interface 7, 20, 34, 36, 44, 45
userid 31, 32

V

versions
See backup
vital records 2, 3
VTAM 52—59, 70—75, 79—81, 115—117

W

wildcards 10, 11, 88, 89, 91, 93
workload 108
workstation interface 20

ITSO Technical Bulletin Evaluation RED000

Getting Started with ADSM AIX Clients

Publication No. GG24-4243-00

Your feedback is very important to help us maintain the quality of ITSO Bulletins. **Please fill out this questionnaire and return it using one of the following methods:**

- Mail it to the address on the back (postage paid in U.S. only)
- Give it to an IBM marketing representative for mailing
- Fax it to: Your International Access Code + 1 914 432 8246
- Send a note to REDBOOK@VNET.IBM.COM

Please rate on a scale of 1 to 5 the subjects below.
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction	____		
Organization of the book	____	Grammar/punctuation/spelling	____
Accuracy of the information	____	Ease of reading and understanding	____
Relevance of the information	____	Ease of finding information	____
Completeness of the information	____	Level of technical detail	____
Value of illustrations	____	Print quality	____

Please answer the following questions:

a) If you are an employee of IBM or its subsidiaries:

Do you provide billable services for 20% or more of your time? Yes____ No____

Are you in a Services Organization? Yes____ No____

b) Are you working in the USA? Yes____ No____

c) Was the Bulletin published in time for your needs? Yes____ No____

d) Did this Bulletin meet your needs? Yes____ No____

If no, please explain:

_____

_____

What other topics would you like to see in this Bulletin?

_____

_____

What other Technical Bulletins would you like to see published?

_____

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

_____ _____
Name Address

_____ _____
Company or Organization

_____ _____
Phone No.

Cut or Fold Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE NECESSARY IF MAILED IN THE UNITED STATES

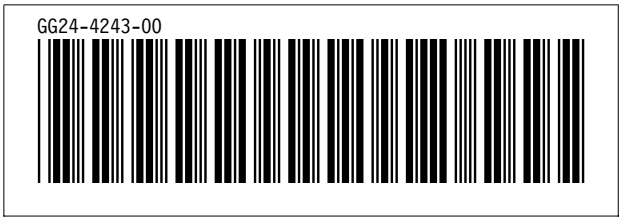
BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM International Technical Support Organization
Department 471, Building 070B
5600 COTTLE ROAD
SAN JOSE CA
USA 95193-0001

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold Along Line

Printed in U.S.A.