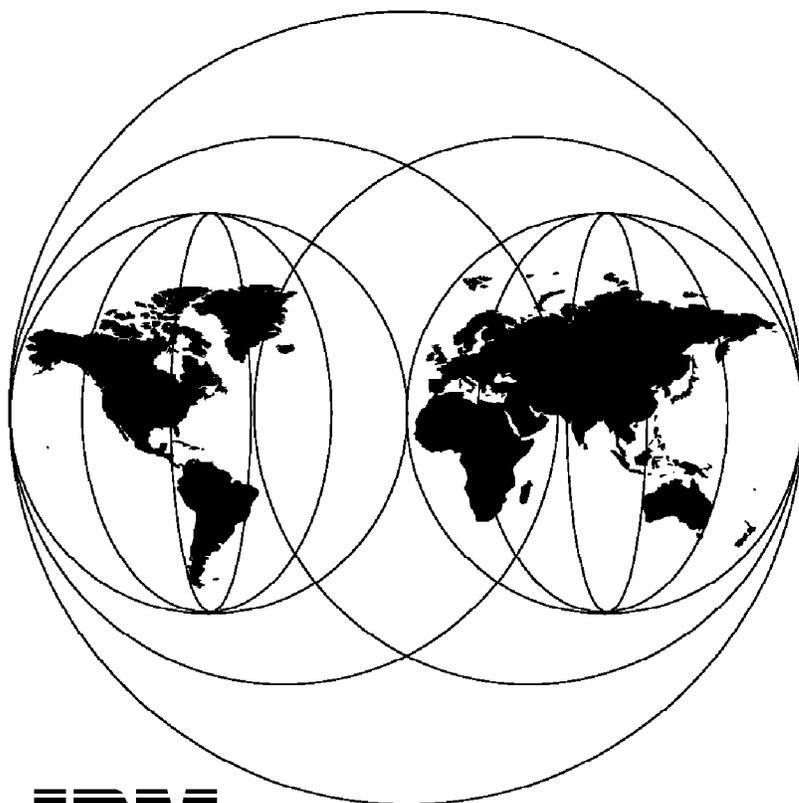


Inside OS/2 Warp Server, Volume 2: System Management, Backup/Recovery and Advanced Print Services

December 1996



**International Technical Support Organization
Austin Center**

IBML

International Technical Support Organization SG24-4702-00

**Inside OS/2 Warp Server, Volume 2: System Management,
Backup/Recovery and Advanced Print Services**

December 1996

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix B, "Special Notices" on page 333.

First Edition (December 1996)

This edition applies to OS/2 Warp Server Version 4 and OS/2 Warp Server Advanced for use with the OS/2 Version 3 Operating System included in the above products.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. JN9B Building 045 Internal Zip 2834
11400 Burnet Road
Austin, Texas 78758-3493

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 1996. 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.

Contents

Figures	ix
Tables	xv
Preface	xvii
How This Redbook Is Organized	xviii
The Team That Wrote This Redbook	xviii
Comments Welcome	xx
Chapter 1. System Management Services	1
1.1 Overview and Concepts	1
1.1.1 What is Systems Management?	1
1.1.2 IBM's SystemView Model and OS/2 Warp Server	2
1.2 SystemView in Warp Server Components	3
1.2.1 SystemView Manager	4
1.2.2 SystemView OS/2 Client	5
1.2.3 SystemView DOS/Windows Client	6
1.3 Installation and Configuration	6
1.3.1 Hardware and Software Prerequisites	7
1.3.1.1 SystemView Manager Prerequisites	7
1.3.1.2 SystemView Client Prerequisites	8
1.3.1.3 Communication Protocols	9
1.3.1.4 NetBIOS Resources	9
1.3.1.5 Summary of Hard Disk Usage	10
1.3.2 SystemView Manager Installation	10
1.3.2.1 Using the OS/2 Warp Server Integrated Installation	11
1.3.2.2 Using SystemView INSTALL	15
1.3.3 SystemView Client Installation	15
1.3.3.1 Using the OS/2 Warp Server Client Installation	16
1.3.3.2 SystemView INSTALL for OS/2	17
1.3.3.3 Using SystemView INSTALL for Windows	18
1.3.4 Configuring the SystemView Manager	19
1.3.5 Configuring the OS/2 Client	24
1.3.6 Installation and Maintenance Utility	26
1.3.7 Product Removal Considerations (Deinstallation)	28
1.4 SystemView Architecture	28
1.5 Getting Started	30
1.6 Managing Client Systems in the Network	31
1.6.1 Creating a Group	31
1.6.2 Using Discovery Filters	33
1.6.3 Discovering Systems in a System Group	34
1.6.4 Accessing Remote Machines	37
1.7 Implementing Security	40
1.7.1 Configuring the Security Manager	40
1.7.1.1 Setting Up the Incoming User ID/Password on a Manager	40
1.7.1.2 Setting Up the Outgoing User ID/Password on a Manager	41
1.7.1.3 How the Password Checking is Done	42
1.7.1.4 Service Execution Alerts	43
1.8 Inventory Management	43
1.8.1 System Information Tool	44
1.8.2 Software Inventory	46

1.8.2.1	Software Information	49
1.8.2.2	Dictionary File	50
1.8.2.3	Modifying Records in a Dictionary File	50
1.8.3	System Profile	55
1.9	Performance Management	58
1.9.1.1	System Monitor Service Window	60
1.9.1.2	Monitor Context Menus	61
1.9.1.3	System Monitor Notebooks	63
1.9.1.4	System Monitor Tips	66
1.10	Operations Management	67
1.10.1	Monitoring Critical Files	67
1.10.2	ECC (Error Checking and Correction) Memory Setup	69
1.10.3	RAID Administration: RAID Manager	70
1.10.3.1	Viewing RAID Device Information	71
1.10.3.2	RAID Device Management	73
1.10.3.3	RAID Adapter Management	73
1.10.3.4	RAID Logical Drive Management	74
1.10.3.5	Supported RAID Adapters	75
1.10.4	File Transfer	75
1.10.4.1	File Transfer Tips	75
1.10.4.2	Local and Remote File Selection and Handling	76
1.10.4.3	Local and Remote Directory Selection and Handling	77
1.10.4.4	Disabling Data Compression	77
1.10.5	Alert Manager	77
1.10.5.1	Information on Individual Alerts	79
1.10.5.2	Configuring Actions	80
1.10.5.3	Error Conditions	85
1.10.6	Power-On Error Detect	85
1.10.7	Predictive Failure Analysis	86
1.10.7.1	Predictive Failure Analysis Window	86
1.10.7.2	PFA Options for Drive Window	88
1.10.8	Scheduling Events	89
1.10.9	System Partition Access	90
1.10.9.1	Available System Partition Access Actions	91
1.10.10	Process Management	92
1.10.10.1	Gathering Process Information	92
1.10.10.2	Running Commands	93
1.10.10.3	Halting Processes	93
1.10.10.4	Process Alerts	94
1.10.11	Managing Systems Connected by Modem	95
1.10.12	Remote Control Functions	96
1.10.13	Remote Session	96
1.10.14	Remote Workstation Control	98
1.10.14.1	Comparison of SystemView Remote Workstation Control and DCAF Functions	100
1.10.14.2	SystemView in Warp Server Remote Workstation Control Configuration	102
1.10.14.3	Change Keystrokes Mode Function	102
1.10.14.4	Session State	103
1.10.15	Capturing a Managed System's Screen Image with Screen View	104
1.11	SystemView Agent for OS/2	105
1.11.1	SystemView Agent, DMI and DPI	105
1.12	License Management	107
1.12.1	Licensing Models	108
1.12.1.1	Nodelocked Licensed Products	108

1.12.1.2	Server-Based Licensed Products	109
1.12.2	Security Levels	111
1.12.2.1	Summary of License Models	112
1.12.3	Planning for SystemView License Management	112
1.13	Coexistence and Interoperability	114
1.13.1	NetFinity	115
1.13.1.1	Coexistence	116
1.13.2	License Management	116
1.13.3	NetView Distribution Manager/2 (NetView DM/2)	116
1.13.3.1	Coexistence	117
1.13.3.2	Migration	117
1.13.4	Distributed Console Access Facility (DCAF)	118
1.13.4.1	Interoperability	118
1.13.4.2	Coexistence and Migration	119
1.14	Summary of the SystemView in Warp Server Functions	120
1.15	Related Publications	121
Chapter 2.	Software Distribution Considerations	123
2.1	Overview and Concepts	123
2.1.1	Installation Modes	123
2.1.1.1	Attended Installation	123
2.1.1.2	Lightly Attended Installation	123
2.1.1.3	Unattended Installation	123
2.1.2	Configuration Installation and Distribution (CID)	124
2.1.3	Redirected Installation	124
2.1.3.1	SRVIFS	125
2.1.3.2	LAN Server	125
2.1.3.3	Novell NetWare	125
2.1.3.4	TCP/IP NFS	125
2.1.4	CASSETUP	126
2.1.5	SystemView in Warp Server Software Distribution	126
2.1.6	Summary Table	127
2.2	Using a Redirected Drive	127
2.2.1	Methods for Obtaining Redirected Drives	128
2.2.1.1	Use of SRVIFS	128
2.2.1.2	Using LAN Server	137
2.2.1.3	SRVIFS and LAN Server Comparison	138
2.2.1.4	Using TCP/IP NFS Server Functions	138
2.2.1.5	Using NetWare as a Code Server	142
2.2.2	Installing Operating Systems Using Redirected Drives	143
2.2.2.1	Installation of DOS, Windows and DOS LAN Services Using LAN Server 5.0	143
2.2.3	Non-CID-Enabled Applications	144
2.2.4	CID-Enabled Applications	144
2.3	Using CASSETUP	144
2.3.1	Setting Up a Code Server	145
2.3.1.1	Code Server Directory Structure	145
2.3.1.2	Setting Up a Code Server with the CASSETUP Utility	151
2.3.1.3	Installation of CASSETUP Utility	151
2.3.1.4	Modify CASSETUP.STR Storage Information File	153
2.3.1.5	Selecting Application Profiles	155
2.3.1.6	Working with the CASSETUP Utility	161
2.4	Creating Product-Specific Response Files	172
2.4.1	Definition of a Response File	172
2.4.2	OS/2 Warp 3.0 Response File	173

2.4.3	Multiprotocol Transport Services Response File	175
2.4.4	NetView DM/2 Change Control OS/2 Client Response File	178
2.4.5	OS/2 LAN Server 5.0 Response File	178
2.4.6	NetView DM/2 CC DOS Client Response File	181
2.4.7	SystemView in Warp Server Manager Response File	181
2.5	SystemView Software Distribution	185
2.5.1	Software Distribution Components	185
2.5.2	System Requirements	187
2.5.3	Prerequisite Tasks	188
2.5.4	Preparing Non-CID-Enabled Applications for Distribution	202
2.5.4.1	Creating a New Software Object - Manual Definition	203
2.5.4.2	Using DiskCamera	210
2.5.5	Preparing a CID Application for Distribution	211
2.5.6	ADF File Structure	214
2.5.6.1	General Information (@DEF)	215
2.5.6.2	Model Change File (@MCF)	216
2.5.6.3	Model Response File (@MRF)	217
2.5.6.4	Variables (@VAR)	218
2.5.6.5	Generating a Software Profile	220
2.5.7	How Distribution Works	221
2.5.8	Distributing Software	223
2.5.8.1	Using a Remote Systems Manager	224
2.5.8.2	Using an Event Scheduler	226
2.5.9	Using the Command Line	227
2.6	Summary	227
2.6.1	CASSETUP	227
2.6.2	Systems Management Services Software Distribution	228
2.6.3	Summary Table	229
2.7	Related Publications	230
Chapter 3. Print Services in OS/2 Warp Server		231
3.1	Printing with OS/2 Warp	231
3.1.1	Creating a Printer Object on OS/2 Warp	232
3.2	Sharing Print Resources with OS/2 LAN Server	234
3.3	Advanced Print Services in OS/2 Warp Server	234
3.4	Print Services Facility (PSF/2) for OS/2 Warp Server	235
3.4.1	Installing PSF/2	236
3.4.2	Creating a Print Device for PSF/2	238
3.4.3	Printer Attachments	239
3.4.4	Printer Attachment Settings	240
3.4.4.1	Parallel Attachment Settings	240
3.4.4.2	TCP/IP Attachment Settings	242
3.4.5	Creating a PSF/2 Queue	243
3.4.6	Setting Up Transforms	243
3.4.7	Generic Transform Filter	245
3.4.8	PostScript, HP-PCL and HP-PGL Passthru	250
3.4.9	Upload-n-Print Transform	250
3.4.10	Using the APRINT Command	251
3.4.11	Using the PSF/2 Print Submitter	251
3.4.12	PSF/2 Resource Library	253
3.5	Bidirectional Print Support	255
3.6	MarkVision for OS/2	255
3.6.1	Installing MarkVision on a Print Server	256
3.6.2	Installing MarkVision on a Client Workstation	258
3.6.3	Configuring MarkVision	259

3.6.4	MarkNet Port Driver on OS/2 Warp	263
3.6.5	Managing Network Printers with MarkVision	264
3.7	HP JetAdmin for IBM OS/2 Warp Server	270
3.7.1	HP Jetadmin Device Support	271
3.7.2	Installing HP JetAdmin	272
3.7.3	Configuring JetAdmin	273
3.7.4	Managing Printers with JetAdmin	274
3.8	Related Publications	275
Chapter 4. Backup and Recovery Services		277
4.1	OS/2 Warp Server Fault Tolerance Features	277
4.2	Overview	278
4.2.1	Positioning	279
4.3	OS/2 Warp Server Backup/Restore Device Support	280
4.3.1	OS/2 Warp Server Backup/Restore Features	283
4.3.1.1	Source	285
4.3.1.2	Compression	285
4.3.1.3	Rulebook	286
4.3.1.4	File Filter	286
4.3.1.5	Changed Files Only	287
4.3.1.6	Preview Selection	287
4.3.1.7	Destination	287
4.4	OS/2 Warp Server Backup/Restore Scenarios	288
4.4.1	Single Server Scenario	288
4.4.2	Multiple Server Scenario	289
4.4.3	Enterprise Scenario	289
4.5	Disaster Recovery Utility	290
4.5.1	Preparing the Disaster Recovery Utility	290
4.6	Defining your Backup/Recovery Strategy	291
4.7	Related Publications	292
Chapter 5. Comparing Adapter and Protocol Services to AnyNet/2		293
5.1	Any Application - Any Network	293
5.1.1	SNA over TCP/IP	296
5.1.2	Sockets over SNA	296
5.1.3	Sockets over NetBIOS (non-native)	297
5.1.4	Sockets over IPX	298
5.1.5	NetBIOS over SNA (Access Node)	298
5.1.6	NetBIOS over SNA and IPX over SNA (Gateways)	298
5.2	Summarizing Native and Non-native Sockets Services	299
5.2.1	Common Transport Semantics (CTS) Functions of Adapter and Protocol Services	299
5.2.1.1	NetBIOS over TCP/IP	299
5.2.1.2	Native Sockets Services	300
5.2.2	Non-native Sockets Services Provided with AnyNet/2	300
5.3	Benefits of Adding AnyNet Function to OS/2 Warp Server	301
5.4	Related Publications	304
Chapter 6. Brief Look at OS/2 Warp Server SMP		305
6.1	Introducing OS/2 Warp Server SMP	305
6.2	Supported SMP Hardware Platforms	306
6.3	New Base Features	307
6.4	Adapter and Protocol Services	308
6.5	File and Print Services	309
6.6	TCP/IP Services	309

6.7 Remote Access Services	310
6.8 Backup and Recovery Services	310
6.9 System Management Services	311
6.10 Advanced Print Services	312
6.11 Client License Management	312
6.12 Related Publications	312
Appendix A. SystemView in Warp Server and Software Distribution: Sample Configuration Files	313
A.1 System Information Tool: SCSI Subsystem Information	313
A.2 Software Inventory	315
A.2.1 Software Inventory Report Example	315
A.2.2 Exporting Software Inventory Data to a Database	317
A.3 CASSETUP Profile Files	319
A.3.1 OS/2 Warp 3.0 (WIN-OS/2 Version) Profile File	319
A.3.2 MPTS 5.0 Profile File	324
A.3.3 SystemView in Warp Server Manager Profile File	328
Appendix B. Special Notices	333
Appendix C. Related Publications	335
C.1 International Technical Support Organization Publications	335
C.2 Redbooks on CD-ROMs	335
C.3 Other Publications	335
How To Get ITSO Redbooks	337
How IBM Employees Can Get ITSO Redbooks	337
How Customers Can Get ITSO Redbooks	338
IBM Redbook Order Form	339
List of Abbreviations	341
Index	343

Figures

1.	Simplified SystemView Network	3
2.	OS/2 Warp Server Advanced Installation Main Panel	12
3.	Systems Management Services Option Panel	13
4.	Systems Management Services Configuration Panel	14
5.	SystemView Manager Installation Panel	15
6.	SystemView OS/2 Client Configuration Screen	17
7.	SystemView OS/2 Client Installation Panel	18
8.	SystemView DOS/Windows Client Installation Panel	18
9.	First Page of SystemView Configuration Notebook - General Network Parameters	19
10.	SystemView Name Restrictions	20
11.	SystemView Configuration Options	21
12.	Second Page of Configuration Notebook - Software Distribution	21
13.	Third Page of Configuration Notebook - Remote Control	22
14.	Fourth Page of Configuration Notebook - Application Sharing (Netware Server)	23
15.	Application Sharing from an OS/2 LAN Server	24
16.	Second Page of the Client Configuration Notebook	25
17.	SystemView Installation and Maintenance Utility	27
18.	Installed Catalog File Example	27
19.	Local Execution of SystemView Services	29
20.	Remote Execution of SystemView Services	29
21.	SystemView Folder	30
22.	SystemView Service Manager	31
23.	Group Definition Examples	32
24.	Adding a New Management Group	33
25.	Selecting Group Discovery Filters	33
26.	Group Discovery Filter Options	34
27.	Icon View of All Systems in the Network	35
28.	Detail View of All Systems in the Network	36
29.	System Group Management Classification Example	37
30.	System Icon Context Menu	39
31.	Group Icon Context Menu	39
32.	Incoming User ID / Password Configuration	41
33.	Outgoing User ID / Password Configuration	42
34.	System Information Tool Window	45
35.	System Information Tool - SCSI Subsystem	46
36.	Software Inventory Full Dictionary Search Example	47
37.	Software Inventory Selected Product Search Example	48
38.	Software Inventory - Menu Options	49
39.	Software Inventory Database Entry Selection Window	50
40.	Creating Records in a Dictionary File	51
41.	Editing and Erasing Records in a Dictionary	51
42.	Adding a New Product to the Software Inventory	52
43.	Matching File Attributes Screen	53
44.	Add Matching File Window	53
45.	Product Defined by SYSLEVEL File	54
46.	Searching for a SYSLEVEL file	55
47.	Creating the SYSLEVEL File Definition	55
48.	System Profile - User Information Page	57
49.	System Monitor Service Windows Drop-Down Menu	60

50.	Export to Database Option	61
51.	Monitor Context Menu	61
52.	Different View Options	62
53.	Setting Thresholds	63
54.	Viewing the Alert Log	65
55.	Monitor-Specific Settings	66
56.	Specifying Files in the Critical File Monitor	68
57.	Alert Manager Message Generated by the Critical File Monitor	69
58.	ECC Memory Setup	70
59.	RAID Manager	71
60.	File Transfer Window	76
61.	Alert Manager Main Window	78
62.	Alert Action Window: How the Alert is Processed	82
63.	Alert Manager Action Editor Window	83
64.	Predictive Failure Analysis	87
65.	Working with Predictive Failure Analysis	88
66.	Scheduling a New Event	90
67.	System Partition Access Misuse Warning	91
68.	System Partition Access Backup Warning	91
69.	Process Management	95
70.	Viewing a Remote Machine's OS/2 Window	97
71.	Text Mode Application: FDISK Example	98
72.	Remote Workstation Control Example	101
73.	Screen View	104
74.	Using the DMI with an SNMP Management Application	106
75.	Using a Nodelocked License	108
76.	Using a Server-Based License	110
77.	Summary of License Models	112
78.	Simple NCS Cell - All Processes Run on One Server	113
79.	Cell with Two License Servers and Three Clients	114
80.	DCAF and SystemView: Rules for Coexistence and Interoperability	119
81.	Output of THINLAPS execution	129
82.	THINLAPS Files Are Copied into the Root	130
83.	THINLAPS Changes to CONFIG.SYS	131
84.	THINLAPS PROTOCOL.INI File Creation	131
85.	Directory \CID\SRVIFS	132
86.	Sample SRVIFS Response Files	132
87.	SERVICE.INI Sample File	133
88.	SERVICE.LST Example	133
89.	THINIFS Client Boot Diskette Files	136
90.	THINIFS Boot Diskette CONFIG.SYS Changes	137
91.	Installing TCP/IP for OS/2 NFS Kit	139
92.	Installation of TCP/IP for OS/2 NFS CSD Kit	140
93.	Code Server Directory Structure Example	146
94.	OS/2 Warp Server CD-ROM CID Directory Structure	148
95.	OS/2 Warp Server CD-ROM CID Directory Structure	149
96.	Creating the CID Directory Structure	150
97.	CASSETUP Code Server Setup Utility	151
98.	CASSETUP Storage File CASSETUP.STR	154
99.	Error Message: MPTS50 Directory Not Created	155
100.	CASSETUP Profile for OS/2 Warp Version 3 (OS230.PRO)	156
101.	CASSETUP Profile for MPTS 5.0 (MPTS50WS.PRO)	157
102.	CASSETUP Profile for SystemView in Warp Server Manager (SYSVIEW2.PRO)	159
103.	Boot Diskette Profile for OS/2 Warp V3 (30WMPTS.SCR)	160

104.	CASSETUP Containers	161
105.	Code Servers Container Selected Menu	162
106.	Load Srvifs/LAN CID Utility Support Window of CASSETUP	162
107.	Load Srvifs/LAN CID Utility Support - CONFIG.SYS Modified Window	162
108.	SRVIFS Support Completed Successfully	163
109.	Updating CASSETUP.STR	163
110.	Definition for OS/2 Warp V3	164
111.	Definition for MPTS	164
112.	Definition for LAN Requester	165
113.	Definition for LAN Server	165
114.	Definition for SystemView	166
115.	Available Applications at Code Server ENRIQUE	167
116.	Create Client (Boot) Diskettes Window of CASSETUP	167
117.	LAN CID Utility Casprep/Command Files Window of CASSETUP	169
118.	LAN CID Utility Casprep File Dialog Window	170
119.	Specifying the Complete Target Path	170
120.	Select CASPREP Source File Window	171
121.	LCU.COMD Information Window	171
122.	Response File for the OS/2 2.11 Base System Installation	174
123.	MPTS Response File IEEE 802.2 and NetBIOS Protocol Drivers	175
124.	MPTS Response File TCP/IP, TCPBEUI and Native NetBIOS	176
125.	Response File for the NetView DM/2 CC OS/2 Client Installation	178
126.	Generating an IBM LAN Server 5.0 Response File	179
127.	IBM LAN Server 5.0 Response File Source Drive	179
128.	Response File for the OS/2 LAN Server 5.0 Server Installation	180
129.	Response File for the OS/2 LAN Server 5.0 Requester Installation	181
130.	Response File for the NetView DM/2 CC DOS Client Installation	181
131.	Response File for the SystemView Manager Remote Installation	182
132.	Software Distribution Topology	187
133.	Prerequisite Tasks for Software Preparation	189
134.	SystemView Manager Configuration Page	190
135.	Configuration Page for Software Distribution	191
136.	SystemView Client Configuration Page	193
137.	Configuration Page for the Software Distribution Clients	194
138.	Software Distribution Agent Window	195
139.	Software Distribution Client Agent Window	196
140.	Creating the Directory Structure for the Code Server	198
141.	CID Directory Structure	199
142.	Creating Aliases for the CID Directories	200
143.	Code Server Setup Utility Page 2	201
144.	Software Preparation Profiles for Non-CID-Enabled Applications	203
145.	Software Preparation - New Profile	204
146.	Software Preparation - Objects Components Window	204
147.	Software Preparation - Object Characteristics	205
148.	Software Preparation - Object Details	206
149.	Destination Options Window	207
150.	Install Script Window	208
151.	Specifying Values for Variables	209
152.	Catalog Message Window	209
153.	Default DSKCAM.INI File	210
154.	DiskCamera Software Installation Window	211
155.	Software Library DB2/2 2.1 Sample Configuration	213
156.	DB2/2 Folder	213
157.	@DEF General Information section of DB2/2 ADF File	215
158.	@MCF Change File Section of DB2/2 ADF File	216

159.	@MCF Change File Section of DB2/2 ADF File	216
160.	@MRF Model Response File Section of the DB2 ADF File	217
161.	Dummy File @MRF Section of the DB2/2 ADF File	217
162.	Generating a Response File in the MRF Section of the DB2/2 ADF File	217
163.	@VAR Parameters Section of the DB2/2 ADF File	219
164.	ADF File Schematic	220
165.	Registering a New ADF File	221
166.	Software Distribution Processes	222
167.	Software Distribution Products Catalog	224
168.	Software Distribution Installation Options	225
169.	Scheduling a Software Distribution Event	226
170.	OS/2 Warp Printer Objects	231
171.	Creating a Print Object	232
172.	Installing a New Printer Driver	233
173.	Access Another Network Printer Window	234
174.	Advanced Print Services Easy Installation Path	236
175.	Warp Server Setup and Installation Menu	237
176.	Advanced Print Services Options	237
177.	PSF/2 Folder	238
178.	Defining a New Device in PSF/2	239
179.	Parallel Settings Window	241
180.	Change Bin Mapping Window	242
181.	TCP/IP Settings Window	242
182.	Setup Queues Window	243
183.	Transform Options Window	244
184.	Setup Transforms Window	246
185.	Add Transform Window	246
186.	Generic Filter Transform Options Window	247
187.	Creating a PSF/2 Device for the Transform Filter Exit	248
188.	Creating a Transform Sequence	249
189.	Creating a Queue	249
190.	Print Submission Window	252
191.	Print Window	253
192.	List AFP Resources Window	254
193.	Resource Librarian - AFP Resources List	254
194.	Warp Server CD-ROM 2 Panel	257
195.	MarkVision Setup Screen	258
196.	MarkNet Port Driver Settings Window	259
197.	MarkNet Network Port Driver Notebook - Adapters List Page	260
198.	MarkNet Network Port Driver Notebook - Filters Page	262
199.	MarkNet Network Port Driver Notebook - Options Page	263
200.	Printer Object with MarkNet Port Driver	264
201.	MarkVision Window	265
202.	4039 Notebook - Status Page	265
203.	4039 Notebook - Operator Panel Page	266
204.	4039 Op Panel Page - MENUS Selected	267
205.	4039 Notebook - Statistics Page	268
206.	Network with Many Printers	269
207.	Printer Requiring Operator Intervention	270
208.	HP JetAdmin Settings Notebook	273
209.	HP Remote Control Panel Notebook - Status Page	274
210.	OS/2 Warp Server Backup/Restore Main Panel	278
211.	OS/2 Warp Server Backup/Restore	279
212.	OS/2 Warp Server Backup/Restore Device Support	280
213.	OS/2 Warp Server Backup/Restore Pipeline	284

214.	OS/2 Warp Server Backup/Restore Rulebook	286
215.	Defining a Storage Device (ADSM)	288
216.	Defining the Communications Options for an ADSM Backup Set	288
217.	OS/2 Warp Server Backup/Restore Disaster Recovery Options Panel	291
218.	IBM Networking Blueprint	293
219.	Common Transport Semantics (CTS) Layer	294
220.	AnyNet Access and Gateway Nodes	295
221.	SNA over TCP/IP	296
222.	Sockets over SNA	297
223.	Sockets over NetBIOS and Sockets over IPX	297
224.	NetBIOS over SNA	298
225.	IPX over SNA and NetBIOS over SNA Gateways	299
226.	Sockets over NetBIOS - Native and Non-native	301
227.	AnyNet and Corporate Networks	303
228.	AnyNet LAN - WAN Convergence Benefits	304
229.	Output of SCSI System Information	313
230.	Software Inventory Report Example	315
231.	Exporting Software Inventory Data to a Database	317
232.	CASSETUP Profile for OS/2 Warp Version 3 (OS2WS.PRO)	319
233.	CASSETUP Profile for MPTS 5.0	324
234.	CASSETUP Profile for SystemView in Warp Server Manager	328

Tables

1.	SystemView Manager NetBIOS Resources	9
2.	SystemView Hard Disk Requirements by Component	10
3.	Products Available in IBM OS/2 Warp Server for Installation Using the SystemView Installation and Maintenance Utility	27
4.	System Profile Information by Page	56
5.	Special Keystrokes and Mouse and their Effects in the Local or Target Machine	102
6.	Analysis and Problem Determination Functions	120
7.	Remote Access to Systems	120
8.	Software Distribution, Management and Inventory	120
9.	Hardware Management and Inventory	120
10.	Miscellaneous	121
11.	Software Distribution Products and Their Capabilities	127
12.	Comparing SRVIFS and LAN Server	138
13.	Comparing Different Methods for Operation System Installation	143
14.	Description of the Recommended Directory Structure	147
15.	OS/2 Keyword=Value Considerations	173
16.	Software Distribution Configuration File	191
17.	Configuring the CID Software Preparation Utility	201
18.	ADFs and Response Files Supplied with SystemView	212
19.	IBM's Software Distribution Managers and Their Features	229
20.	Types of Print Files and Printers Supported by PSF/2 for Warp Server	235
21.	Transforms Provided with PSF/2	244
22.	8mm Tape Drives Supported by OS/2 Warp Server Backup/Restore	282
23.	4mm Tape Drives Supported by OS/2 Warp Server Backup/Restore	282
24.	QIC Tape Drives Supported by OS/2 Warp Server Backup/Restore	283
25.	DLT Tape Drives Supported by OS/2 Warp Server Backup/Restore	283
26.	Systems Supported by OS/2 Warp Server SMP	306

Preface

This redbook, a companion to *Inside OS/2 Warp Server, Volume 1*, SG24-4602, provides information about the Systems Management, Software Distribution, Backup and Recovery, and Advanced Print Services components of IBM OS/2 Warp Server. It is the result of a residency project conducted at the IBM ITSO, Austin Center.

Systems Management is a vast and complex topic. We discuss many systems management issues and how the SystemView product within OS/2 Warp Server can address many of the issues and problems that arise in a computerized environment. We describe how the administrator can monitor important files for unauthorized changes, query systems remotely for hardware and software inventory information, view and control desktops remotely, and process alerts from systems that require attention. All this can be done from the administrator's desktop, quickly solving problems and saving money.

Electronic Software Distribution is an excellent mechanism for companies, large and small, to cut unnecessary costs while maintaining a productive desktop environment for employees. This redbook describes software distribution considerations and how SystemView Software Distribution within OS/2 Warp Server can address your desktop software maintenance problems. We also provide recommendations on selecting the best products and functions for your distribution needs.

Printing can often be a frustrating task for both the end user and the administrator. We explore Advanced Print Services functions, such as remote management of network printers and converting print streams, to enable the use of a much wider variety of printers, such as host printers.

Backing up critical files and being able to restore them quickly is a requirement in virtually all environments. We investigate the functions of OS/2 Warp Server Backup/Restore to effectively manage the server environment and describe some unique capabilities, such as the intuitive user interface and the ability to use client/server-based resources for backup and restore.

Many customers run multiple protocols, such as NetBIOS, IPX, TCP/IP, and SNA. Having applications communicate seamlessly across these protocols can be a daunting task. We describe how the AnyNet component of the IBM Communications Server can be used to expand OS/2 Warp Server's reach into the WAN environment, embracing virtually any communications protocol need.

Some customers have a need for very large processing capacity on the Intel hardware platform. We briefly discuss the OS/2 Warp Server SMP product and the improvements and changes from OS/2 Warp Server. With this information, the administrator can decide how and when to migrate to this enterprise-ready environment.

Knowledge of IBM OS/2 Warp and IBM OS/2 LAN Server 3.0 or 4.0, and an understanding of TCP/IP are assumed.

How This Redbook Is Organized

This redbook contains 346 pages. It is organized as follows:

- Chapter 1, “System Management Services”

OS/2 Warp Server features a rich set of systems management functions. This chapter describes each of these functions in detail.
- Chapter 2, “Software Distribution Considerations”

A subset of Systems Management Services is software distribution. This chapter discusses the many different ways that you may distribute CID and non-CID enabled software using OS/2 Warp Server.
- Chapter 3, “Print Services in OS/2 Warp Server”

This chapter describes the print functionality included in the base operating system, such as bidirectional printer support, and also describes the capabilities of Advanced Print Services, including support for host printing of several hundred pages per minute.
- Chapter 4, “Backup and Recovery Services”

This chapter discusses how you may secure your OS/2 Warp Server environment and quickly recover from catastrophic failures by using the OS/2 Warp Server Backup/Restore component of OS/2 Warp Server.
- Chapter 5, “Comparing Adapter and Protocol Services to AnyNet/2”

This chapter describes the differences between the features found in OS/2 Warp Server Adapter and Protocol Services and the additional functions that are included in the IBM AnyNet products. The AnyNet products are included with IBM Communications Server.
- Chapter 6, “Brief Look at OS/2 Warp Server SMP”

This chapter describes the changes between OS/2 Warp Server and OS/2 Warp Server SMP at a very high level. It lists the hardware platforms which are supported by OS/2 Warp Server SMP and mentions changes in the various components, such as the File and Print Sharing Services and OS/2 Warp Server Backup/Restore.
- Appendix A, “SystemView in Warp Server and Software Distribution: Sample Configuration Files”

This appendix contains sample files related to Software Distribution and SystemView configuration.

The Team That Wrote This Redbook

This redbook project was managed by **Toshi Shimizu**, formerly of the International Technical Support Organization, Austin Center, and **Oscar Cepeda** of the International Technical Support Organization, Austin Center.

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization Austin Center.

Geraldo Macedo, retired, was a member of the Client/Server Marketing and Strategy team in IBM Brazil. He has 27 years of experience and was responsible for LAN and interoperability.

Martin Murhammer is a Systems Engineer in IBM Austria. He has 11 years of experience in the personal computing environment and was responsible for customer projects in heterogeneous connectivity, server design, system recovery, and Internet solutions. He is now a member of the ITSO - Raleigh Center.

Indran Naick is an Advisory Systems Engineer in the IBM Software Company of IBM South Africa. He has seven years of field experience in OS/2 LAN Server and related networking products. He is a Certified LAN Server Engineer and Certified NetWare Engineer.

Emmanuel Odier is a Software Specialist in IBM France. He has six years of experience, mainly in LANs and desktop software. He is responsible for pre-sales support in OS/2, OS/2 LAN Server and OS/2 Warp Server.

Hermann Pauli is a Systems Engineer in IBM Germany. He has eight years of field experience in OS/2, OS/2 LAN Server and OS/2 Communications Manager. He is currently responsible for technical marketing support for Internet and intranet technology solutions.

Alain Rykaert is a Specialist Systems Engineer in IBM Belgium. He has 18 years of field experience, primarily in the LAN environment. His areas of expertise include LAN, OS/2 and OS/2 LAN Server/Warp Server.

Andrew Taylor is a LAN Systems Specialist in IBM United Kingdom. He has 13 years of experience in software programming and support on mainframe and personal computer operating systems. His areas of expertise include OS/2 Warp and OS/2 LAN Server/Warp Server. He is a Certified OS/2 Warp Server Engineer and a co-author of the ITSO Redbook titled "Inside OS/2 LAN Server 4.0".

Enrique Daniel Testini is a Senior Software Specialist in IBM Italy. He has seven years of experience, including OS/2 and DOS Communications products and protocols and REXX Programming. He is currently the Chief Designer of the Fast Connect project in IBM EMEA.

Colin Vernon is a Senior Specialist in the Personal Software Support group in IBM United Kingdom. He has eight years of field experience, providing customer support in all areas of PSP products. His areas of expertise include OS/2, LAN Server protocols, LAN Distance, and Wide-Area Networking.

Thanks to the following people for their invaluable contributions to this project:

IBM Austin

Bill Hartner
Gary Hunt
Lloyd Stearns

IBM Raleigh

Mike Almasy
Alfred Daun
Sanjay Khanna

IBM Italy

Lucio Bortolotti
Claudio Valant

IBM Boulder
Scott Mastie

IBM United Kingdom
Michael Fabianski
Mary Visser

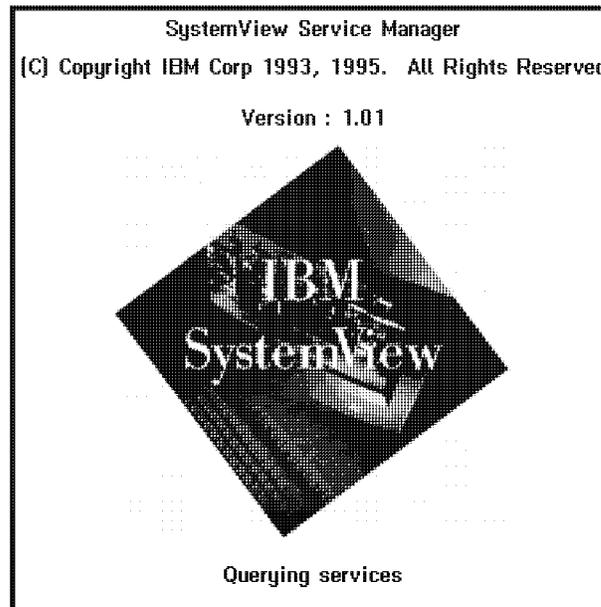
Comments Welcome

We want our redbooks to be as helpful as possible. Should you have any comments about this or other redbooks, please send us a note at the following address:

redbook@vnet.ibm.com

Your comments are important to us!

Chapter 1. System Management Services



In this chapter we introduce the systems management and services included in OS/2 Warp Server. Systems management is a vast topic, and this chapter is intended to provide an overview of the systems management disciplines together with the tools provided in OS/2 Warp Server to aid administrators.

1.1 Overview and Concepts

This section gives an overview of systems management together with some of the terms and concepts that will be used during the course of this chapter.

1.1.1 What is Systems Management?

Systems management covers the management of systems, networks, hardware, data, applications, transactions, voice, and so on. These are all resources that need to be managed. The result of the systems management processes is that it increases the availability of information system services to users in the network.

Organizations are relying to a greater extent than ever before on local area networks (LANs) to run their critical business applications. As a result, systems management has become a key customer requirement for keeping the network and the workstations working efficiently.

Examples of some systems management processes are:

- Keeping track of hardware resources and software levels
- Efficiently providing help to end users when they have problems
- Installing and maintaining software levels
- Tracking performance data

1.1.2 IBM's SystemView Model and OS/2 Warp Server

SystemView is IBM's systems management brand. IBM SystemView is a structure that groups systems management operations into disciplines, thus simplifying the complex task of systems management. A discipline is a broad category of systems management tasks and the functions that address those tasks. There are six systems management disciplines:

- **Business Management**

The focus here is to improve control of I/S assets and provide efficient and effective administrative processes. Some of the major tasks of business management include asset, license and financial management.
- **Change Management**

The change management discipline is the discipline that manages and controls the introduction of change into an information system environment. Change management includes planning, scheduling, distributing, synchronizing, installing, activating, and monitoring changes to system software, applications, hardware, and data.
- **Configuration Management**

Configuration management is one of the most critical systems management disciplines. It spans administration and operations of networks and systems and must provide function and data to many different users and applications (such as problem, change, and asset) in the enterprise. Successful configuration management is one of the keys to cost-effective systems management.
- **Operations Management**

The operations management discipline manages the use of systems and resources to support the workloads of an enterprise's information system. This discipline includes tasks for planning, distributing, evaluating, scheduling, and controlling workloads, as well as the resources needed to support those workloads.
- **Problem Management**

The problem management discipline is the process of managing problems or potential problems from their detection through their final resolution. Problem management encompasses the detection, analysis, recovery, resolution, and tracking of problems occurring in the information system. It also includes establishing the policies for problem management, any planning associated with problem management, as well as creation and maintenance of the problem-management process. It has the objective of reducing the number and duration of outages which, in turn, reduces the resources needed for the process.
- **Performance Management**

The performance management discipline addresses the effectiveness with which information systems deliver service to their users. The discipline includes planning, evaluation, and control tasks/functions in support of delivering a quality of service which meets customer-defined service goals and policies.

The OS/2 Warp Server product implements IBM's SystemView model and provides a systems management solution for a LAN workgroup environment. This type of environment is typical of a small company that needs workstation

interconnection to enable sharing of application data, or of an enterprise departmental organization that works with autonomy from the enterprise's main information-system infrastructure.

In general, workgroup LANs are set up to have one central point to administer and control all the workstations in the network that have an operational application focus, but these workstations can also administer and control their own resources.

In the next few sections, we discuss some of the SystemView services contained within OS/2 Warp Server. Many of the services could belong to more than one of the SystemView disciplines. We have categorized them into the three broad areas of performance, inventory and operations management. The Remote Systems Manager, Security, Remote Workstation Control, License Management and the SystemView Agent are discussed outside of their SystemView discipline.

1.2 SystemView in Warp Server Components

A typical system management environment would consist of a NetBIOS, TCP/IP or IPX LAN with five to 300 workstations. SystemView in Warp Server is able to manage both OS/2 and Windows 3.11 clients. Figure 1 shows a simplified system management environment. Workstation A is installed as the SystemView Manager. Workstations B and C are installed as OS/2 and Windows clients, respectively. All the selectable components are installed.

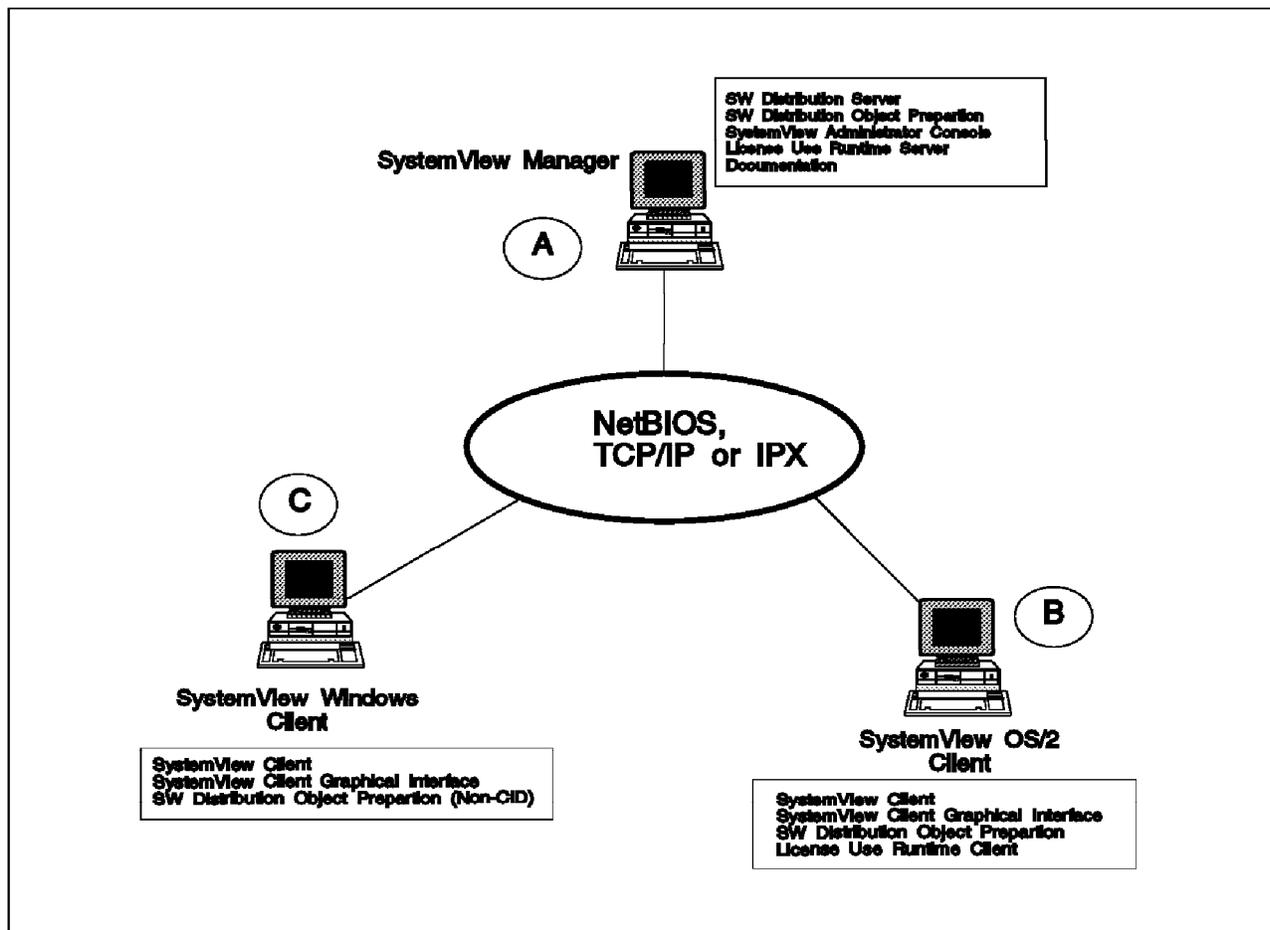


Figure 1. Simplified SystemView Network

1.2.1 SystemView Manager

In this environment, Workstation A, the SystemView Manager, would be the central point of control for all the workstations. This workstation is called the manager, and from this central point of control the administrator could:

- Monitor and detect problems generated from any workstation and gather relevant data for problem determination
- Track the hardware and software inventory of all workstations
- Keep the software up-to-date on all workstations
- Gain remote access to any workstation to control its processes
- Control license usage to adhere to the terms and conditions for that software

The ability to perform any of the above functions is dependent on which components are selected on installation. The following is a description of the SystemView Manager components selectable on installation:

- SystemView Administrator Console

This component allows you to run administrator operations for systems management, remote workstation control and software-distribution tasks. This component provides the basic SystemView Manager functionality and is a prerequisite to the rest of the components listed below.

- License Use Runtime Server (optional)

This provides the capability to manage and control software license use on remote SystemView Clients and Administrator Consoles from this Administrator Console. If you want to run license management in your SystemView network, you should install this component on at least one Administrator Console. The product will be installed in the IFOR directory of the drive chosen for SystemView installation.

If you choose not to install the License Use Runtime Server component, the License Use Runtime Client will be installed.

- Software Distribution Server

Adds the Software Distribution Catalog to the Administrator Console. You must have at least one distribution server in your SystemView network if you want to run software distribution.

If you choose not to install the Software Distribution Server, the Software Distribution Client is installed. This will enable the SystemView Manager to receive software updates from some other distribution server in the network.

- Software Distribution Object Preparation (optional)

Provides the graphical user interface to prepare objects for software distribution. You can prepare and distribute three types of objects: software products, application sharing and CID-enabled products. If you want to run software distribution in your SystemView network, you should install this component on at least one Administrator Console.

- SystemView in Warp Server Documentation, BookManager Format

These are the BookManager versions of SystemView in Warp Server publications together with the Library Reader.

- SystemView in Warp Server Documentation, IPF Format

These are the INF versions of SystemView in Warp Server publications.

1.2.2 SystemView OS/2 Client

A SystemView OS/2 Client would typically be an OS/2 V2.11 or OS/2 Warp user workstation, but could include other bridges, print servers and so forth. This machine is normally referred to as the managed, or client, workstation. The managed workstation can:

- Control its own system resources in order to optimize its application processes
- Request software updates
- Share application software and data from other workstations
- Prepare software objects to be distributed by the central point of control

The ability to perform any of the above functions is dependent upon which components are selected on installation. The following is a description of the SystemView OS/2 Client components that are selectable on installation:

- SystemView Client

The SystemView Client provides the capability to run your workstation as a target for SystemView management operations from a remote Administrator Console. In addition to this, it allows you to execute alert and security management as well as the serial control locally. The SystemView Client contains the Software Distribution Client.

This component provides the basic SystemView Client functionality and is a prerequisite for installing all the other components.

- SystemView Client Graphical Interface (optional)

This component adds a graphical interface to the SystemView Client. The Client Graphical Interface allows you to execute at a local level the same workstation-management operations that are run remotely from the Administrator Console.

The graphical component also allows the client to run as a *pull* Software Distribution Client. You can locally select the software object from the server and start the distribution process.

A client with the graphical interface installed is referred to as an *active* client. A client without the graphical interface installed is referred to as a *passive* client. A passive client can only access functions provided by the SystemView Client component, as described.

- License Use Runtime Client (optional)

This component provides functions for monitoring use of software that is enabled for license use monitoring. If you have license-enabled software, you should include this component. The License Use Runtime Client is available only for OS/2 workstations.

- Software Distribution Object Preparation (optional)

This component is exactly the same as the Software Distribution Object Preparation installed on the SystemView Manager. Installing this component on a SystemView Client allows you to prepare software objects for distribution at this workstation.

- SystemView in Warp Server Documentation, BookManager Format

These are the BookManager versions of SystemView in Warp Server publications, including the Library Reader application to access the documentation.

- SystemView in Warp Server Documentation, IPF format

These are the INF versions of SystemView in Warp Server publications.

1.2.3 SystemView DOS/Windows Client

The SystemView DOS/Windows Client has functions similar to the OS/2 client with the exception of the License Use Runtime Client. The following components are selectable for the SystemView DOS/Windows Client:

- SystemView Client

Like the OS/2 Client, this component provides the basic SystemView Client functionality and is a prerequisite to the other components listed below.

- SystemView Client Graphical Interface (optional)

This component adds a graphical interface to the SystemView Client. The Client Graphical Interface allows you to execute at a local level the same workstation-management operations that are run remotely from the Administrator Console.

- Software Distribution Object Preparation (optional)

This component is similar to the Software Distribution Object Preparation installed on the SystemView Manager. However, the Software Distribution Object Preparation component installed under Windows only allows for the preparation of non-CID Windows applications for distribution.

1.3 Installation and Configuration

As described previously, a workstation can either be a manager or a client. The manager can only be installed on an OS/2-based workstation, whereas the client could be an OS/2 or a Windows-based machine. Depending on the systems management requirements, a number of functional components are selectable for the manager and the clients during installation. In this section, we describe the installation of the three types of workstations that can be installed and configured using SystemView in Warp Server. They are:

- SystemView Manager
- SystemView OS/2 Client
- SystemView DOS/Windows Client

Although these components may be configured differently on each workstation, we will generically cover all the selectable components for each of the SystemView workstation types.

The following considerations should be taken into account when setting up your SystemView environment:

- License control is not required when using SystemView as a part of the OS/2 Warp Server product. If you are using the SystemView for OS/2 *stand-alone* product, at least one License Use Runtime Server must be set up in the network within 60 days after the SystemView Manager installation.

- A distribution server is necessary only for using Software Distribution. It is an optional component when installing each SystemView Manager.
- Software distribution servers do not communicate with each other. In addition, a Software Distribution Client can communicate to only one Software Distribution Server. Due to this restriction, if you have a large number of clients, you should create logical workgroups and install a Software Distribution Server for each logical workgroup.

1.3.1 Hardware and Software Prerequisites

The requirements for SystemView in Warp Server are dependent on how the systems management environment is set up, as well as the number of clients to be managed by each SystemView Manager.

For example, you may choose to have a single SystemView Manager which may also be a Distribution Server and/or a License Use Runtime Server. Alternatively, you may choose to have multiple SystemView Managers with the distribution server and License Use Runtime Server on any of the SystemView Managers.

1.3.1.1 SystemView Manager Prerequisites

For a SystemView Manager, that is also a License Use Runtime Server, the prerequisites are:

Hardware:

1. If the Software Distribution Server is installed on the same machine:
 - A minimum 486 50 MHz processor
 - A minimum 28 MB RAM (for 20-30 clients)
 - A minimum 48 MB RAM (for 100 clients)
 - Disk space for SystemView use:
 - 27.5 MB for the SystemView Administrator Console
 - 7 MB for the License Use Runtime Server
 - 5 MB for the License Use Runtime Client (automatically installed on every SystemView Manager)
 - 4 MB for the Software Distribution Server
 - 5 MB for the Software Distribution Object Preparation
 - 1 MB for the INF versions of the manuals
 - 11 MB for the BookManager versions of the manuals
 - 1.4 MB for Library Reader
 - An appropriate amount of disk space to store the distribution change files, software objects for distribution and Inventory Databases
 - 25 MB required temporarily during the installation process
 - A CD-ROM drive for product installation
 - An appropriate token-ring or Ethernet card
 - Modem (for serial connection control)

Note:

- a. In a LAN configuration for 20-30 clients, the Distribution Server requires 9 MB RAM when the Software Distribution Clients are active.

- b. In a LAN configuration for 100 clients, the Distribution Server requires 30 MB RAM when the Software Distribution Clients are active.
2. If the Software Distribution Server is not installed on the same machine:
 - A minimum 486 50 Mhz processor
 - A minimum 16 MB RAM (for 20-30 clients)
 - A minimum 24 MB RAM (for 100 clients)
 - 15 MB disk space for SystemView in Warp Server use
 - Disk space for inventory databases
 - 25 MB required temporarily during the installation process
 - A CD-ROM drive for product installation
 - An appropriate token-ring or Ethernet card
 - Modem (for serial connection control)

Software: The SystemView Manager requires the following prerequisite software:

1. OS/2 Warp (contained in the OS/2 Warp Server)
2. Products to support the appropriate communication protocols (see 1.3.1.3, "Communication Protocols" on page 9)

If you need to export data, such as hardware, software inventory information and alerts, to a database, you must have one of these database systems:

- DB2/2 CAE Version 1.2 with Service Pack Level WR07037 or later, plus REXX
- Lotus Notes Release 3.2 or later on the Lotus Notes server, plus Lotus Notes Client Release 3.2 or later on SystemView Manager systems that will export to the database.

1.3.1.2 SystemView Client Prerequisites

The hardware and software requirements for the OS/2 and Windows Clients are:

Hardware:

- 386 processor minimum
- 8 MB RAM for a passive client; 12 MB RAM for an active client with all components installed
- Disk space for SystemView in Warp Server use:
 - 16 MB for the SystemView in Warp Server client in OS/2, 14 MB in Windows
 - 2.5 MB for the SystemView in Warp Server Client Graphical Interface in OS/2, 4 MB in Windows
 - 5 MB for the License Use Runtime Client
 - 5 MB for Software Distribution Object Preparation in OS/2, 0.32 MB in Windows
 - 1 MB for the INF versions of the manuals
 - 11 MB for the BookManager versions of the manuals
 - 1.4 MB for Library Reader
- 8 MB required temporarily during the installation process

Software:

One of the following is required on the client workstation:

- OS/2 2.11 or later
- IBM DOS 6.3 and Microsoft Windows 3.1
- IBM DOS 7.0 and Microsoft Windows 3.1
- MS-DOS 6.2 and Microsoft Windows 3.1
- Products to support the appropriate communication protocols (see 1.3.1.3, "Communication Protocols")

1.3.1.3 Communication Protocols

SystemView in Warp Server supports NetBIOS, TCP/IP or IPX. The workstations could be on a single LAN or on multiple LANs interconnected by routers or bridges. Serial connection is also supported for all SystemView functions except for software distribution.

Below is a list of the supported protocols and the products required to obtain the necessary support.

Protocol Description

NetBIOS In OS/2, NetBIOS support is provided through Multiprotocol Transport Services (MPTS) 1.0 or later (LAPS level WR08000).

In DOS/Windows, NetBIOS support is provided by the LAN Support Program 1.35 or later.

TCP/IP In OS/2, TCP/IP support is provided by IBM TCP/IP for OS/2 2.0 with CSD UN64092 or later.

Note: OS/2 Warp Server has IBM TCP/IP for OS/2 3.0.

In DOS/Windows, TCP/IP support is provided by IBM TCP/IP for DOS 2.1.1 or later.

IPX/SPX In OS/2, IPX/SPX support is provided by Novell NetWare Requester for OS/2 2.10 or later.

In DOS/Windows, IPX/SPX support is provided by Novell Netware Client for DOS and Windows 1.21.

Note:

1. OS/2 Warp Server has Novell NetWare Requester for OS/2 2.11.
2. License Use Runtime Servers and Clients in an IPX/SPX network must run NetBIOS in MPTS in addition to the Novell NetWare Requester for OS/2 and must be configured with the NetBIOS communication protocol.

1.3.1.4 NetBIOS Resources

If you choose to have NetBIOS as your protocol, the NetBIOS resources required by SystemView Manager are shown in Table 1.

Table 1 (Page 1 of 2). SystemView Manager NetBIOS Resources

SystemView in Warp Server	Manager	Distribution Server	License Use Runtime (Server or Client)	Full Configuration
Sessions	2	25	1	28
Commands	9	25	40	74

<i>Table 1 (Page 2 of 2). SystemView Manager NetBIOS Resources</i>				
SystemView in Warp Server	Manager	Distribution Server	License Use Runtime (Server or Client)	Full Configuration
Names	3	2	2	7

NetBIOS resources required on an OS/2 Client are: three sessions, nine commands and four names.

1.3.1.5 Summary of Hard Disk Usage

The following table summarizes the DASD usage selected by component.

<i>Table 2. SystemView Hard Disk Requirements by Component</i>	
SystemView in Warp Server Component	DASD in Mb
SystemView Administrator Console	27.5
Software Distribution Server	4.0
Software Distribution Object Preparation	5.0
License Use Runtime Server	7.0
License Use Runtime Client	5.0
SystemView Documentation IPF format (.INF)	1.0
SystemView Documentation BookManager format	11.0
IBM Library Reader/2	1.4
SystemView OS/2 Client	16.0
SystemView DOS/Windows Client	14.0
SystemView Client Graphical Interface for OS/2	2.5
SystemView Client Graphical Interface for Windows	2.5
Software Distribution Object Preparation for OS/2	5.0
Software Distribution Object Preparation for Windows	0.32
Note: <ul style="list-style-type: none"> • Additional disk space for software change files should be available when the Software Change Control function is used. • Hard Disk requirements should be carefully evaluated at installation time. The user should consider more space to allow the installation procedure to unpack the files. For example: <ul style="list-style-type: none"> - Manager requires 25 MB extra - Client requires 8 MB extra • Hard disk overflow generates the misleading warning message EPFIE604 "Unable to transfer <file name>. The file is in use or locked" 	

1.3.2 SystemView Manager Installation

The SystemView Manager can be installed using a number of different methods. The method that you choose would often be determined by the available hardware within your organization or your existing configuration.

The following installation methods are possible:

- OS/2 Warp Server Integrated Installation

The most direct method of installation is using the OS/2 Warp Server integrated installation program. This method would usually be chosen when installing a new or an existing OS/2 LAN Server machine with OS/2 Warp Server. This installation program offers two methods of installation:

- The Advanced installation

This selection allows a user greater control over the installation and configuration of the SystemView Manager installation.

- The Easy installation

This selection makes a number of decisions on your behalf, allowing you little control over the installation and customization of the SystemView Manager.

- Install Program

You can install the SystemView Manager from the CD-ROM using the `INSTALL` command from the `\CID\SERVER\SYSVIEW2\SERVER_2` directory off the OS/2 Warp Server CD-ROM. This method is usually chosen when installing the SystemView Manager component on an existing machine that already has all the prerequisite software installed.

- Redirected Installation

You can run the `INSTALL` command from a redirected drive. This method would usually be chosen when installing the SystemView Manager component on an existing machine that already has all the prerequisite software installed but does not have a CD-ROM drive attached.

1.3.2.1 Using the OS/2 Warp Server Integrated Installation

The OS/2 Warp Server integrated installation program allows you to select any of the components of OS/2 Warp Server for installation. It is accessed by creating two installation disks using the `CDINST` command, booting the system using the diskettes, and selecting an installation type. The OS/2 Warp Server integrated installation program allows you to select either an easy or an advanced installation.

Should you select the easy installation you will be given the choice to install the System Management Services. Should you choose to install the System Management Services, the following components will be installed automatically:

- Software Distribution Server
- License Use Runtime Server
- Software Distribution Object Preparation
- SystemView Administrator Console

You can install the rest of the SystemView in Warp Server components at a later time by using the Installation and Maintenance Utility. Although the Easy Installation installs operating system and MPTS on drive C:, you will be given a choice to select the drive for each of the other OS/2 Warp Server components.

The Advanced installation allows you more control over the installation.

Figure 2 on page 12 is the main installation panel. You may select the OS/2 Warp Server components you wish to install, including System Management Services.

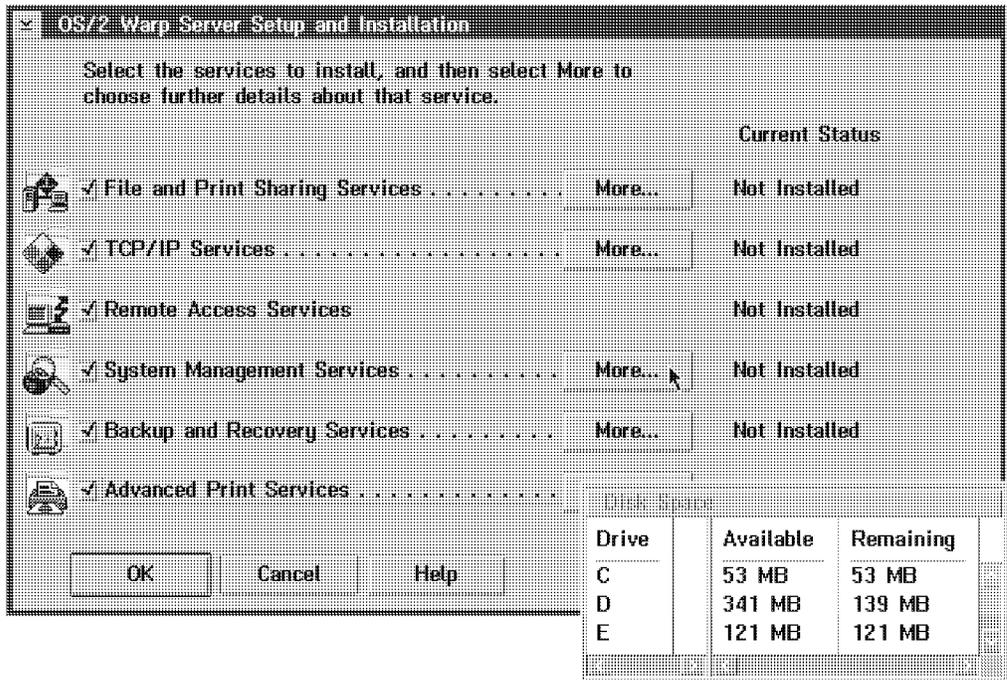


Figure 2. OS/2 Warp Server Advanced Installation Main Panel

If you select the **More** button, you will be presented with Figure 3 on page 13 where you may select which system management components you wish to select. These options are described in 1.2, “SystemView in Warp Server Components” on page 3. The following should be noted:

- The SystemView Administrator Console is not selectable; it is installed automatically because it is a prerequisite to all the other components.
- If you do not choose to install the License Use Runtime Server, the License Use Runtime Client will be installed.
- The SystemView Service Manager icon is substituted by the SystemView Service Client Manager icon if you do not install the Software Distribution Server component.
- The Distribution OS/2 Server folder is substituted by the Distribution OS/2 Client folder when you do not install the Software Distribution Server component.
- Additional components can be installed at a later stage.

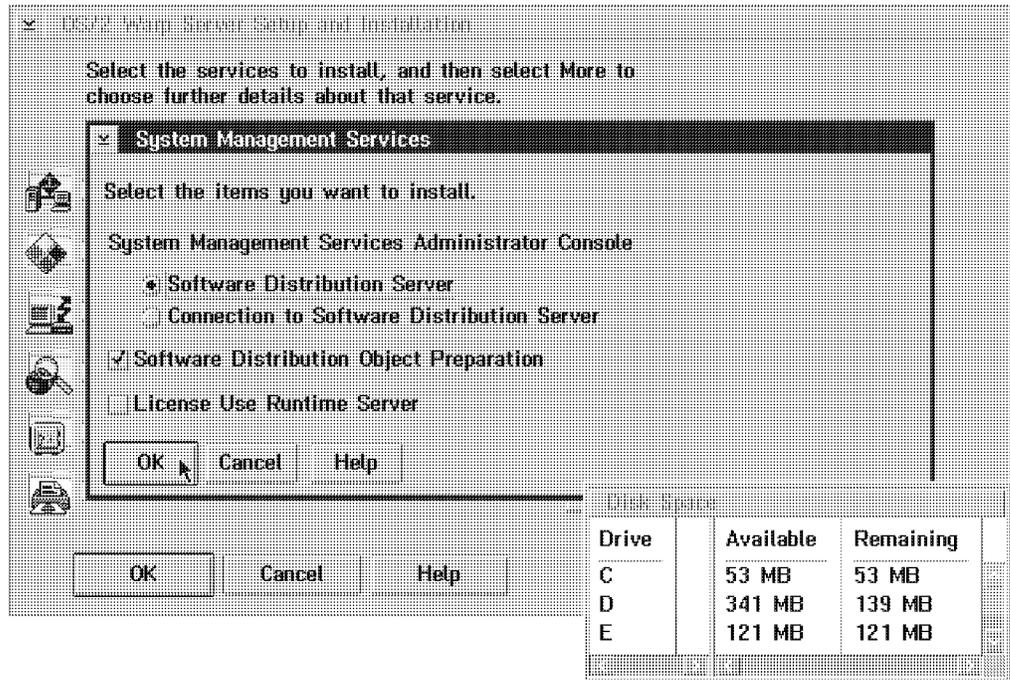


Figure 3. Systems Management Services Option Panel

Once the System Management Services and the components are selected, you will be required to enter configuration parameters. Defaults are generated for you, partly from the information you supplied in earlier panels. You may choose the defaults or modify them.

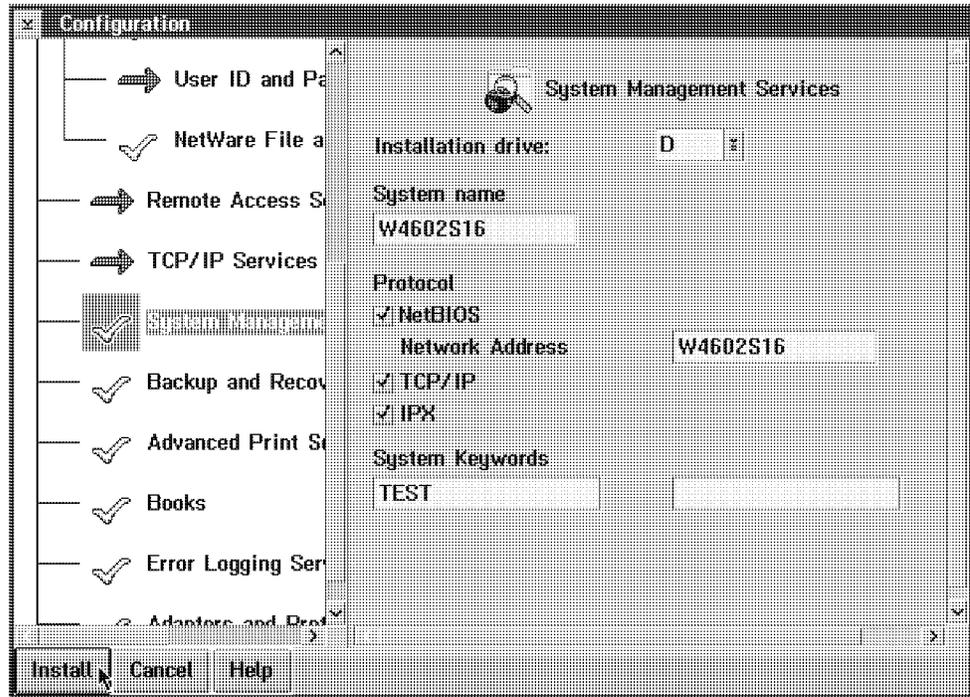


Figure 4. Systems Management Services Configuration Panel

As shown in Figure 4, you are required to supply the following information:

Parameter	Description
System name	<p>This is the name that this system will be identified by in the SystemView environment.</p> <p>This name can be, but is not required to be, the same as the NetBIOS name or TCP/IP hostname.</p> <p>The length of the name can be up to 16 characters, and special characters are not allowed</p>
System Keywords	<p>The system keywords will be used by the discovery process to identify your system in the SystemView environment.</p> <p>These keywords can be used to group the clients at the SystemView Manager. For example, we could use the keyword TEST, then when we create a group for all Warp Server machines, the discovery process will use this keyword to identify the machine.</p> <p>Note: Keywords are case sensitive.</p> <p>Some suggested keywords for grouping your system are:</p> <ul style="list-style-type: none"> • Department name (for example, marketing or technical support) • Department ID (for example, 5053 or YD-674) • Workstation role (for example, manager or client) • Workstation operating system (for example, OS/2 Warp, DOS)

Protocol Check the appropriate protocol box to enable the SystemView Manager to communicate with SystemView Clients using this transport protocol. You have to ensure that the SystemView Manager and SystemView Clients share a common protocol.

Once you have configured all the components, click on the **Install** button on the installation panel, and allow the installation to complete. You will be able to reconfigure or install additional components once the OS/2 Warp Server installation has completed.

1.3.2.2 Using SystemView INSTALL

The SystemView **INSTALL** program can be run off a local CD-ROM drive or off a redirected drive. It can also be run with or without parameters. See the online documentation for command line details. Figure 5 shows the component selection window when installing the systems management components using the **INSTALL** program.

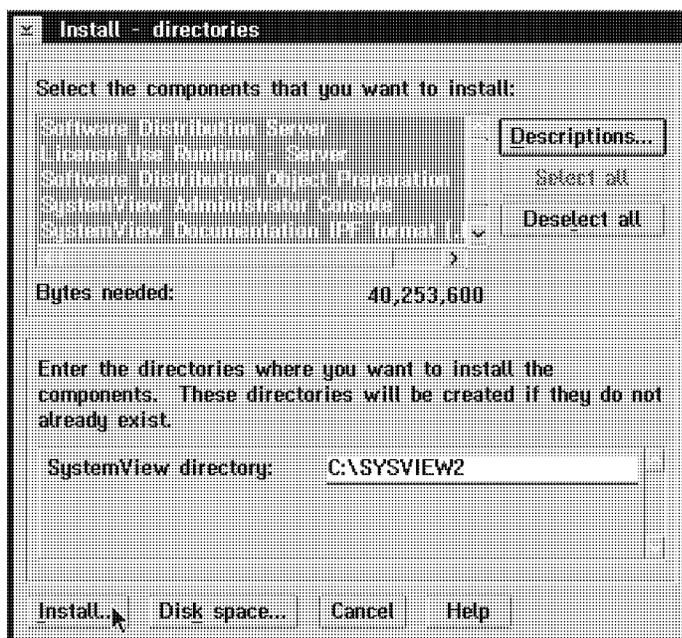


Figure 5. SystemView Manager Installation Panel

See 1.2, “SystemView in Warp Server Components” on page 3 for details on each of the components. During the installation procedure, you will be presented with the SystemView configuration notebook. For more information on the configuration, refer to 1.3.4, “Configuring the SystemView Manager” on page 19.

1.3.3 SystemView Client Installation

Like the SystemView Manager, there are a number of different installation methods that can be used to install both the SystemView OS/2 Client and SystemView DOS/Windows Client. The method you choose is often determined by the state of the existing client machines within your organization.

The following installation methods are possible:

- OS/2 Warp Server Client Installation

The most direct method of installation is using the OS/2 Warp Server integrated client installation program. This method is usually chosen when

installing the OS/2 Warp Server client components over existing OS/2 or Windows-based machines.

- **INSTALL**

You can install the SystemView OS/2 Client from the CD-ROM by using the `INSTALL` command from the `\CID\CLIENT\SYSVIEW\CLIENT_2` directory off the OS/2 Warp Server CD-ROM.

The SystemView DOS/Windows Client can be installed from the CD-ROM by using the `INSTALL` command from the `\CID\CLIENT\SYSVIEW\CLIENT_W` directory off the OS/2 Warp Server CD-ROM.

This method is usually chosen when installing the SystemView Manager component on an existing machine that already has all the prerequisite software installed.

- **Redirected Installation**

You can also run the installation commands from a redirected drive. This method is usually chosen when installing the SystemView OS/2 Client component on an existing machine that already has all the prerequisite software installed but does not have a CD-ROM drive attached.

1.3.3.1 Using the OS/2 Warp Server Client Installation

The client installation has to be started on an existing OS/2 Warp Server machine. The client installation program is contained in the OS/2 System Setup folder in the OS/2 System folder. The installation program creates two boot diskettes for the OS/2 Clients and a single diskette for Windows workstations. When creating the diskettes you will be prompted for the workstation adapter type.

The OS/2 Warp Server then starts a SRVIFS server, a code server utility, while waiting for both Windows and OS/2 clients to connect and start installing. Please refer to the online documentation for more information on using the OS/2 Warp Server Client Installation program.

SystemView OS/2 Client: When installing the OS/2 Warp Server Client, you will be prompted as to whether you want to install each of the components. One of the selectable components is the systems management Client. Should you choose to install this component, you will be presented with the configuration panel shown in Figure 6 on page 17.

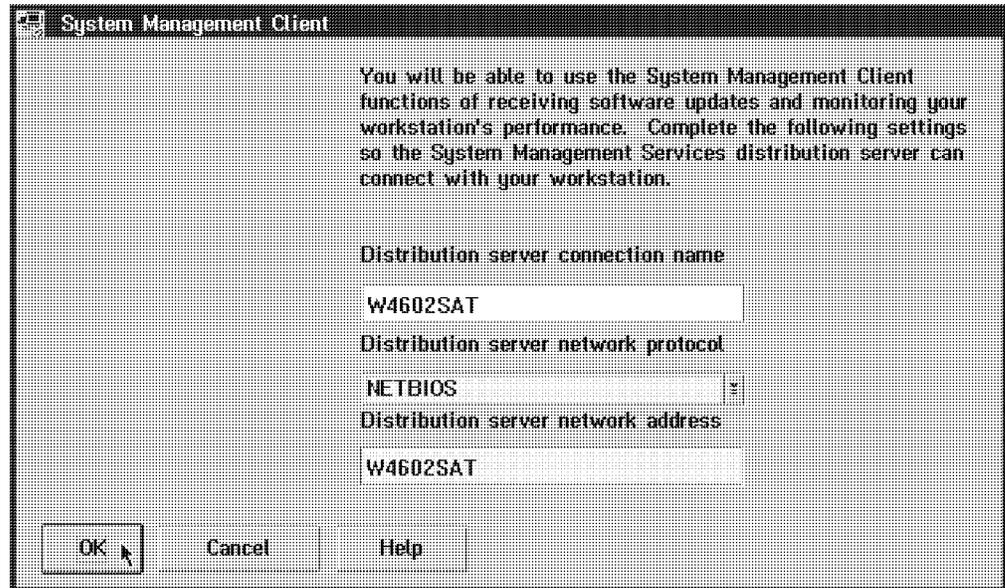


Figure 6. SystemView OS/2 Client Configuration Screen

You will need to configure the following parameters:

Parameter	Description
-----------	-------------

Distribution server connection name	This is the name of the distribution server this client will connect to. This name is specified when you define the SystemView Manager.
--	---

Distribution server network protocol	Specify here the protocol this client will use to connect to the Software Distribution Server. Note, it is up to you to ensure that both the Software Distribution Server and the Software Distribution Client support a common protocol.
---	---

Distribution server network address	This is the network address of the Software Distribution Server. This name is specified when you define the SystemView Manager.
--	---

Once you have configured all the components, select the **Install** button on the installation panel and allow the installation to complete. You will be able to reconfigure or install additional components once the installation has completed.

SystemView DOS/Windows Client: The SystemView DOS/Windows Client requires the same parameters as the OS/2 Client, as listed above. One difference is that the License Use Runtime-Client is available only for the OS/2 Client, not the SystemView DOS/Windows Client.

Once you have configured all the components, select the **Install** button on the installation panel and allow the installation to complete. You will be able to reconfigure or install additional components once the installation has completed.

1.3.3.2 SystemView INSTALL for OS/2

The SystemView `INSTALL` program can be run from a local CD-ROM drive or from a redirected drive for the SystemView OS/2 Client installation. It can also be run with or without parameters. See the online documentation for command line details. Figure 7 on page 18 shows the component selection window when installing the SystemView OS/2 Client using the `Install` program.

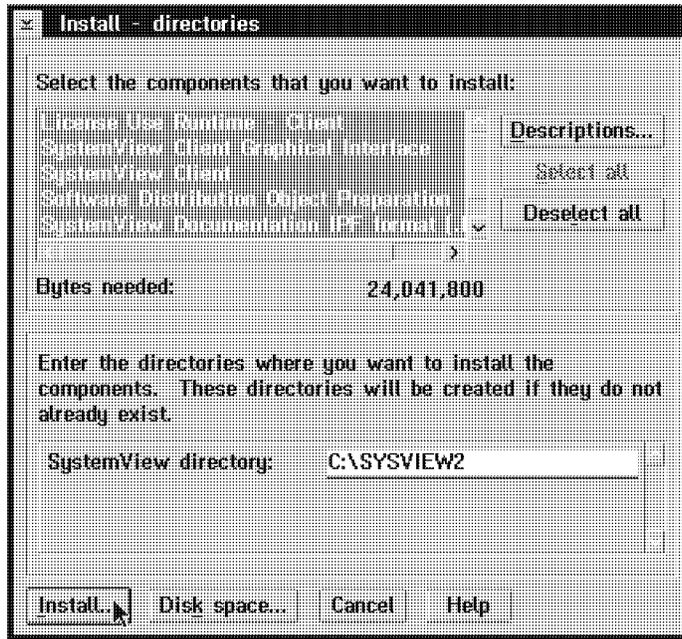


Figure 7. SystemView OS/2 Client Installation Panel

See 1.2, “SystemView in Warp Server Components” on page 3 for details on each of the components. During the INSTALL installation procedure, you will be presented with the SystemView configuration notebook. For more information on the configuration, refer to 1.3.4, “Configuring the SystemView Manager” on page 19.

1.3.3.3 Using SystemView INSTALL for Windows

INSTALL can be run from a local CD-ROM or from a redirected drive for the SystemView DOS/Windows Client. Figure 8 shows the component selection window when installing the SystemView DOS/Windows Client using the INSTALL program.

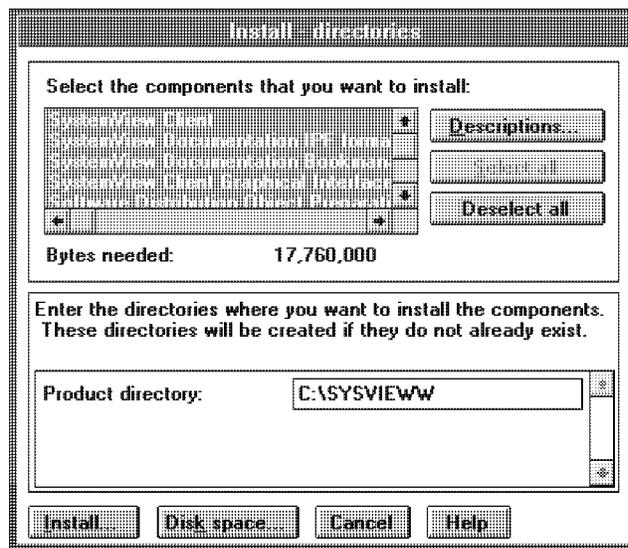


Figure 8. SystemView DOS/Windows Client Installation Panel

See 1.2, "SystemView in Warp Server Components" on page 3 for details on each of the components. During the INSTALL procedure, you will be presented with the SystemView configuration notebook. For more information on the configuration, refer to 1.3.4, "Configuring the SystemView Manager" on page 19.

1.3.4 Configuring the SystemView Manager

There are two ways to configure the SystemView in Warp Server network driver and other parameters:

1. During the OS/2 Warp Server integrated installation
2. From the SystemView Configuration icon in the SystemView in Warp Server folder

First page - General: Network Configuration Parameters:

The network drivers represent the communication paths available between the SystemView Manager and its clients.

Note

You can implement up to four SystemView network drivers (NetBIOS, serial connection, IPX/SPX, and TCP/IP) on each SystemView Manager or Client.

For example, if you configure the NetBIOS and the TCP/IP driver on the SystemView Manager, the SystemView Manager can communicate with SystemView Clients with either NetBIOS or TCP/IP, or both, configured.

Figure 9 shows an example of the first page of the SystemView configuration notebook.

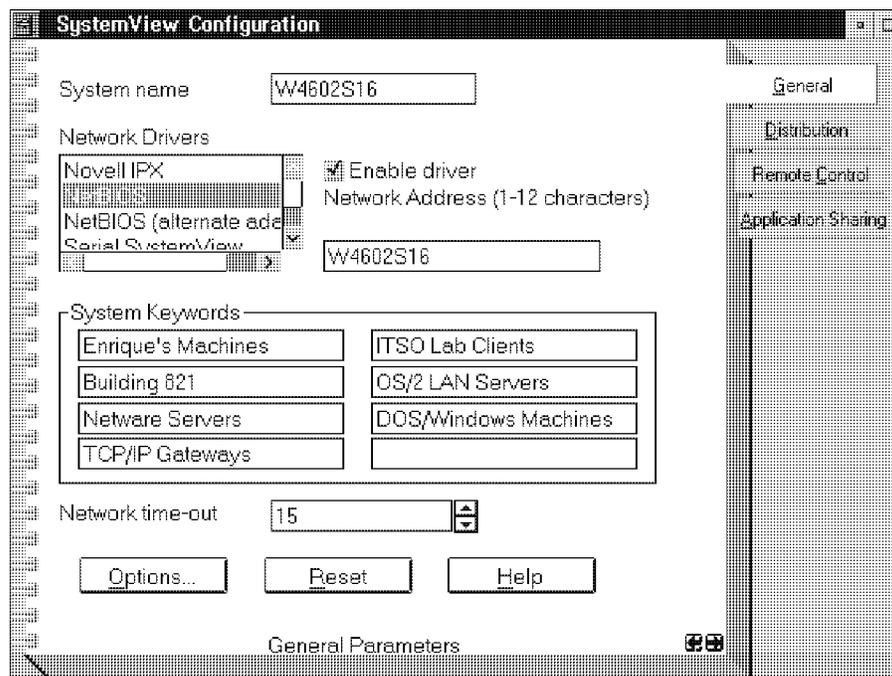


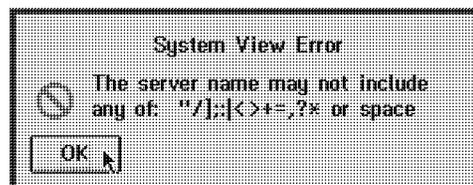
Figure 9. First Page of SystemView Configuration Notebook - General Network Parameters

Depending on the network driver you select, you may have to enter additional parameters that are required for that specific selection. When this information is required, after your selection of that network driver, an input field is displayed below the Enable Driver check box, and a description of this required information is displayed above the input field. Most network drivers that require additional information provide a default value for this field.

For example, if NetBIOS is selected, an input field is displayed below the Enable Driver check box, and the description of the Network Address (1-12 characters) field is displayed above, across from the System Name. Enter the information to continue, or accept the default value (which, for NetBIOS, is the LAN Requester machine name or the last eight characters of the burned-in address of the adapter).

Network drivers that do not require additional parameters depend on the existing configuration for the supported protocol.

Parameter	Description
System name	<p>This is the name of this system in the SystemView environment.</p> <p>This name can be, but is not required to be, the same as the NetBIOS name or TCP/IP hostname.</p> <p>The length of the name can be up to 16 characters, and special characters are not allowed (see Figure 10).</p>
System Keywords	<p>The system keywords identify your system to the SystemView environment. These keywords can be used to group the clients at the SystemView Manager.</p> <p>Note: Keywords are case sensitive.</p> <p>Some suggested keywords for grouping your system are:</p> <ul style="list-style-type: none"> • Department name (for example, marketing or technical support) • Department ID (for example, 5053 or YD-674) • Workstation role (for example, manager or client) • Workstation operating system (for example, OS/2 Warp, DOS)
Network time-out	<p>Defines the time-out that a SystemView managing application waits for a response from a client.</p>
Enable driver	<p>Check this box to enable the SystemView Manager to communicate with SystemView Clients over this transport protocol.</p>



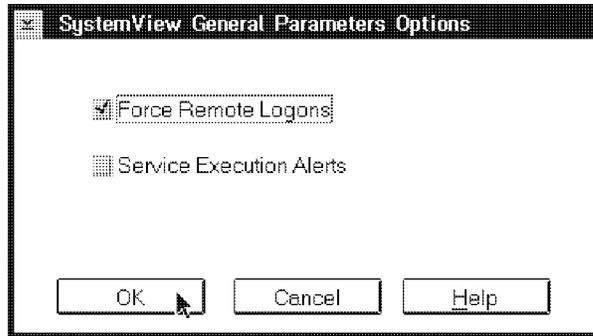


Figure 11. SystemView Configuration Options

Check **Force Remote Logons** to disable the public level of access to the system.

Check **Service Execution Alerts** if you want an alert to be generated every time a user at a remote manager starts a SystemView service at this system.

Second page - Distribution: Software Distribution Configuration Parameters:

Use the second page of the SystemView Configuration Notebook to select the software distribution configuration parameters, as shown in Figure 12.

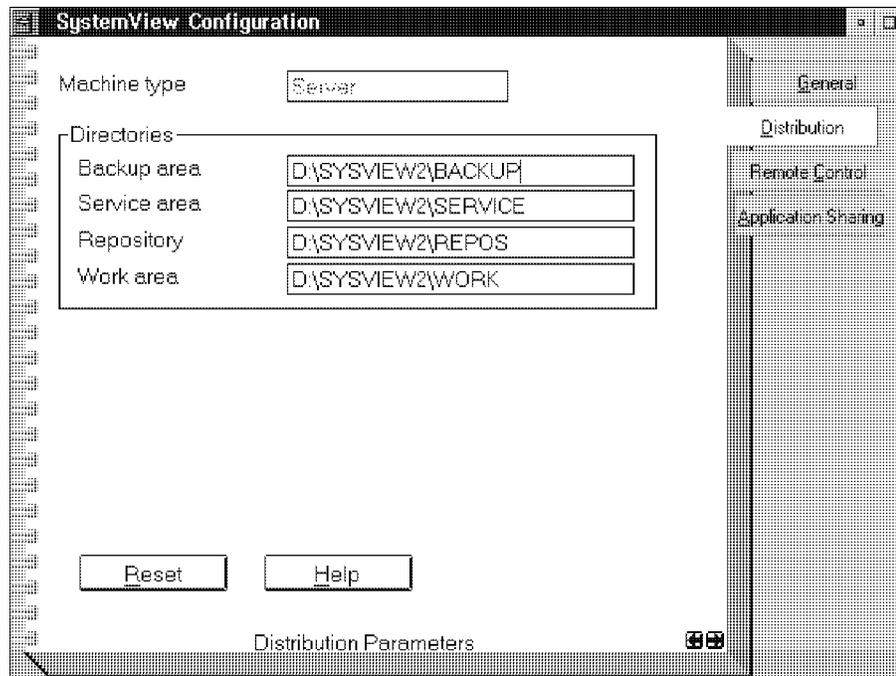


Figure 12. Second Page of Configuration Notebook - Software Distribution

Parameter	Description
Machine type	Software Distribution workstation role. Because you installed the Software Distribution Server component of SystemView, this entry is set to Server and cannot be changed.

- Backup area** An area where backups of previous levels of applications are kept. This is for applications installed that can be removed.
- For example, when you install Microsoft Word for Windows 2.0b on this machine and after six months you install Word for Windows 6.0, a backup of the previous version is stored in the backup area.
- This entry applies to applications installed through software distribution on this machine from another Software Distribution Server.
- Service area** Temporary area for installations.
- Repository** Subdirectory for profiles and software objects.
- Work area** Temporary area used by SystemView during the resolution of change-management requests.

Third page - Remote Control: Configuration Parameters for Remote Workstation Control:

Figure 13 shows an example of the third page of the SystemView configuration notebook. It's divided into the following fields:

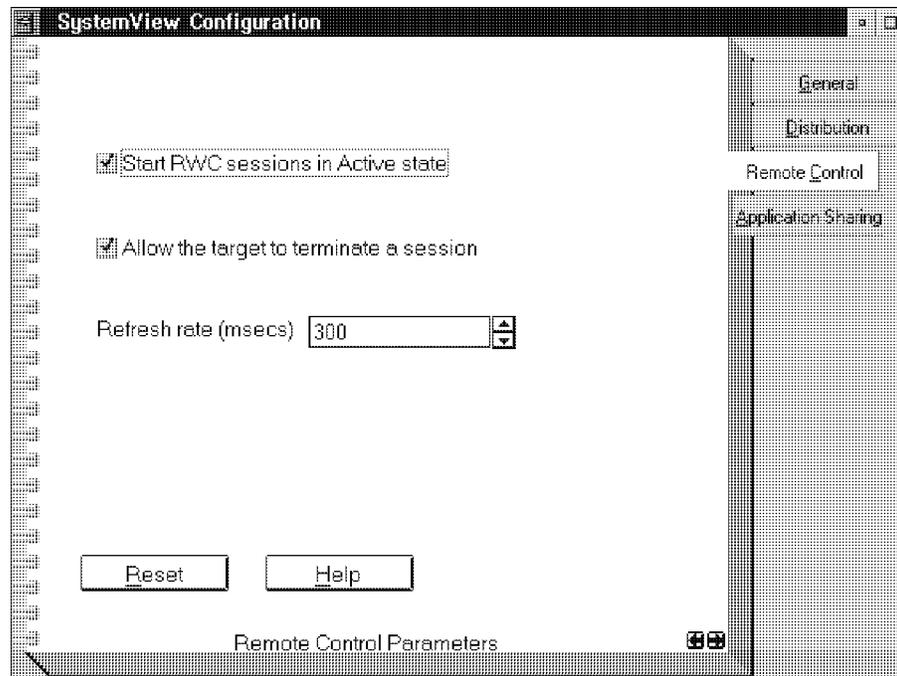


Figure 13. Third Page of Configuration Notebook - Remote Control

- **Start RWC sessions in Active state.** Sessions from remote SystemView Managers are started in an *active* state. In this state, the manager takes control of the keyboard and mouse of the client system.
In *monitoring* state, the manager copies the local display, but control of the keyboard and mouse remains with the client workstation.
- **Allow the target to terminate a session.** Select this box to enable the end-user to terminate the session by pressing **Alt+T**.

- **Refresh rate (msecs).** Defines the rate in milliseconds at which the display is refreshed at the remote workstation.

Fourth page - Application Sharing: Configuration Parameters Related to Application Sharing:

Use the 4th and last page of the SystemView Configuration Notebook to select parameters related to application sharing, as shown in Figure 14 and Figure 15 on page 24.

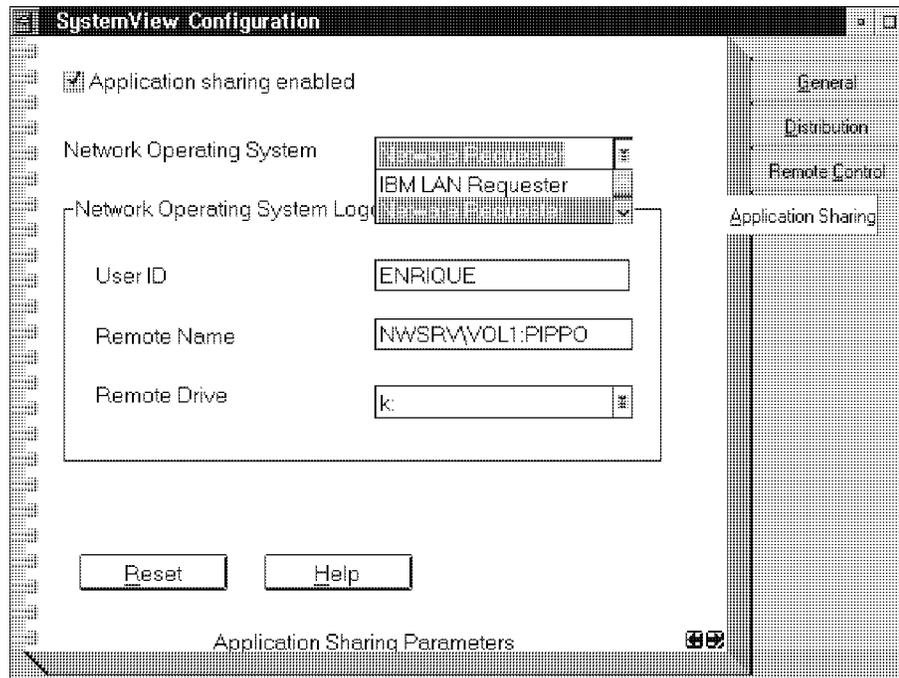


Figure 14. Fourth Page of Configuration Notebook - Application Sharing (Netware Server)

- **Application sharing enabled.** Select this box to activate application sharing.
- **Network Operating System.** Select the network requester type you use to communicate with the SystemView Manager.

The choices are:

- IBM LAN Requester
- Netware Requester
- NFS Client

- **User ID.** Enter the client logon ID to access the file server.
- **Remote name.** Enter the alias drive to be mounted for the remote shared directory.

Redirector	Net Name
LAN Requester	\\<ServerName>\<Alias>
NFS Client	<host>:<mount>
Netware Requester	<ServerName>\<VolumeName>:<directory>

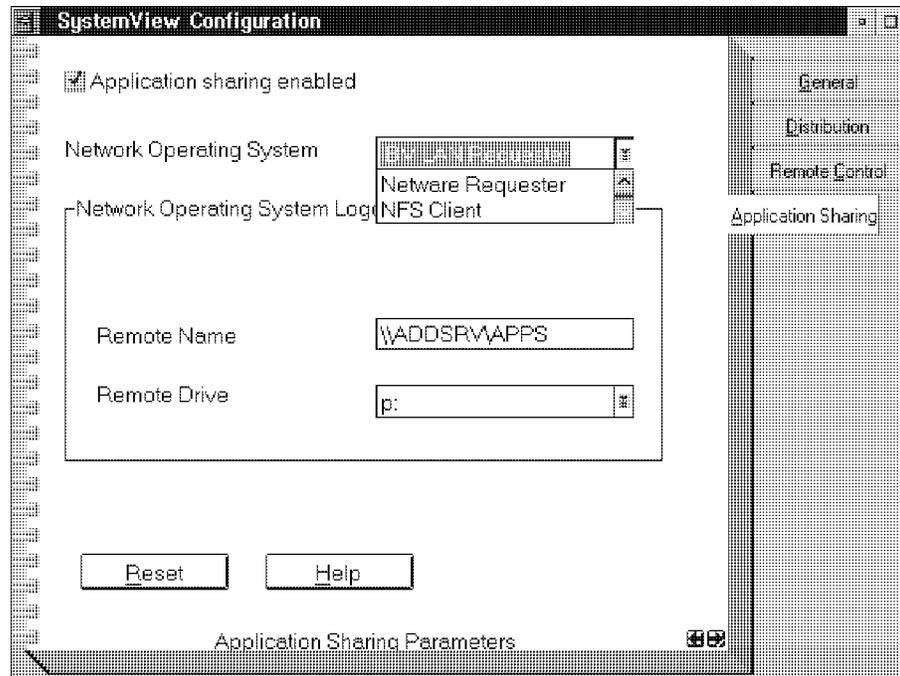


Figure 15. Application Sharing from an OS/2 LAN Server

- **Remote drive.** Enter the name of the drive that attaches to the shared directory.

1.3.5 Configuring the OS/2 Client

Using the SystemView configuration panels from the SystemView in Warp Server folder or through the OS/2 Warp Server integrated installation, you can configure the SystemView in Warp Server network driver and other parameters.

1st. page - General: Network Configuration Parameters:

Please see the section titled “First page - General: Network Configuration Parameters” on page 19 for a description.

2nd. page - Distribution: Software Distribution Configuration Parameters:

Use the second page of the SystemView Configuration Notebook to select the software distribution configuration parameters, as shown in Figure 16 on page 25.

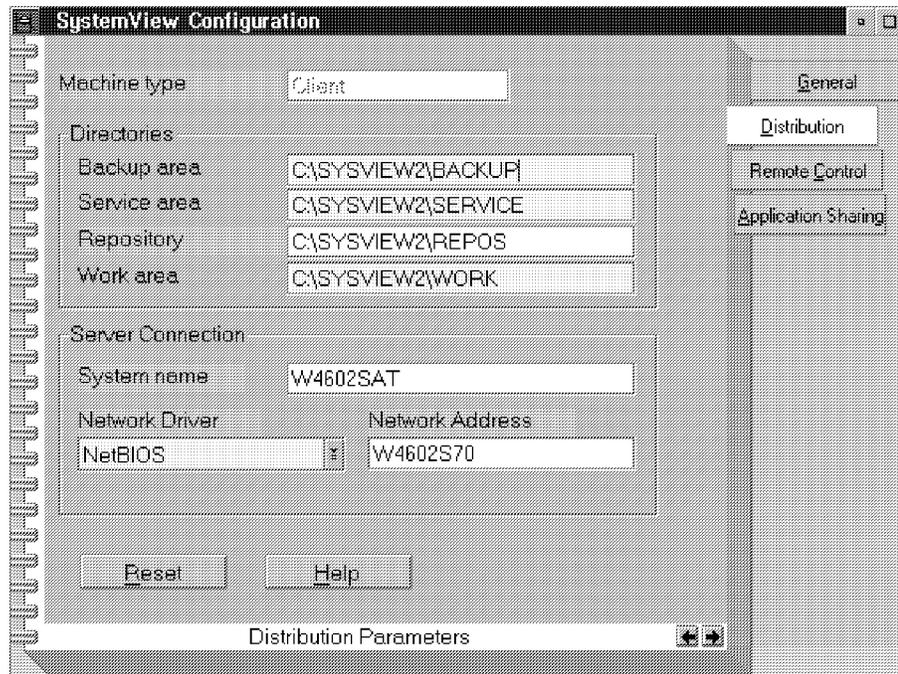


Figure 16. Second Page of the Client Configuration Notebook

Parameter	Description
Machine type	Software distribution workstation role. Because you installed the Software Distribution Server component of SystemView, this entry is set to Server and cannot be changed.
Backup area	An area where backups of previous levels of applications are kept. This is for applications already installed that can be removed. For example, when you install Microsoft Word for Windows 2.0b on this machine and after six months you install Word for Windows 6.0, a backup of the previous version is stored in the backup area. This entry applies to applications installed through software distribution on this machine from another Software Distribution Server.
Service area	Temporary area for installations.
Repository	Subdirectory for profiles and software objects.
Work area	Temporary area used by SystemView during the resolution of change-management requests.
System name	System name of the SystemView Manager workstation. The length of the name can be up to 16 characters, and special characters are not allowed (see Figure 10 on page 20).
Network Driver	Protocol used to connect to the Software Distribution Server. A drop-down list containing all the supported installed protocols on your workstation.

Network Address The network address of the distribution server.

If you select NetBIOS, enter the network address of the server which is in the General page of the server's configuration notebook.

If you select TCP/IP, enter the first token of the host name of the server.

If you select IPX, enter the 8-character network ID, followed by the 12-character node address for the adapter (which you can get from \IBMCOM\LANTRAN.LOG), followed by 869F.

3rd. page - Remote Control: Configuration Parameters for Remote Workstation

Control: Refer to the section "Third page - Remote Control: Configuration Parameters for Remote Workstation Control" on page 22.

4th. page - Application Sharing: Configuration Parameters Related to Application

Sharing.: Please refer to "Fourth page - Application Sharing: Configuration Parameters Related to Application Sharing" on page 23.

1.3.6 Installation and Maintenance Utility



Installation Utility

The SystemView in Warp Server Installation and Maintenance Utility or software installer utility can be used to:

- Determine which products' components are installed
- Determine which products' service level is installed
- Install add-on components of the product
- Update the product

When you select to update a product, you have the option of saving a backup of the current version of the product. You should note that additional disk space will have to be available for both versions to be on the disk.

- Restore the product

The product is restored to the previous level. The backup made during the update is restored, and the update is removed.

- Delete the product or components of the product

You also have the option to delete any backup versions that may have been saved on previous updates.

Figure 17 on page 27 shows the software installer window.

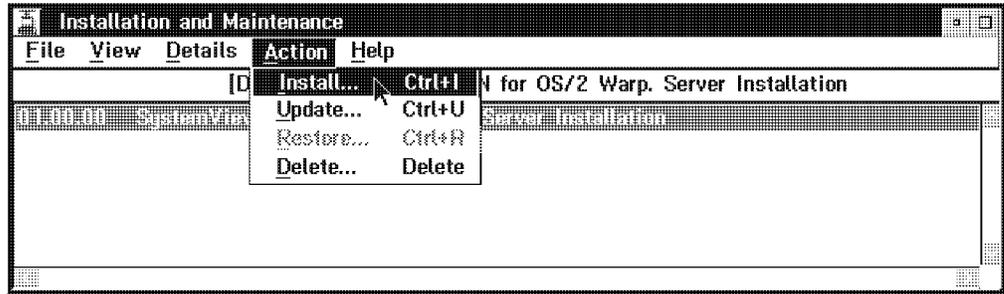


Figure 17. SystemView Installation and Maintenance Utility

The IBM OS/2 Warp Server product comes with several products that can be installed using the SystemView in Warp Server Installation and Maintenance Utility. These are shown in Table 3.

Product	File ICF	Location on the CD-ROM
CasePoint	CSEPNT.ICF	\BPIU\ASKPSP\CPINST
IBM SystemView Agent for OS/2	COMMONAG.ICF	\BPIU\CAG
Network SignON Coordinator	NSC.ICF	\CID\SERVER\NSC
IBM Print Server Facility/2	PSF2.ICF	\CID\SERVER\PSF2
SystemView in Warp Server Client Installation	SYSVCLI.ICF	\CID\CLIENT\SYSVIEW2\CLIENT_2
License Use Runtime Client	I4LS_CRK.ICF	\CID\CLIENT\SYSVIEW2\CLIENT_2
SystemView in Warp Server Services	KARAT.ICF	\CID\CLIENT\SYSVIEW2\CLIENT_W
SystemView in Warp Server Server Installation	IKOBASE.ICF	\CID\SERVER\SYSVIEW2\SERVER_2
License Use Runtime Server	I4LS_SRK.ICF	\CID\SERVER\SYSVIEW2\SERVER_2

```

*****
* SystemView Services for OS/2 Nvdma/2 Software Installer catalog file
*****

* Define the catalog.
* There is only one CATALOG entry in each catalog file.

CATALOG
  NAME      = 'SystemView LAN for OS/2 Warp. Server Installation',
  DESCRIPTION = 'Catalog of SystemView LAN for OS/2 Warp Server Installation'

PACKAGE
  * name that appears in the catalog list.
  NAME      = 'SystemView LAN for OS/2 Warp. Server Installation',
  NUMBER    = '5697-146',
  VRM      = '010000',
  FEATURE   = '0000',
  PACKAGEFILE = 'DRIVE: IKOBASE.PKG',
  PKGDESCRFILE = 'DRIVE: IKOBASE.DSC',
  SIZE      = '6000000'

* END OF IKOBASE.ICF CATALOG FILE

```

Figure 18. Installed Catalog File Example

1.3.7 Product Removal Considerations (Deinstallation)

To deinstall the product, you can use the SystemView in Warp Server Installation and Maintenance Utility. Select the **SystemView Catalog** and select **Delete**. You will be prompted for the components that you wish to delete. Select the components and delete them.

1.4 SystemView Architecture

SystemView consists of a number of services that can be started on either the local or the remote machine. Each service performs in the same way, both locally and remotely. Starting the service on a remote machine is just like starting the same service on the local machine; it's as if the user is sitting in front of the remote machine.

This way of processing is internally called *passthru*. It is seen from the perspective of the user using the Remote System Manager and passing through the selected workstation. The process can be iterated if the selected workstation is a SystemView Manager itself.

The above is achieved by the manner in which the SystemView services have been structured. Each SystemView service has two executables associated with it:

- Base component
- Graphical User Interface (GUI) component

The component that installs the GUI component on the SystemView Client is the SystemView Client Graphical Interface. The GUI component on the administrator is called the SystemView Administrator Console.

The administrator should always have the GUI for all the services installed because managing client workstations may require services that the administrator machine does not support. The corresponding base component may, however, not always be present.

On the client, SystemView installation will only install services that apply to the machine on which the code is installed.

When the user starts a service on a SystemView machine, the following things happen:

1. The related base component is started on the selected system and is waiting for requests.
2. The related GUI component is notified on the local system.
3. The GUI asks the base for initial information via the SystemView Transport.
4. The GUI shows the data to the end user, waits for the end-user request, and routes the request to the base in order to process it.
5. The GUI displays the user request results.

SystemView Machine

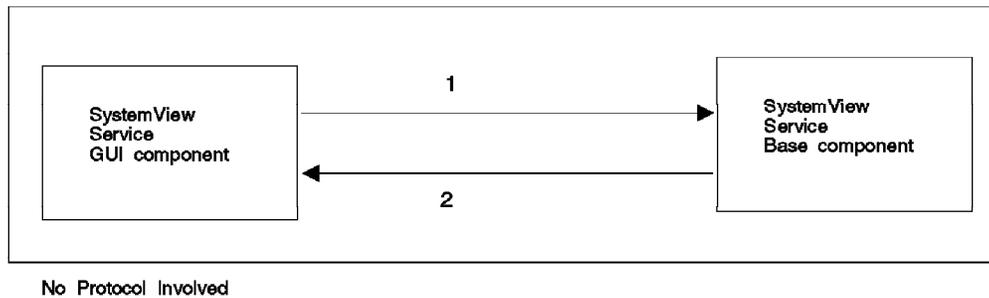


Figure 19. Local Execution of SystemView Services

Figure 19 shows the SystemView services being executed on a machine. Since the machine is querying local services, no transport protocol is required.

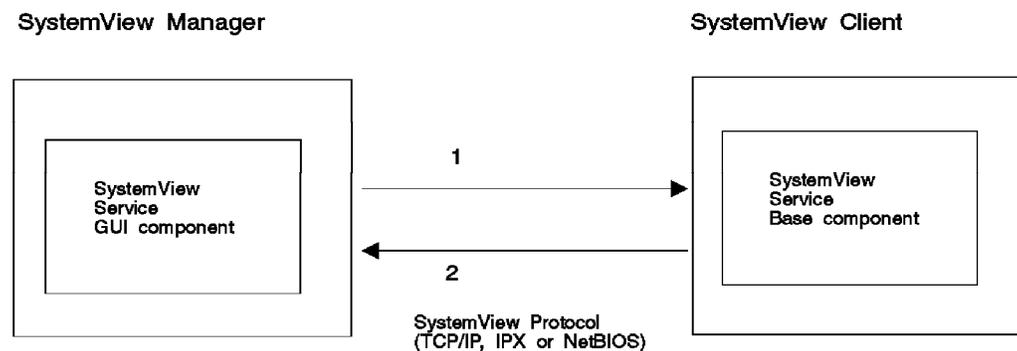


Figure 20. Remote Execution of SystemView Services

Figure 19 shows the SystemView Manager querying services on a remote SystemView Client. The only additional component active in this figure versus Figure 19 is that a protocol is required for communication between the GUI and base components. Both, the GUI and base components react in exactly the same way whether they are providing services for a local or a remote machine.

When the user stops a service on a SystemView machine, the following things happen:

1. The related base component is stopped on the selected system.
2. The related GUI component is stopped on the local system.

Note: The base component can provide service to one GUI at a time or to multiple GUIs, depending on the service itself.

1.5 Getting Started

After installing SystemView in Warp Server, you will have a SystemView System Management folder on your desktop. All the SystemView functions are contained in this folder.

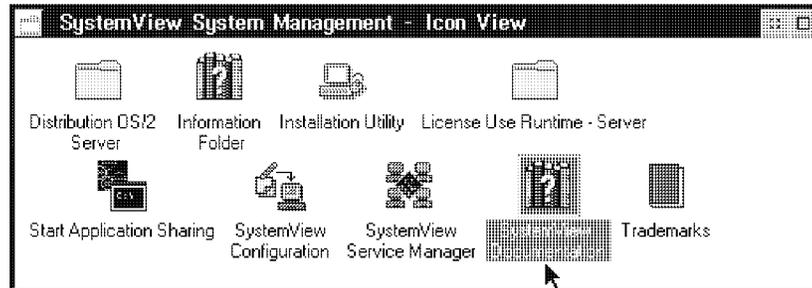


Figure 21. SystemView Folder

Figure 21 shows the contents of the folder. The contents of the folder will vary depending on the components chosen during installation. In Figure 21, the SystemView applications are contained in the SystemView Service Manager folder. Administrator workstations will have an additional SystemView service, the Remote System Manager, that enables them to access services on the client workstations. Other services that are installed are specific to the machine on which they are installed.

When SystemView starts up, it launches a detached process called the SystemView LAN Support program. This program initializes the selected protocols, such as NetBIOS, TCP/IP and IPX. Once the transport initializes the SystemView services are accessible remotely. If you stop this process, it will be started up each time you start the SystemView Service Manager.

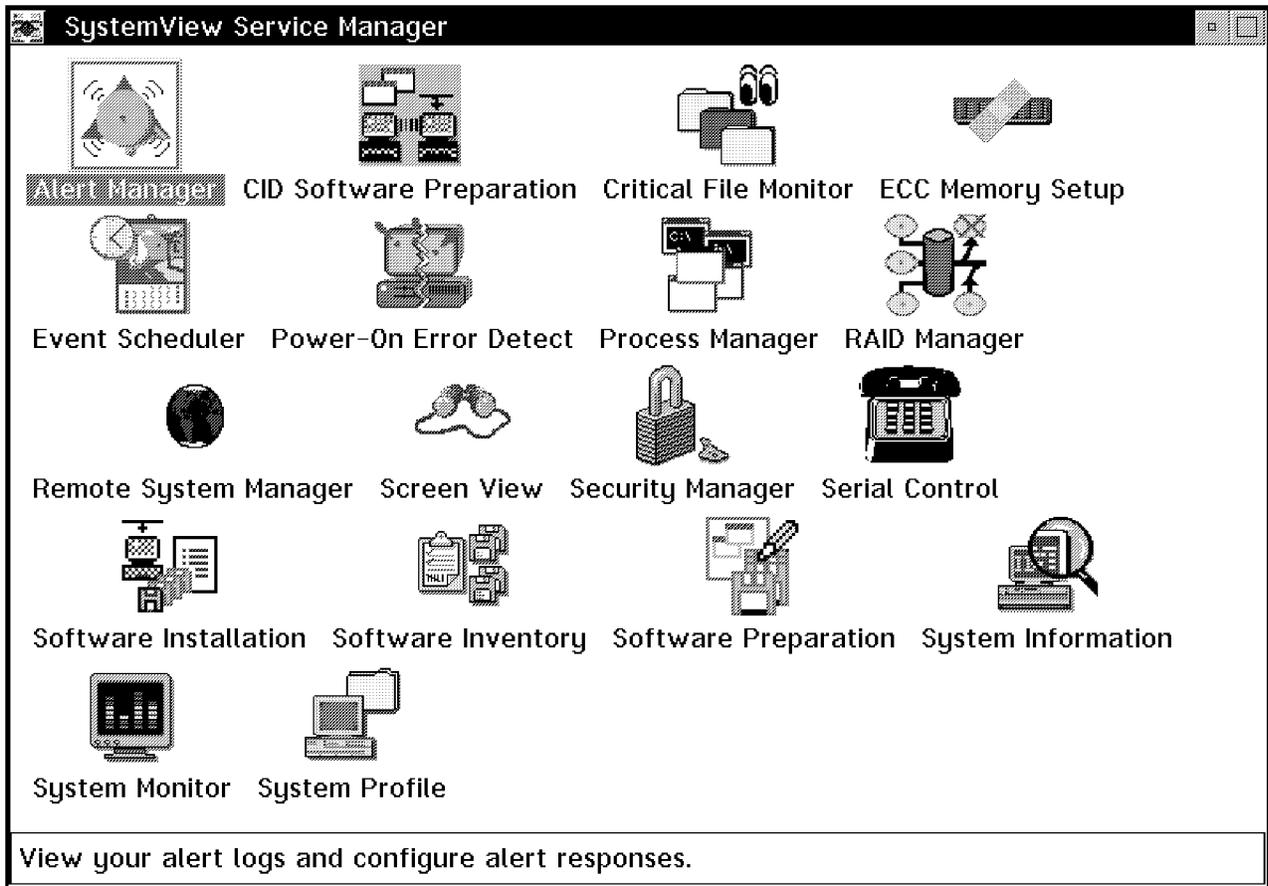


Figure 22. SystemView Service Manager

Figure 22 shows the SystemView services installed on a system management workstation. All services in this window are the GUI components for access to the locally installed base components. In order to access remote machines, a Remote Systems Manager is provided. This is only available on SystemView Manager machines. This service provides you with access to the GUI for the services on remote machines.

1.6 Managing Client Systems in the Network

Client systems are accessed in the network using the Remote System Manager. The administrator can quickly and easily set up groups of client systems to be managed. For the administrator to access a client system, that system must be defined as a member of a group (even if it is a group with only one member).

1.6.1 Creating a Group

It is best to create groups based on some logical structure. For example, you could create a group called Accounting that would consist of all machines that are in the Accounting department. This will make it easier for you to find the machine when a problem occurs.

The group creation process uses the keywords that were assigned to the client systems during installation (for more information, please see "First page - General: Network Configuration Parameters" on page 19 and Figure 9 on page 19).

To generate the groups shown in our example, we used the the following keywords:

- ITSO - for ITSO machines
- Test Lab - for machines in the Test LAB
- Warp Server - for equipment used in the Warp Server Project
- OS/2 - for OS/2-based machines
- MCA - for Micro Channel machines in the network

Figure 23 shows an example of a systems management group built using some of the keywords defined above.

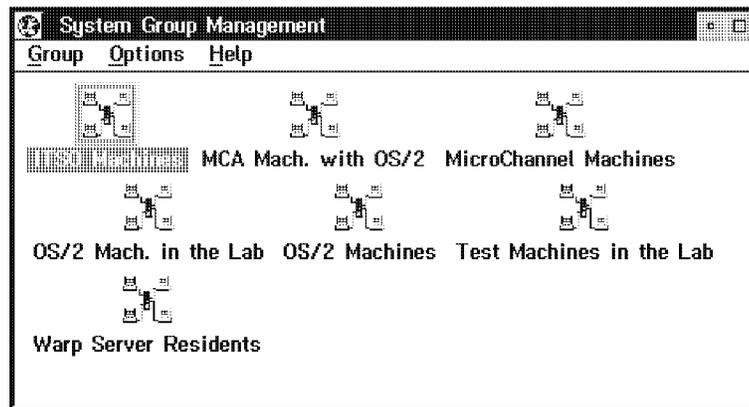


Figure 23. Group Definition Examples

To create a new group, select the **Add Group** option from the Group pull-down menu. The Add System Group window, shown in Figure 24 on page 33, is displayed.

You specify here the conditions for a managed system to belong to the group.

Note: Adding a group *does not* put any managed systems into the group. The discovery process puts managed systems into a group. So, after the creation of a new group, you need to open the new group, and click on **System** and **Discover Systems** to obtain all managed systems that belong to that group.

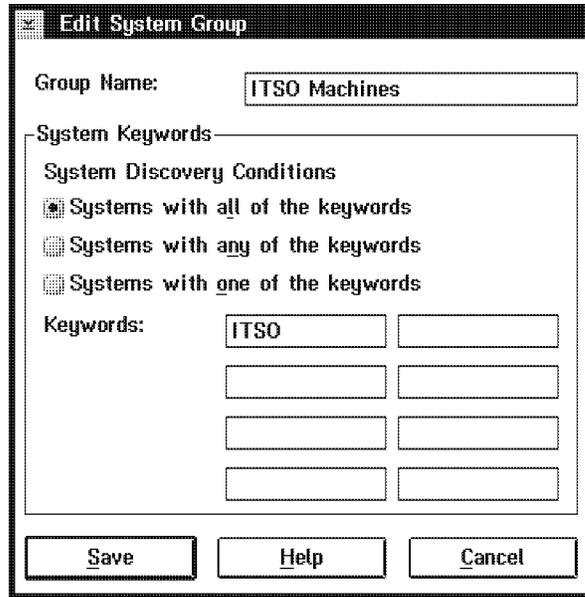


Figure 24. Adding a New Management Group

1.6.2 Using Discovery Filters

In addition to using keywords, the administrator can restrict systems in a group to those that use a:

- Specific operating system, or a
- Specific communications protocol

Open the system group, and then select **Group Discovery Filters** (see Figure 25 and Figure 26 on page 34).

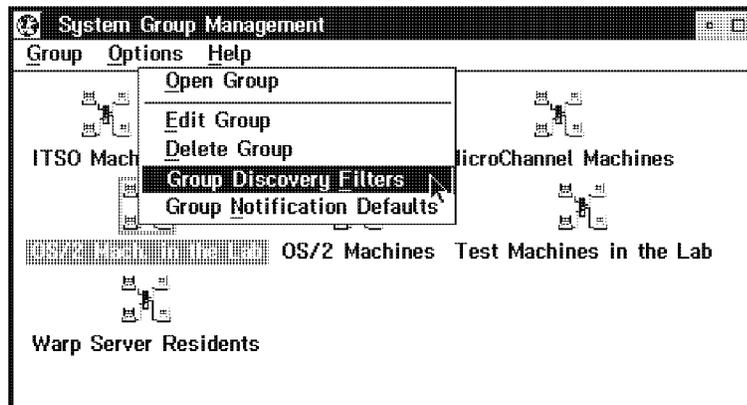


Figure 25. Selecting Group Discovery Filters

In the example in Figure 26 on page 34, only TCP/IP and NetBIOS, and only machines with OS/2 and MS Windows, have been chosen for the Group Discovery.

The rest of the machines, even those having the same keywords, will not apply for the group.

Note: Having this alternative for filtering, it makes no sense to define a keyword as OS/2, Windows, TCP/IP, or Novell, for example.

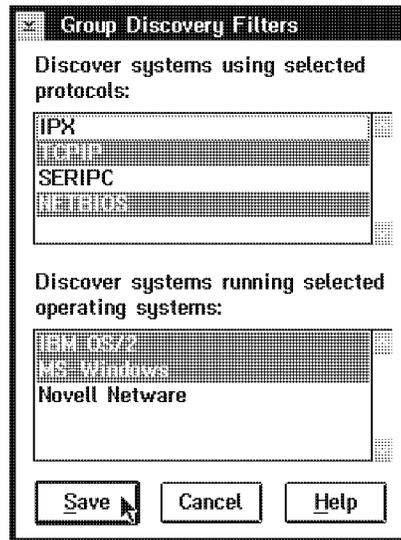


Figure 26. Group Discovery Filter Options

1.6.3 Discovering Systems in a System Group

You can start the discovery process in two ways:

- From the System Group Management window, select **Discover Systems in All Groups** from the Group pull-down menu.
- Open the system group, and then select **Discover System** from the System pull-down menu.

In either case, SystemView sends a short message over the LAN requesting that any remote systems that have the specified keywords assigned acknowledge their presence on the LAN.

The remote systems that have the correct keywords then send a response to the system that initiated the discovery process. This response contains all of the information necessary to add the individual system to the system group (System Name, Network Address and Network Type). The individual remote systems are then automatically added to the system group. Icons representing each of the remote systems appear in the System Group window, sorted alphabetically. Figure 27 on page 35 shows an example of an icon view of all systems in the network. Most of the machines are running NetBIOS, but there are a small number of them that are running TCP/IP and IPX. There are a set of Micro Channel machines and some ThinkPads.

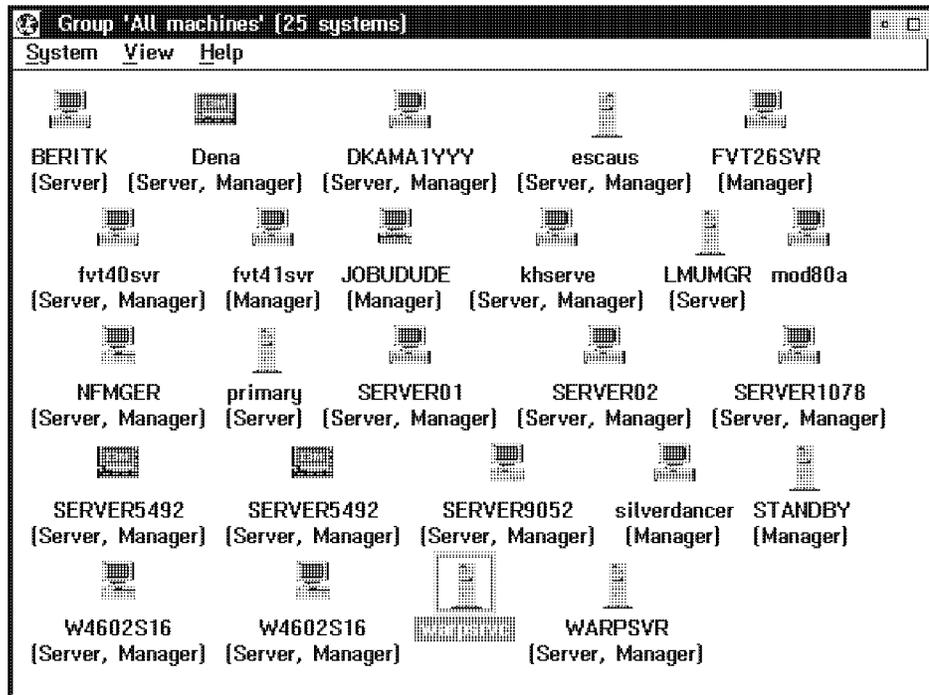


Figure 27. Icon View of All Systems in the Network

Figure 28 on page 36 shows a detail view of the same example. You can see:

- Icon showing the machine
- System Name
- Network Type
- Network Address
- System Model
- Operating System (not shown)
- Presence Check Interval (not shown)
- ON/OFF Notify Service (not shown)

Group 'All machines' [27 systems]				
System View Help				
	System Name	Network Type	Network Address	System Model
	SERVER1070 [Server, Manager]	NETBIOS	5A8864A1	IBM PS/2 Model 90 XP
	SERVER5492 [Server, Manager]	TCP/IP	os2itsc6.austin.ibm.com	IBM PS/2 Thinkpad 755
	SERVER5492 [Server, Manager]	NETBIOS	SERVER54	IBM PS/2 Thinkpad 755
	SERVER5492 [Server, Manager]	IPX	7007.4EEEEEEEEEE0	IBM PS/2 Thinkpad 755
	SERVER9052 [Server, Manager]	NETBIOS	5A1D2F04	IBM PS/ValuePoint
	silverdancer [Manager]	NETBIOS	SILVERDA	
	STANDBY [Manager]	NETBIOS	SERVER3C	IBM PS/2 Model 95 XP
	W4602S16 [Server, Manager]	TCP/IP	os2itsc4.austin.ibm.com	IBM PS/2 Model 77 I/S
	W4602S16 [Server, Manager]	NETBIOS	W4602S16	IBM PS/2 Model 77 I/S
	WARPSVR [Server, Manager]	IPX	7007.00005A00400E	IBM PS/2 Model 77 I/S
	warpsrv	NETBIOS	warpsrv	IBM PS/2 Model 85 486
	WARPSVR [Server, Manager]	NETBIOS	5AC45E92	IBM PS/2 Model 95 XP

Figure 28. Detail View of All Systems in the Network

Figure 29 on page 37 shows an example of how we classify a typical System Group Management in our network:

- All machines. Neither restriction nor keywords set.
- IPX Machines. Using Group Discovery Filters (see Figure 25 on page 33 and Figure 26 on page 34) and selecting only machines that run IPX.
- TCP/IP machines. Using Group Discovery Filters and selecting only machines that run TCP/IP protocol.
- NetBIOS OS/2 Machines. Using Group Discovery Filters and selecting only OS/2 machines that run NetBIOS protocol.
- Micro Channel Machines. Machines that have one keyword set as MCA (see Figure 24 on page 33).
- ThinkPads. Machines that have one keyword set as TP.

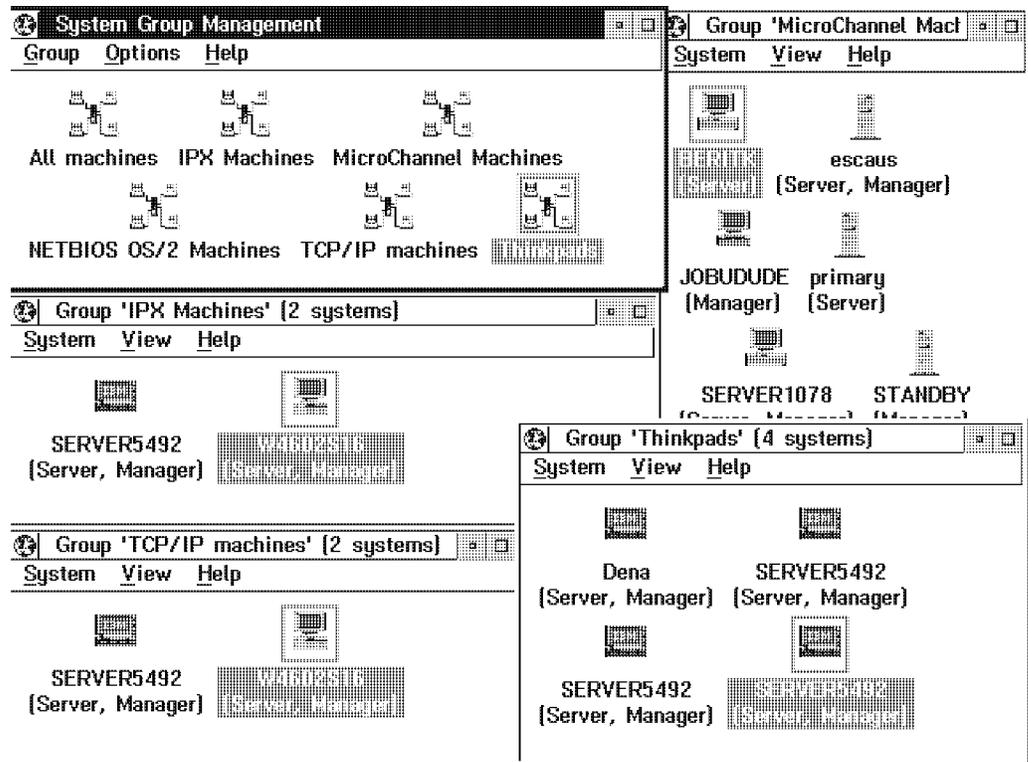


Figure 29. System Group Management Classification Example

You can compare the systems that belong to every defined group with the detailed information provided in the Figure 28 on page 36.

1.6.4 Accessing Remote Machines

Once the groups have been set up and the discovery process has added the machines to the group, you will be able to access the remote machine. You can either access the remote machine by double clicking on it, in which case you will be presented with the systems management applications available on that machine, or by using the right mouse button.

If you click with the right mouse button on each icon representing a system, you will have the following additional functions available (see Figure 30 on page 39).

Function	Description
Open System	Access to all management functions available for that machine.
Edit and Delete System	Manipulate the information contained in the icon.
System Restart	Restart the remote system.
Presence Check	Query whether the managed system is active. If a managed system becomes inactive during operations, its icon is grayed out, and it cannot be opened for communication. When the system becomes active again, the SystemView Manager will recognize the remote system is active again. Presence check

forces the SystemView Manager to check the remote system's status immediately.

Login System

Override an outgoing user ID/password for that system. If the system has more than one user ID/password combination to allow access to the system's services, this option can be used to try a combination without destroying the current outgoing user ID/password combination.

System Notifications

Notify when the selected managed system goes online or offline.

Set User ID and Password

Set the user ID/password combination that will be used automatically when opening this system. Using the Set User ID and Password option yields the same results as using the Set Outgoing User ID and Password option in the Security Manager (for more information see 1.7, "Implementing Security" on page 40).

Set Keywords and System Name

View or change the selected system's keywords or name. Changing the system's keywords and system name can enable you to better organize your system groups through effective use of the discovery process.

Note:

1. To view a system's keywords, you must have at least PUBLIC access to one or more of the system's SystemView services.
2. To change a system's keywords or system name, you must have access to the system's Security Manager service, or you must have a specific user ID and password configured and saved for that system.

Error Conditions

Open the system's Error Condition Log window. This section will not be available if the Error Condition Log is empty.

Error Conditions are generated by the Alert Manager in response to alerts. Error Conditions simply alert the Remote System Manager that a significant event has occurred on one of the systems on the LAN. When you configure the Alert Manager to generate an Error Condition in response to an alert, you must specify a name for the Error Condition. When the Alert Manager generates an Error Condition, it will place an Error Condition entry, using the name you specified, in the Error Condition Log of the system that generated the alert.

If a system currently has one or more entries in its Error Condition Log, its individual icon is replaced by a generic system icon with a red circle and slash symbol. Any system groups in the System Group Management windows that contain this system also change. This will help to alert you that the system group contains one or more systems that have entries in their Error Condition Logs.

Error Conditions can be cleared in either of two ways:

- Generate a Clear Error Condition message with the Alert Manager.

When the Alert Manager generates a Clear Error Condition message, it clears only one identically named Error Condition from the log.

- Select **Reset** from the Error Condition Log window.

This clears all Error Conditions from the log.

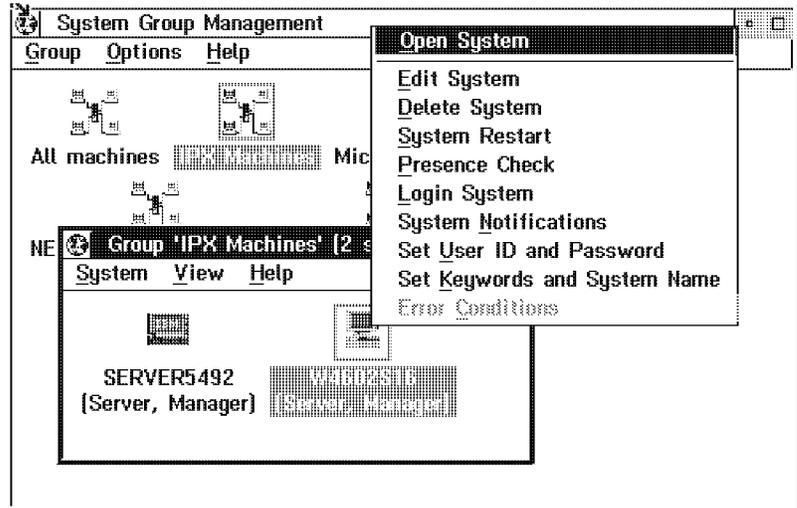


Figure 30. System Icon Context Menu

Figure 31 shows the pop-up menu corresponding to Group Management.

You can:

- Open, Edit and Delete one group
- Set Group Discovery Filters
- Set Group Notification Defaults

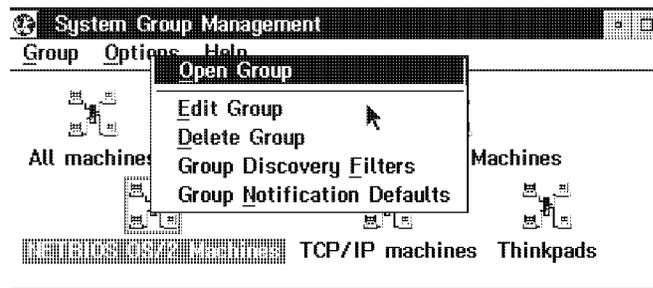


Figure 31. Group Icon Context Menu

The process of assignment, changing, or deletion of group keywords requires you to have SystemView administration privileges.

1.7 Implementing Security



Security Manager

Once you have access to the remote systems and the SystemView Manager applications, one of the first items that need to be addressed is security. Due to the nature of the SystemView product, misuse could lead to the loss of valuable data. In order to protect data that exists on the network from malicious intent or ignorance, security is included. The security is configured using the Security Manager which is designed to help prevent network access to some or all of the SystemView services to which a SystemView Manager workstation has access.

Both the SystemView Server and the SystemView Clients have the Security Manager installed. This is contained within the SystemView Service Client or Manager folder. The following services pose the most potential risk if used irresponsibly:

- Remote System Manager
- System Partition Access
- File Transfer
- Remote Session
- Remote Control
- Process Manager
- RAID Manager

1.7.1 Configuring the Security Manager

The Security Manager uses a User ID and password combination to determine which services are available to the managing system.

On each managed workstation, an incoming User ID has to be defined. On each managing workstation, an incoming and an outgoing User ID has to be defined.

When a managing workstation attempts to access services on a managed workstation, the outgoing User ID/password of the managing workstation is matched against the incoming User ID/password of the managed workstation. If there is a match, then the corresponding services are made available to the managing workstation.

1.7.1.1 Setting Up the Incoming User ID/Password on a Manager

To configure the incoming User ID/password combination you need to complete the following tasks:

1. Start Security Manager.
2. Select **Edit/Display Incoming passwords**. Figure 32 on page 41 will be displayed.

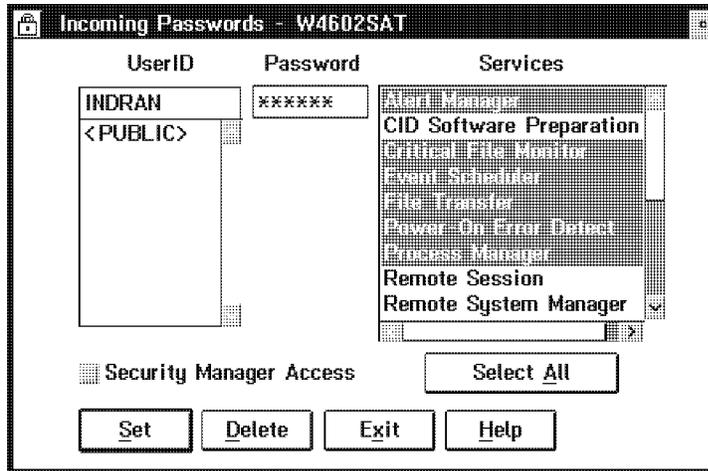


Figure 32. Incoming User ID / Password Configuration

3. Enter a User ID.

The User ID may be between 1 and 16 characters in length. The userid can contain any standard ASCII characters.

If you are editing a User ID, select the ID off the User ID list and perform the changes.

4. Enter a Password.

You are required to enter a password for each User ID. The password must be from 1 to 8 characters in length. The password can contain any standard ASCII characters. The password will not be displayed when you enter it.

5. Select one of the available Services.

Select one or more services from the Services selection list. The selected services will be available to users who provide the user ID and password you have entered in the corresponding fields.

6. Determine access to the Security Manager.

Select the Security Manager Access check box to allow access to your Security Manager.

Note: Allowing access to the Security Manager enables the remote system to alter your User IDs and passwords and enable or disable the services available. This will also enable the Remote System Manager's System Restart operation on your system; that is, it will enable the remote manager to reboot your system on demand.

In Figure 32, the User ID *INDRAN* is being created with access to the highlighted services and with no access to the Security Manager.

1.7.1.2 Setting Up the Outgoing User ID/Password on a Manager

To set the outgoing User ID/Password combination and determine access to services:

1. Start Security Manager.
2. Select **Edit/Display Outgoing Passwords**.
3. Select **Add**. This opens the Edit Outgoing Passwords window as displayed in Figure 33 on page 42.

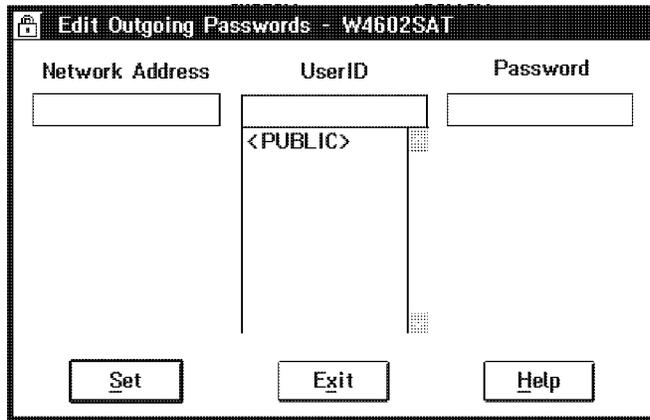


Figure 33. Outgoing User ID / Password Configuration

4. Enter a Network Address.

In the Network Address entry field, type the Network Address of the system for which you are creating the outgoing User ID/password combination. This address must be identical to the Network Address used by the Remote System Manager to locate the remote system. This address is specified on the first page of the SystemView Configuration Notebook.

5. Enter a UserID.

Select a User ID from the selection list, or type a new User ID in the UserID entry field. This User ID will be used (along with the password) when you attempt to access the remote system. The User ID may be between 1 and 16 characters in length and can contain any standard ASCII characters.

6. Enter a Password.

Type the password that will be used in combination with the specified user ID to attempt to gain access to the remote system. The password must be from 1 to 8 characters in length. The password can contain any standard ASCII characters. The password will not be displayed.

7. Save your outgoing user ID/password configuration.

1.7.1.3 How the Password Checking is Done

If you do not define an Outgoing Password for a SystemView Manager and you attempt to gain access to the SystemView services, the following occurs:

1. If any service on User ID PUBLIC is enabled on SystemView client, you will be given access to those services without specifying a user ID/password.
2. If you choose to log in to a system by using the Context menu for the particular workstation, you will be given access to the security services that have been defined for that user ID.
3. If PUBLIC has all services disabled and another user ID has been defined, you will be asked to specify a User ID and Password.
4. If you are asked to save the User ID and Password as a default, this will be the default when you access this workstation and will override the PUBLIC access.

If you define an Outgoing Password for a SystemView Client at a SystemView Manager and you attempt to gain access to the SystemView services, the following occurs:

1. If the Outgoing Password matches an Incoming Password on the managed station you are given access to the related services.
2. If the Outgoing Password does not match an Incoming Password on the managed station, you will be given an opportunity to specify one and save it as the default. Once you define an Outgoing User ID/Password combination for a system, you will be forced to logon. You can no longer use the PUBLIC access defined on the remote system.

You can override the option to save the User ID and password combination in the SystemView Configuration Notebook. See “First page - General: Network Configuration Parameters” on page 19. Using the **Options** button on the first page you can select to **Force Remote Logons**. The managing system will then not be able to save user ID/password combinations as defaults. This will force you to manually log on to any remote system that you want to access each time you access that system. If you do not have a User ID/password defined for a remote system you will be given PUBLIC access.

To improve the security within your SystemView system, you should define an Outgoing User ID/Password combination for each remote system at the SystemView Manager. Adding the *Force Remote Logons* option will further secure the manager. A person who has gained physical access to the manager will still need to supply the User ID/Password combination to gain access to the remote system.

1.7.1.4 Service Execution Alerts

With SystemView, you have the option to generate an alert each time a remote system attempts to access any of the SystemView services on your machine.

This option is by default turned off. You can enable the Service Execution Alerts by selecting the **Options** button on the first page of the SystemView configuration notebook and then selecting the **Service Execution Alerts** checkbox.

These alerts are provided to aid you in tracking which users are accessing what systems, as well as to provide a record of users who have attempted to access others systems using invalid User ID/password combinations. Alerts are also generated when a remote user attempts (successfully or unsuccessfully) to use Remote System Manager's System Restart action (System Restart) to restart your system.

The alert includes the name of the service that was initiated and information about the user that started the service.

1.8 Inventory Management

One of the problems that face administrators is keeping track of computing resources, both hardware and software, in their network.

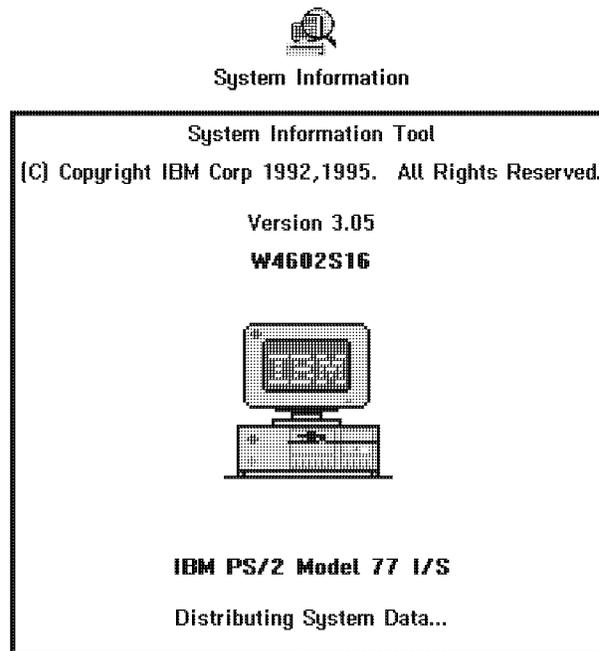
SystemView in Warp Server provides the following services for inventory management:

- System Information
- Software Inventory
- System Profile

OS/2 Warp Server also includes a DMI Browser. If your system is DMI-compliant, the corresponding components and icons will be installed. You can also install the SystemView Agent, which includes the SNMP and DMI browsers. The Agent is installed from the OS/2 Warp Server CD-ROM 2. Refer to the online *Up and Running!* Guide for additional information about the DMI and SNMP functions.

We will describe each of the SystemView in Warp Server inventory management functions listed above and how they may be used productively.

1.8.1 System Information Tool



The System Information Tool gathers and displays a broad variety of information about the hardware configuration of managed systems. The administrator can run the tool against any group of managed systems and view the information online, direct it to a file or printer or export it to a database.

The System Information Tool collects information on the following system features:

- Pentium processor information
- Model and microprocessor information, including model name, processor type and speed, and BIOS date
- Drive information, including file system type, available space on disk drives, disk drive size, and partition layout
- Memory configuration, including total physical memory, installed single inline memory module (SIMM) identification and supported memory upgrades
- Keyboard information
- Mouse type and settings
- Parallel and serial port configuration
- Video system information, including adapter type, screen resolution and video display identification

- System security features, including power-on password and secondary security features
- Micro Channel adapter identity with configuration information available on many common adapters
- Extended industry standard architecture (EISA) and peripheral component interconnect (PCI) adapter identity
- Error log display and interpretation
- Printer configuration, including data on installed printer drivers
- Small Computer System Interface (SCSI), enhanced small device interface (ESDI), integrated drive electronics/Seagate Technologies 506 (IDE/ST506), or other disk adapter information, including devices attached, device sizes and adapter data
- Operating system information, including version, DOS support, session limits, current task list, and CONFIG.SYS information

Figure 34 shows the System Information Tool window.

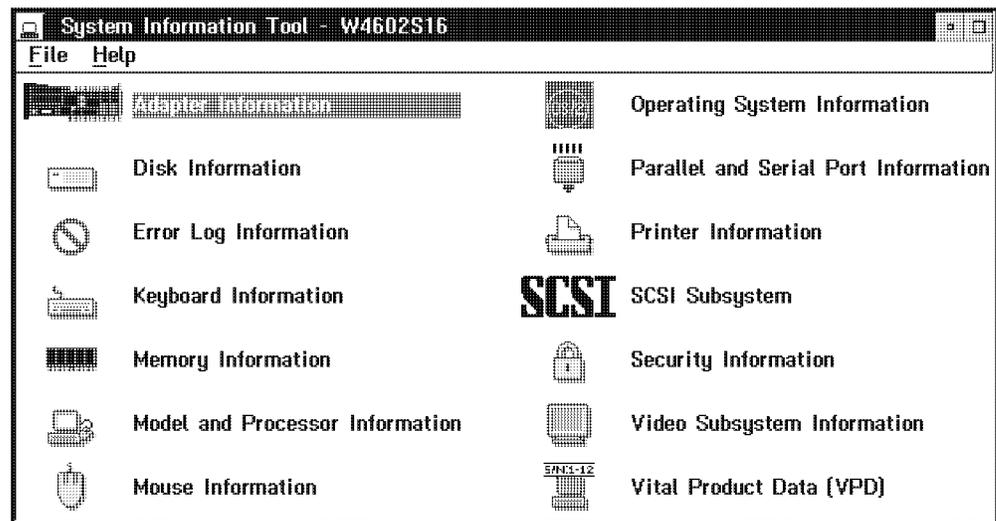


Figure 34. System Information Tool Window

To display information gathered by the System Information Tool, select the object or name of the component from the System Information Tool window.

The window that is displayed shows more specific information regarding the component you selected.

For example, you can display information about your SCSI subsystem. Figure 35 on page 46 shows one possible output.

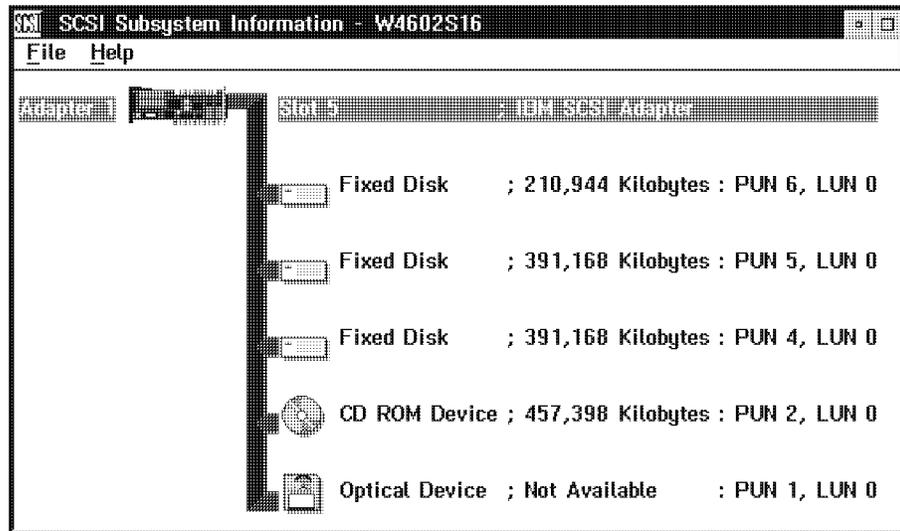


Figure 35. System Information Tool - SCSI Subsystem

You can use the File pull-down menu to print the data or write it to a file or a database.

Note: The end user can perform hardware inventory on the local system and direct the result to a printer or a file.

1.8.2 Software Inventory

The Software Inventory service gathers and displays information about the software installed on managed systems. It is possible to :

- Search for specific products
- Search for types of products (such as word processors or graphics viewers)
- Compile a record of all recognized software on a system

The administrator can:

- View the information online
- Direct it to a file or printer
- Export it to a database

The Software Inventory service checks the software installed on a workstation against a list of products called a dictionary file. A dictionary file, complete with many product definitions, comes as a part of SystemView. The administrator can edit the dictionary file to add and delete products or to provide multiple dictionary files, selecting one for a given Software Inventory.

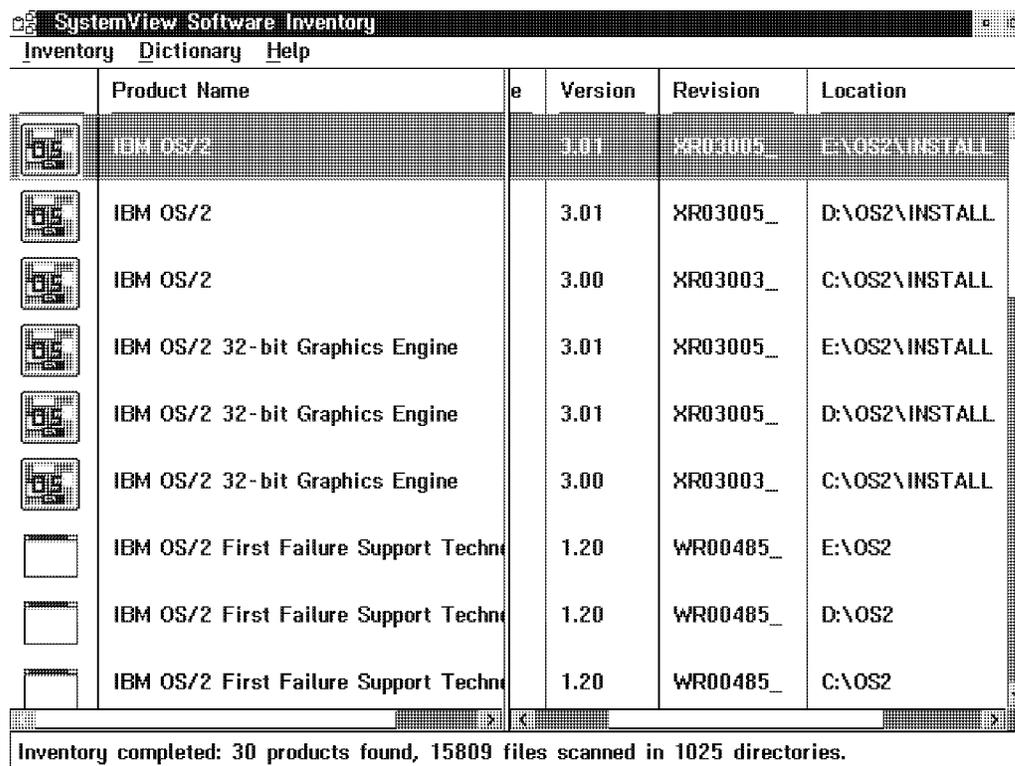
The products in the dictionary file supplied with SystemView in Warp Server are listed in *SystemView Up and Running*, Appendix A, SH19-4184 .

Software Inventory has a simple graphical interface that makes it possible to add or edit product definitions quickly and easily. Products can be defined and identified by the presence of specified file names (including files that are of a specific size or that were created on a specific date, making it possible to search for only certain versions of software) or by the presence of a SYSLEVEL file.

Finally, Software Inventory works with SystemView Software Distribution and with other IBM system-management software. Software Inventory provides a mechanism to integrate a workstation's existing Software Inventory information into the Software Distribution Catalog. This is accomplished by the creation of a file named FNDSWINV which contains a listing of the software that was discovered on that workstation by the Software Inventory service.

Software Inventory also provides a software dictionary import function for existing QSoft dictionary files (as used by IBM's Network Door/2 product) and Software Distribution inventory list files (used by the INVSCAN utility).

Note: There is a Qsoft dictionary DICT.QSF in the OS/2 Warp Server CD-ROM. The user now has this dictionary available and can import it on its own dictionary. Figure 36 shows an example of Software Inventory output.



Product Name	Version	Revision	Location
IBM OS/2	3.01	XR03005_	E:\OS2\INSTALL
IBM OS/2	3.01	XR03005_	D:\OS2\INSTALL
IBM OS/2	3.00	XR03003_	C:\OS2\INSTALL
IBM OS/2 32-bit Graphics Engine	3.01	XR03005_	E:\OS2\INSTALL
IBM OS/2 32-bit Graphics Engine	3.01	XR03005_	D:\OS2\INSTALL
IBM OS/2 32-bit Graphics Engine	3.00	XR03003_	C:\OS2\INSTALL
IBM OS/2 First Failure Support Techn	1.20	WR00485_	E:\OS2
IBM OS/2 First Failure Support Techn	1.20	WR00485_	D:\OS2
IBM OS/2 First Failure Support Techn	1.20	WR00485_	C:\OS2

Inventory completed: 30 products found, 15809 files scanned in 1025 directories.

Figure 36. Software Inventory Full Dictionary Search Example

In this example, you can see that the system has two partitions: C and D. The first one has Warp Connect, and the second one has Warp Server.

The SystemView Software Inventory provides the following information:

- Product Name
- Vendor Name (hidden in Figure 36)
- Version
- Revision
- Location
- Description (hidden in Figure 36)

We can see, for example, that the version and revision level of the OS/2 Warp contained in Warp Server is higher than the one contained in Warp Connect.

Figure 36 on page 47 shows the result of what is called a Full Dictionary Search.

You can do also a Selected Product Search, selecting only specified software products (see Figure 37):

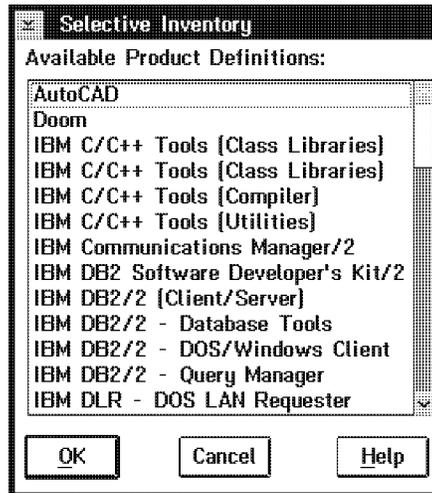


Figure 37. Software Inventory Selected Product Search Example

The list of default software products provided by SystemView is contained in a binary file called DEFAULT.SID in the \SYSVIEW2\BIN directory, also called the Default Dictionary.

SystemView contained in OS/2 Warp Server provides two dictionary files:

- DEFAULT.SID
- ALT.SID

The products in the dictionary file supplied with SystemView in Warp Server are listed in *SystemView LAN - Up and Running! V1.1*, Appendix A, SH19-4184.

Another search criterion is the Search by Product Type option. Using this option, you can classify the software products into categories such as:

- Network
- Communications
- Word Processing
- Desktop Publishing
- Database
- Mail
- Server
- Spreadsheet
- Financial
- Entertainment
- Multimedia
- Graphics Viewer/Editor
- Education
- Operating System
- Software Development

- Presentation Graphics
- Systems Management
- Documentation
- CAD/CAM
- Others

1.8.2.1 Software Information



Figure 38. Software Inventory - Menu Options

Once you have gathered the software information, you can proceed to do the following:

- **Saving/Printing Software Inventory Reports**

You can choose the option **Print to File** from the Inventory pop-up menu (see Figure 38) to save all of the currently displayed Software Inventory information to a file.

You can choose the option **Print the Data to a Printer** from the Inventory pop-up menu (see Figure 38) to send all of the currently displayed Software Inventory information to a printer attached to your system.

- **Update Software Distribution Directory**

You can choose to update Software Distribution directory from the Inventory pop-up menu (see Figure 38) to update your Software Distribution directory with all product definitions in the Software Inventory dictionary file that contain Software Distribution-specific data.

Note

This function will be available only if the Software Distribution is installed and running on the system.

- **Exporting Software Inventory Data to a Database**

You can choose the option **Export to Database** from the Inventory pop-up menu (see Figure 38), to export all of the currently gathered Software Inventory information to a database.

This opens the Database Entry Selection window. You can use this window to select the database to which the Software Inventory will export the data (see Figure 39).

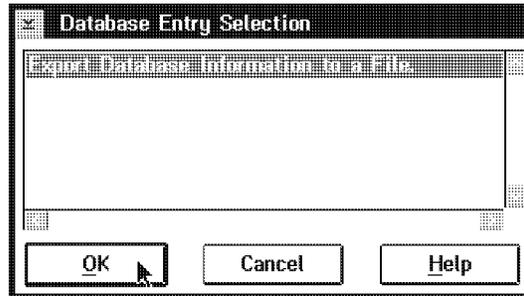


Figure 39. Software Inventory Database Entry Selection Window

Following this, enter the name of the file with extension DBF, and save it.

Support for DB2/2 and Lotus Notes Databases

If you install DB2/2 or Lotus Notes in the local system, you'll be able to export the Software Inventory data in one of these database formats. Software Inventory detects the presence of the Database Managers installed and enables the option in the menu.

1.8.2.2 Dictionary File

You can create or modify existing dictionary files to match the software you have installed on your network. The following options are available:

- Create a Dictionary
- Edit a Dictionary
- Delete a Dictionary
- Import a Dictionary

Software Inventory provides a software dictionary import function for:

- Existing QSoft dictionary files (as used by IBM's Network Door/2 product)
- Software Distribution inventory list files (used by the INVSCAN utility)

1.8.2.3 Modifying Records in a Dictionary File

In the Edit Dictionary window, you will find two fields (see Figure 41 on page 51):

Fields	Description
Description	A Brief description used as a header of the dictionary file
Product Definitions	A Record of the dictionary file

Click on **Add** to add a new record. You will have to choose between two options (see Figure 40 on page 51):

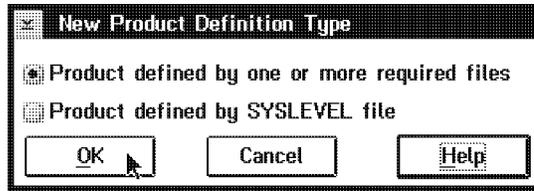


Figure 40. Creating Records in a Dictionary File

1. **Product defined by one or more required files.** Select this option if you need to configure a Software Inventory product definition that will determine whether a product is installed on a system by checking for one or more files of your choosing. In addition to the name of the file or files that Software Inventory will search for, you can specify minimum (or maximum) file size and exact date or date ranges for the file. For more information, see “Product defined by one or more required files.”
2. **Product defined by SYSLEVEL file.** Select this option if you need to configure a Software Inventory product definition that will determine whether a product is installed on a system by checking for a specified SYSLEVEL file.

In addition to the name of the SYSLEVEL file, you can specify a SysID Value or Component ID. You must type in this SysID Value field from the 16-bit hexadecimal product code contained in the product's SYSLEVEL file. For more information, see “Product defined by SYSLEVEL file” on page 54.

Click on **Edit** or **Delete** to update and erase, respectively, one record. See Figure 41.

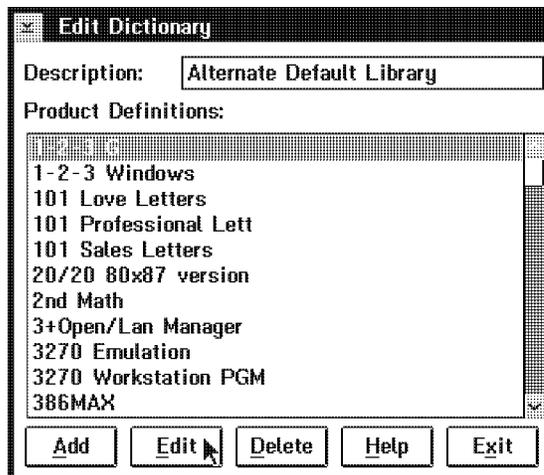


Figure 41. Editing and Erasing Records in a Dictionary

Product defined by one or more required files: Working in the Edit Dictionary window (see Figure 41), select **Add** and then select the **Product defined by one or more required files** option (see Figure 40). A window will be displayed as shown in Figure 42 on page 52:



Figure 42. Adding a New Product to the Software Inventory

You need to provide information for the following fields:

Fields	Description
Product Name	Name of the software product that you are defining.
Vendor Name	Name of the manufacturer of the software product that you are defining.
Description	Brief description of the software product that you are defining.
Product Type	Describe the product category, such as Spreadsheet (see the list of available selections on page 48).
Version	Major Version number of the software product that you are defining.
Revision	Revision or minor version number of the software product that you are defining.
NVDM Change Object	The Software Distribution identification string for use with the software product you are defining. Note: This data is used only for the Update Software Distribution Inventory function. For more information about NetView Distribution Manager Change Objects, please see the online help of the Software Preparation icon.
NVDM Location Token	The Software Distribution location token string for use with the software product you are defining.

Matching Attributes

Matching Attributes are the data items used by the Software Inventory service to detect whether the software product you are defining is installed on a system. Because you are creating a file product definition, the matching attributes will be key files belonging to the application.

Note: Although you don't need to fill in all of these fields, you should fill in as many as possible in order to maximize the information available to you when a product is found by the Software Inventory service.

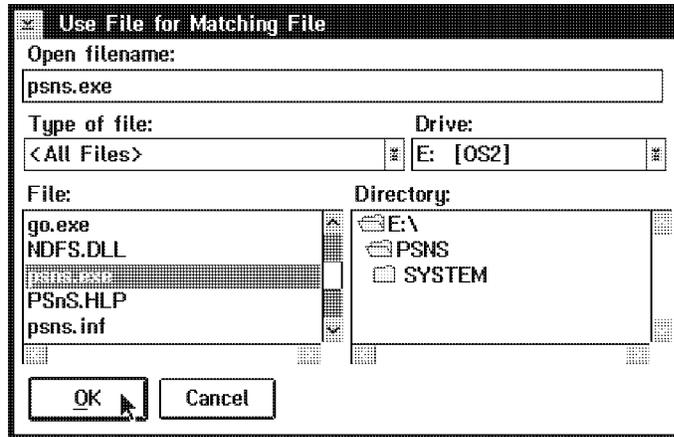


Figure 43. Matching File Attributes Screen

You can browse the file system in order to gather information about these files by clicking on the **Add** option in the Add File List Product Definition window (see Figure 42 on page 52) and selecting the **Use File** option (see Figure 44). Once you've found the key file for the application to be added (see Figure 41 on page 51), just click on **OK**, and a window will be displayed as shown in Figure 44:

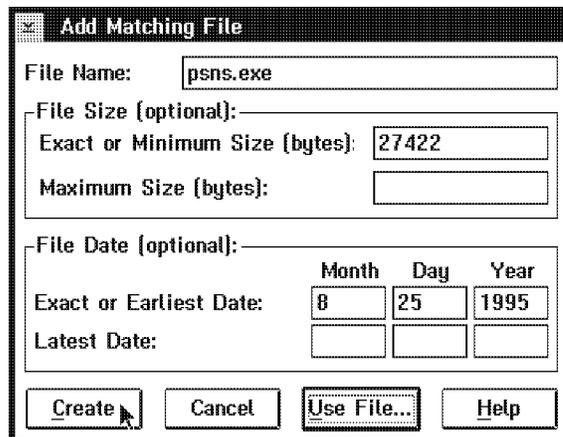


Figure 44. Add Matching File Window

By selecting **Create**, the information about the file (size and date) is copied into the Matching Attributes window.

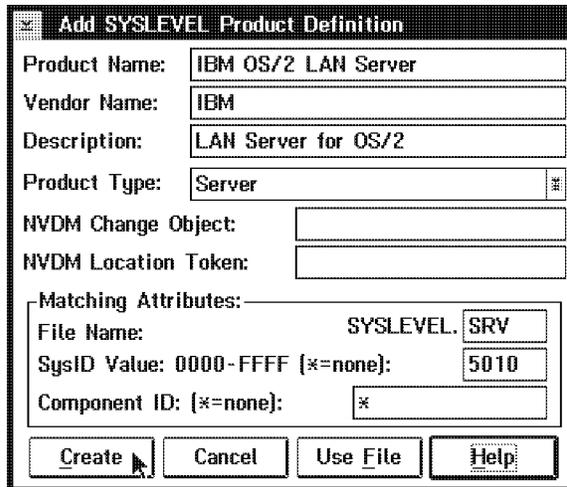
You can do the same for other files that need to be controlled in order to validate the application.

When you finish entering all the requested information, press **Save**.

Product defined by SYSLEVEL file: A SYSLEVEL file product definition enables Software Inventory to search your system's drives for a specific SYSLEVEL file that is found in a specific product.

If the specified SYSLEVEL file is found, then the Software Inventory service will report the software package that contains the specified SYSLEVEL is installed on the system.

Figure 45 shows an example of this.



The screenshot shows a dialog box titled "Add SYSLEVEL Product Definition". It contains the following fields and values:

- Product Name: IBM OS/2 LAN Server
- Vendor Name: IBM
- Description: LAN Server for OS/2
- Product Type: Server
- NVDM Change Object: (empty)
- NVDM Location Token: (empty)
- Matching Attributes:
 - File Name: SYSLEVEL.SRV
 - SysID Value: 0000-FFFF [*=none]: 5010
 - Component ID: [*=none]: *

At the bottom of the dialog are four buttons: Create, Cancel, Use File, and Help.

Figure 45. Product Defined by SYSLEVEL File

You need to provide information for the following fields (for more information about each entry, see the list on page 52):

- Product Name
- Vendor Name
- Description
- Product Type
- NetView DM Change Object
- NetView DM Location Token
- Matching Attributes

Note: Although you don't need to fill in all of these fields, you should fill in as many as possible in order to maximize the information available to you when a product is found by the Software Inventory service.

Matching Attributes are the data items used by the Software Inventory service in order to detect whether the software product you are defining is installed on a system. Because you are creating a SYSLEVEL file product definition, the matching attributes will be the SYSLEVEL file name, the SysID and the Component ID.

You can browse the file system in order to gather information about the SYSLEVEL file by clicking on the **Use File** option in the Add SYSLEVEL Product Definition window (see Figure 46 on page 55) and selecting the **Use File** option

(see Figure 47 on page 55). Once you've found the SYSLEVEL file for the application to be added (see Figure 47), click on **OK**, and a window will be displayed as shown in Figure 47:

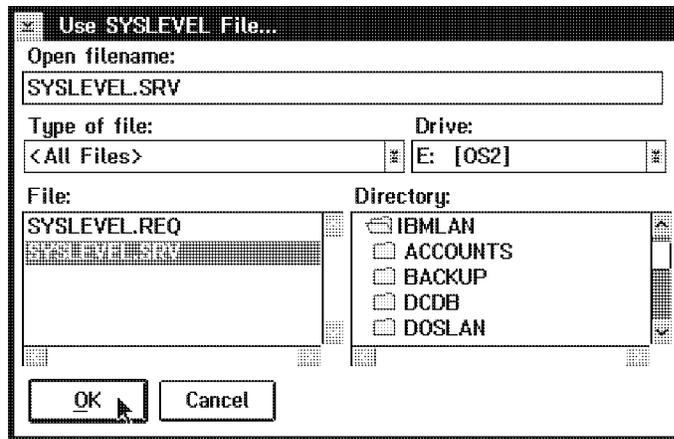


Figure 46. Searching for a SYSLEVEL file

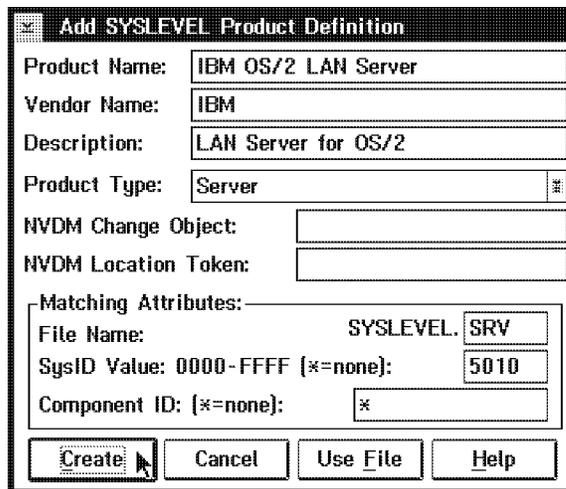


Figure 47. Creating the SYSLEVEL File Definition

1.8.3 System Profile



System Profile

The System Profile provides an easy-to-organize repository for a variety of information about a workstation. This information complements that collected by the Hardware and Software Inventory processes. The System Profile comes with many fields already defined to help simplify organization and entry of data about the system. The notebook also features many user-definable fields to help customize the System Profile. The administrator can collect information from all the System Profiles and save it in a file or export it to a database.

The System Profile is made up of five sections, each identified by its own tab:

1. **System.** Helps organize and track information specific to a:
 - System
 - Display
 - Printer
 - Modem
2. **User.** Helps organize and track the information specific to a system's primary user.
3. **Location.** Helps organize and track the information specific to a system's physical location.
4. **Contacts.** Helps organize information regarding ways of contacting the system's primary user and other personnel associated with the primary user.
5. **Miscellaneous.** Contains undefined fields for additional information.

Use at a Managed System

The end user can view and update the System Profile at the local system.

Table 4. System Profile Information by Page

System	User	Location	Contacts	Miscellaneous
Model Name	Name	Company Name/Address	Internal/External/ Cellular Phone	
Model/Serial Number	Employee ID	Site/Office/Building/ Floor	Pager Number	
Board Serial Number	Title		Fax Number	
Processor Card Serial Number	Department Name/Number		E-mail Address	
Date Purchased	Division		Backup/Technical/ Manager/Secretary	
	Start Date/Shift			
	Scheduled Hours			
	Home Phone/Address			
	Emergency Contact			

Figure 48 on page 57 shows an example of the User Information page of the notebook.

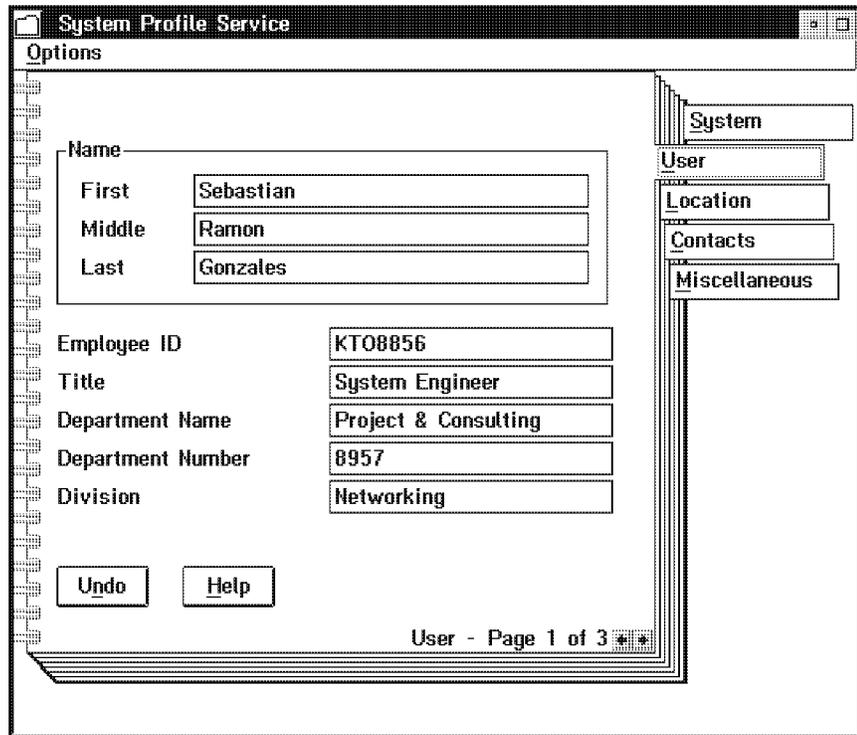


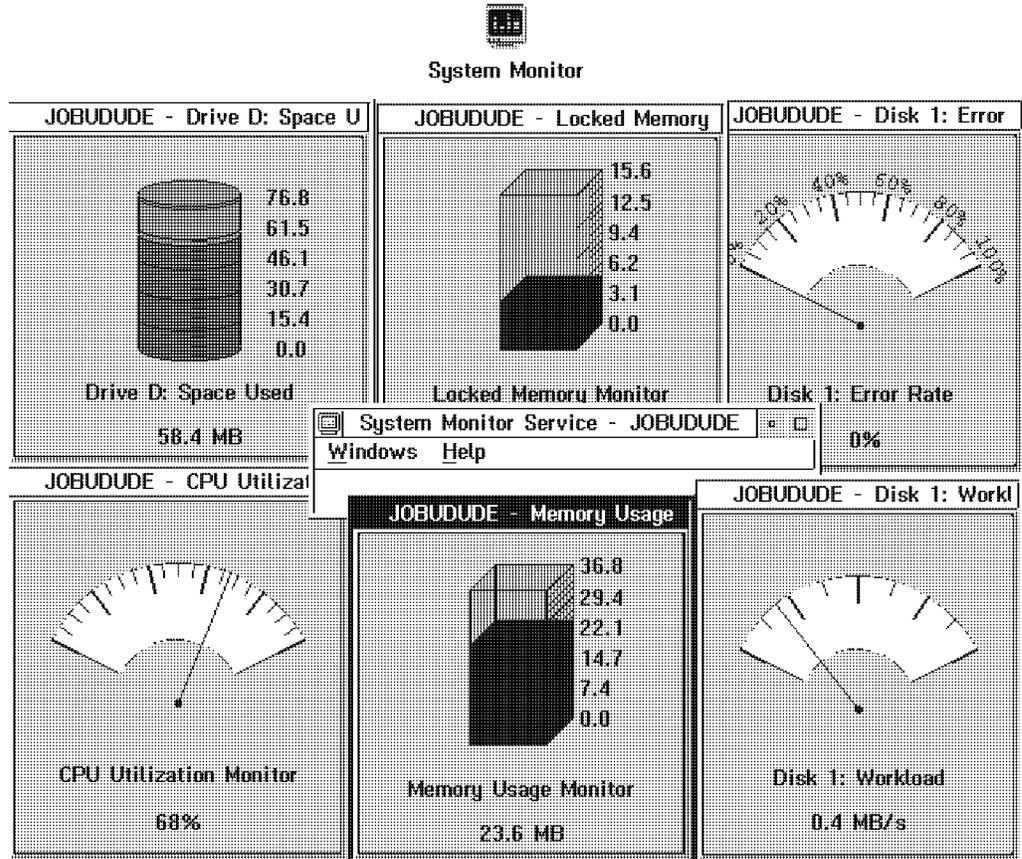
Figure 48. System Profile - User Information Page

Refreshing the Notebook: This function updates what is displayed by the System Profile.

Changes can be made to the notebook's contents by other users while you are viewing it, and selecting **Refresh** will update the data displayed in the System Profile's fields.

Printing to a file: This option saves all information contained in the System Profile to an ASCII text file.

1.9 Performance Management



Performance monitoring is provided in the SystemView in Warp Server product by the System Monitor.

The System Monitor provides a convenient method of monitoring and displaying the activity of a number of components of a system, such as:

- Continuous monitoring of systems, including:
 - Locked memory usage
 - Virtual memory usage
 - CPU usage
 - DASD (Direct Access Storage Device)
 - Disk space available and remaining
 - Disk space utilization
 - Disk error rate
 - Disk workload
 - TCP/IP Protocol Functions
 - UDP (User Datagram Protocol) Datagrams Sent/Received
 - IP (Internet Protocol) Packets Sent/Received
 - IP Packets Received with Errors
 - TCP (Transmission Control Protocol) Connections
 - TCP/IP Sockets

For each TCP/IP interface, it can retrieve:

- Unicast Packets Sent/Received
- Broadcast Packets Sent/Received
- Bytes Sent/Received

- Print Jobs Queued
- Processes Running
- Threads Running
- Pentium Processor Computations
- RAID Device Attributes
- Read/Write Errors (SystemView Manager only)
- Swap File
- ECC Memory Monitor
 - Size
 - Remaining
- LAN Server
 - Sessions
 - Connections
 - Opens
 - Shares
 - Bytes Sent/Received
 - Response Time
 - Request Buffers/Big Buffers shortage
- Integer Instructions Rate
- Floating Point Operation Rate
- Interrupt Rate
- Port I/O Rate
- Memory I/O Rate
- CPU Cache Hit Rate
- Laptop Battery Status
- PCMCIA Information
- Ability to export System Monitor data to a database.
- Detachable, scalable, and user-configurable monitors
- Generation of alerts when thresholds set by the administrator are exceeded
- Choice of line-graph, text, and real-time graphic representations of system activity
- Descriptive output for devices for which numeric output is not meaningful

The System Monitor uses a data-handling technique that allows for both long-term system activity profiles and short-term, high-resolution system activity monitoring.

As samples of system activity are taken, they are stored and displayed. However, after a number of samples have been taken, their individual values are weighed, several concurrent samples are averaged, and they are posted as a single, long-term value.

This process prevents System Monitor data files from taking up a large amount of space on a system and also allows for a reasonable measurement of average long-term system load values without sacrificing short-term monitoring abilities.

If the administrator does not need records of a monitor's previous activity, or does not want to use disk space to maintain these records, it is possible to disable record keeping.

Note: The System's Monitor Record Data option is enabled by default on the local system and disabled by default on the remote systems.

1.9.1.1 System Monitor Service Window

When the System Monitor Service is started, all monitors currently set to be visible appear on the display, along with the System Monitor Service window.

The System Monitor Service window controls the service as a whole. If the System Monitor Service window is closed, all of the monitors close as well.

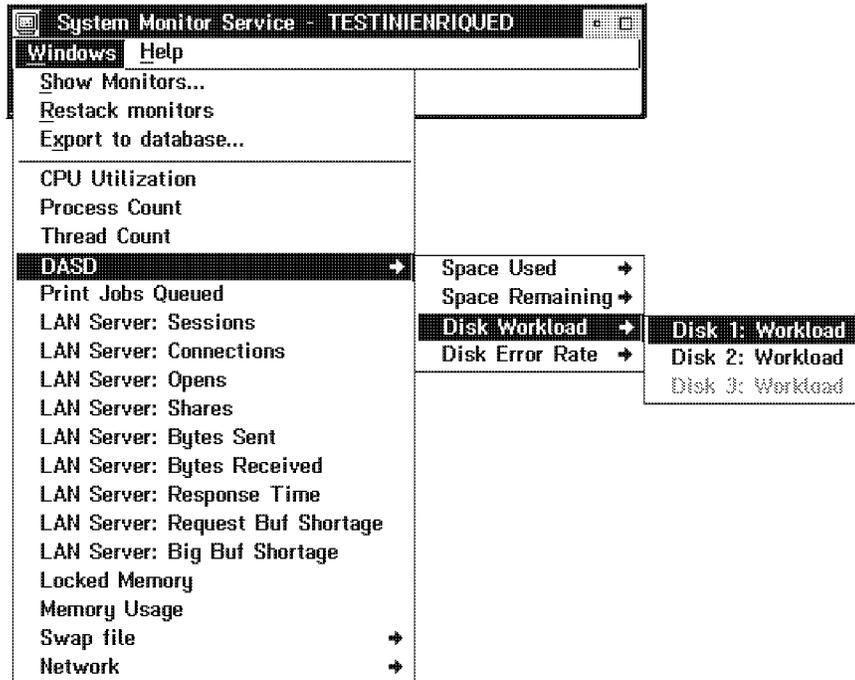


Figure 49. System Monitor Service Windows Drop-Down Menu

The Windows choice of the System Monitor Service window (see Figure 49), allows you to:

- Show Monitors
Select **Show Monitors...** to select which of the System Monitors you want to be visible on your desktop, and select **Accept** to display or hide monitors as appropriate.
In addition, you can select the name of the monitor you want to bring to the foreground. This can only be done if the monitor was not selected to be hidden.
- Restack monitors
Select **Restack monitors** to overlap your existing monitors onto each other. They will move from their current positions and reappear in the lower left-hand corner of your display.
- Export to database...
The current time, date, and reported value of any selected monitors can be exported to a database. To export monitor data from one or more component monitors:

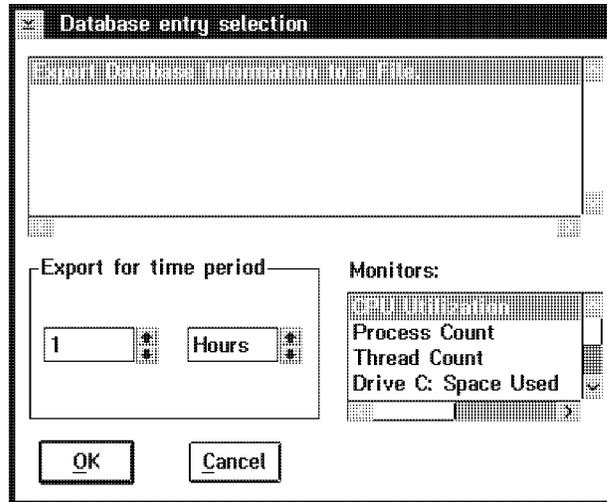


Figure 50. Export to Database Option

1. Select **Export to database...** from the System Monitor Service Windows drop-down menu (see Figure 49 on page 60).
2. Select from the Monitors field (see Figure 50) the names of the monitors from which the data will be exported.
3. Select **OK**.
4. Select the database to which the monitor data will be exported.
5. Select **OK** to export the data.

1.9.1.2 Monitor Context Menus

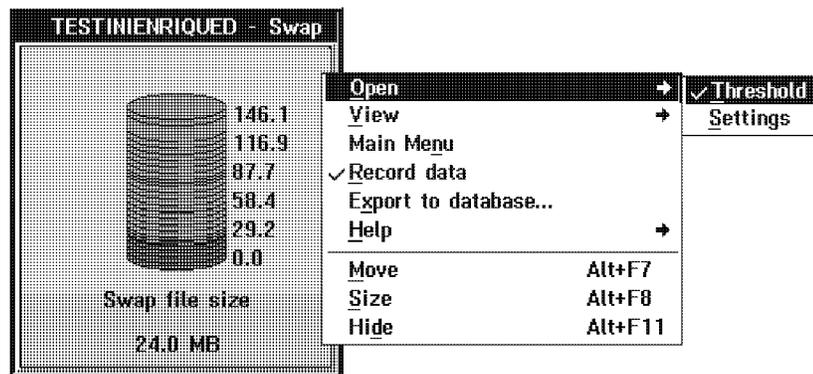


Figure 51. Monitor Context Menu

Each monitor has its own Monitor Context menu. To open the Monitor Context menu, place the cursor over the monitor and press mouse button 2 (as shown in Figure 51). Your choices are:

- **Open & Threshold**— Configure System Monitor thresholds (see Figure 53 on page 63).
- **Open & Settings**— Change System Monitor settings (see Figure 55 on page 66).
- **View**— Change the appearance of the System Monitor that is displayed. The available monitor types are:
 - Line-Graph

- Real Time
- Text Display

(see Figure 52). This figure shows **Disk 1: Workload** as a Line-Graph, **CPU Utilization** as a Real Time display, and **Thread Count** as a Text Display.

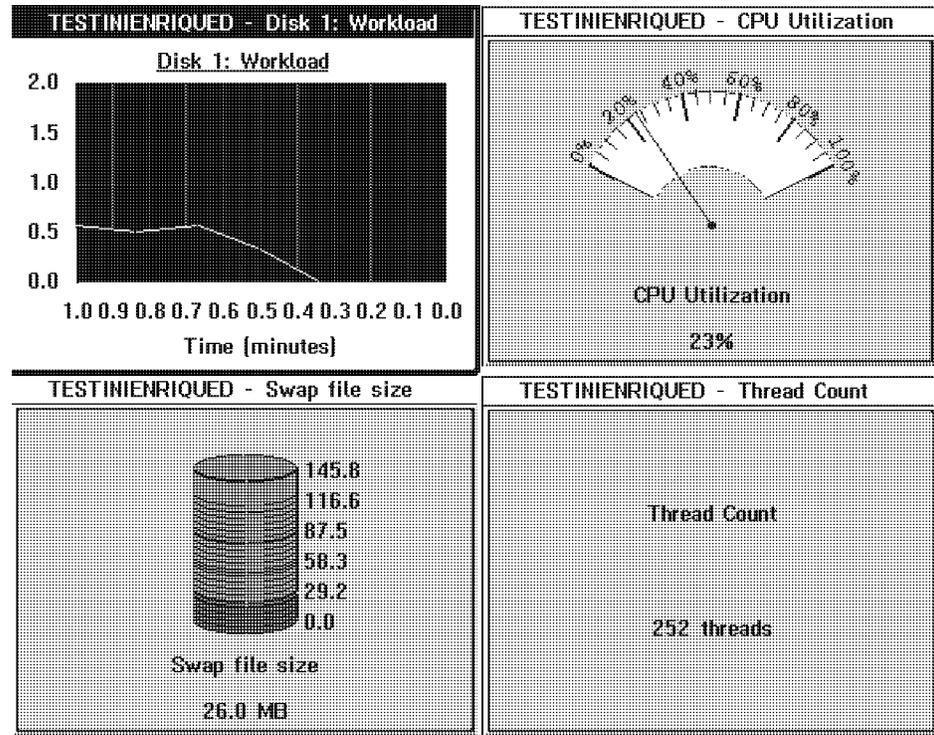


Figure 52. Different View Options

- **Main Menu**— Bring the System Monitor Service window to the foreground.
- **Record data**— Enable or disable recording of data.

When Record Data is enabled, System Monitor continually gathers and updates data from this monitored component and saves it for use in the Line Graph monitor display.

Note: Disabling this option on monitors that are not used frequently, or from which long-term data isn't needed, will also disable the Line Graph view. However, it can help you to save disk space and memory needed to maintain this monitoring data.

- **Export to Database..**— Export data to a database.
- **Help**— Access online help.
- **Move**— Move the monitor onto the desktop.
- **Size**— Size the monitor.

Note: If you make a monitor too small for the monitor's text to be shown fully, the text disappears. This has no effect on the monitor's function.

- **Hide**— Hide the monitor. The monitor will continue to function and collect data, but it will not be visible on the Desktop.

Note: To make a hidden monitor visible again, open the System Monitor Service window, and select **Show Monitors...** to open the Select Visible

Monitors window. To export data from an individual monitor (see Figure 50 on page 61):

To export data from an individual monitor:

1. Select **Export to Database...**
2. Select the Database to which the monitor data will be exported.
3. Select **OK** to export the data.

In the Database entry selection window (see Figure 50 on page 61), we can set:

- Destination for export database information
- Period of time for export, from one hour to several weeks
- Monitors to be exported (for example, CPU Utilization)

The time, date and current value reported by the monitor can be exported to the database.

1.9.1.3 System Monitor Notebooks

The System Monitor notebooks can be used for two important functions:

1. To set thresholds at which alerts will be generated.

You can create different profiles, including the following parameters (see Figure 53 and Figure 54 on page 65):

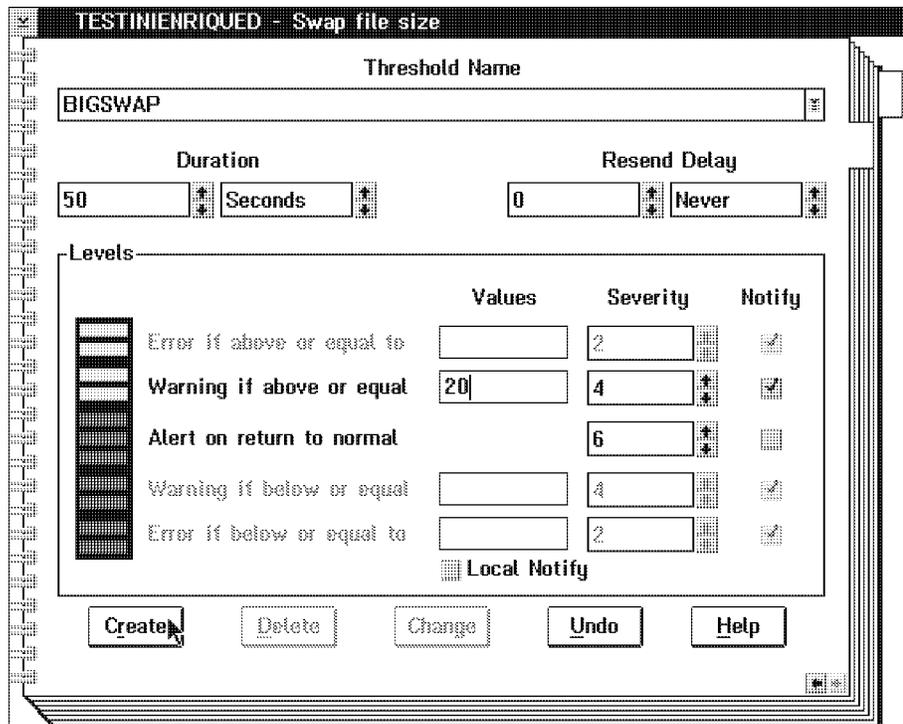


Figure 53. Setting Thresholds

- **Threshold Name**—This is the name you assigned to the threshold.
- **Duration**— The time the threshold must be exceeded before an alert is generated.
- **Resend Delay**— The amount of time the threshold must continue to be exceeded before a duplicate alert is generated.

- **Levels**— Determine the point at which the threshold begins. You can set up four different thresholds for each of your monitored system components. These thresholds are:
 - Error if above or equal to
 - Generate an alert with an "Error" Alert Type. The threshold value must be:
 - Less than or equal to the maximum value for this system component, and
 - Greater than or equal to the "Error if above or equal to" value.
 - Warning if above or equal
 - Generate an alert with a "Warning" Alert Type. The threshold value must be:
 - Less than or equal to the maximum value for this system component, and
 - Less than or equal to the value (if any) assigned for "Error if above or equal to", and
 - Greater than or equal to the value (if any) assigned for "Warning if below or equal to" and "Error if below or equal to"
 - Alert on return to normal
 - Select this alert if you want the System Monitor to generate a separate alert to notify you that threshold values that were previously exceeded are no longer being exceeded.
 - Warning if below or equal
 - Generate an alert with a "Warning" Alert Type. The threshold value must be:
 - Less than or equal to the maximum value for this system component, and
 - Less than or equal to the value (if any) assigned for "Error if above or equal to", and "Warning if above or equal to", and
 - Greater than or equal to the value (if any) assigned for "Error if below or equal to".
 - Error if below or equal to
 - Generate an alert with an "Error" Alert Type. The threshold value must be:
 - Less than or equal to the maximum value for this system component, and
 - Less than or equal to the value (if any) assigned for "Error if above or equal to", "Warning if above or equal to", and "Error if below or equal to"
 - Values
 - The value corresponding to the variable you're monitoring that generates an alert.
 - Severity
 - Each threshold value provides a default severity level. Depending of the importance of the alert you need to send, you can adjust this value to one more convenient.
 - Notify
 - Makes a pop-up window appear on your system to notify you whenever this threshold is exceeded.
 - Local Notify

Select this option if you want the threshold to generate an alert on the system on which the threshold is being configured (thus enabling the local system to use its Alert Manager to respond to the alert).

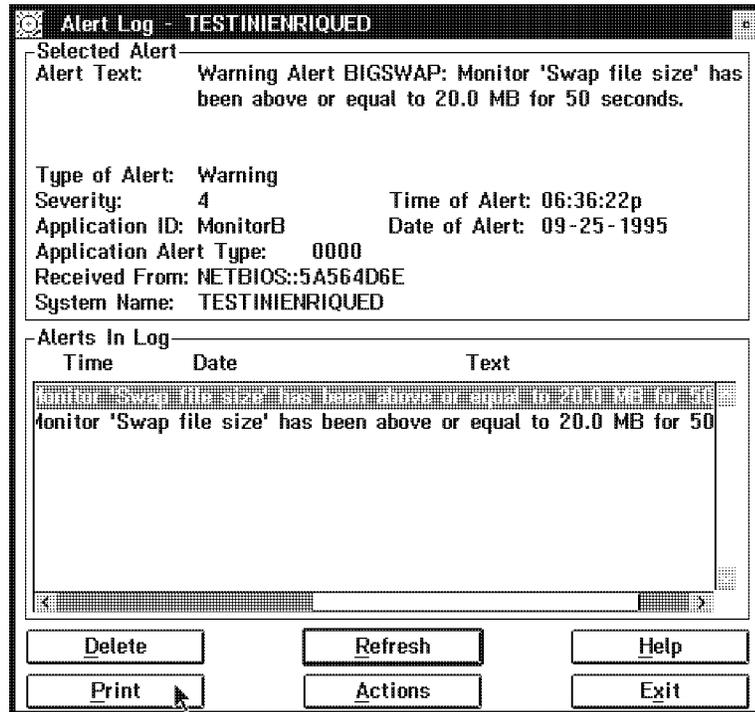


Figure 54. Viewing the Alert Log

2. **Configure** monitor-specific settings.

Using the Monitor Configuration Notebook, you can configure (see Figure 55 on page 66):

- **Enable title bar**— Activate/Disactivate the title bar. This bar shows the System Name of the machine on which the System Monitor is being executed (only appears if the service is being run on a remote system) and the type of monitor (for example, "Swap file size").
- **View**— Type of monitor that will be displayed. The available monitor types are:
 - Line Graph. A *heartbeat-style* chart of the system component's activity using user-specified Line Graph settings to determine the length of the graph and the units in which it is measured.
 - Real Time. A graphic representation of this system component's current status. The real time monitor that is displayed depends on what system component it is meant to represent. For example:
 - The CPU monitor uses a speedometer-style real-time monitor to show percentage of CPU utilization.
 - The Hard Drive Space Used monitors use a cylinder to depict how full the drive is.
 - Text Display. Displays a textual readout of the system component's current activity only, without any graphical representation.
- **Line Graph Settings**— These settings are applied to the Line Graph view, and are:

- Scale. Length of time graphed when viewing this monitor's Line Graph. You have to enter a number in the left box, and use the spin buttons to the right box to select the unit of time the Line Graph will use to graph component activity. The available units of time are:
 - Seconds
 - Minutes
 - Hours
 - Days
 - Weeks
- Fill Graph. Enable or Disable Line Graph Fill Graph
- Fill Color. Select the Line Graph Fill Color
- **Real time settings**— Configures the monitor real-time view.
 - Background texture. The background pattern for this monitor's real-time view.
 - Filled color. Color for the full part of the monitor's real-time view.
 - Empty color. Color for the empty part of the monitor's real-time view.
- **Font**—
 - Name
 - Color

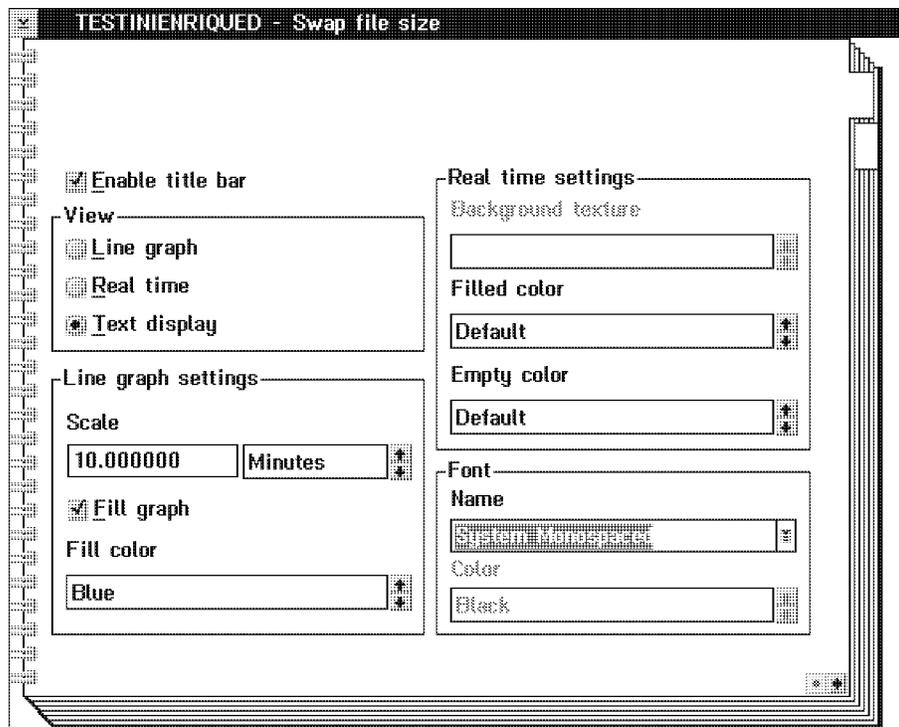


Figure 55. Monitor-Specific Settings

1.9.1.4 System Monitor Tips

1. The minimum time you can set the *Export data to Database* function is one hour. This time is arbitrary and is based on the fact that most administrators will want to track long-term data and can display short-term data visually on their screen using the Line Graph function under the monitors.

2. The sample interval is fixed in this release of SystemView in Warp Server. The sample interval varies by monitor according to the ease and burden of data collection (for example CPU = 5 seconds and disk = 5 minutes).

The exported file has a field called *monitor interval* which is in seconds.

Export to file/Database is a user-initiated function that is not performed automatically by the system. If you don't initiate a new export, you won't see the new data in your file/Database.

3. System Monitor doesn't export data to a printer or to a flat ASCII file. There is a lot of data to export under the monitors that would be difficult to read as a flat online or printed file.

Under the Database option you are able to export to a common delimited file (.DBF) which can be parsed and imported to a spreadsheet or another Database type.

4. DB2/2 and Lotus Notes formats are also supported but System Monitor will not display these options unless either of these two databases are present (if the client/server is not physically present it doesn't do much good to export to them).

1.10 Operations Management

SystemView in Warp Server provides the following services for operations management:

- Critical File Monitor
- ECC Memory
- RAID Administration
- File Transfer
- Alert Manager
- Power-On Error Detect
- Predictive Failure Analysis
- Event Scheduler
- System Partition Access
- Process Manager
- Serial Control
- Remote Session
- Remote Workstation Control
- Screen View

1.10.1 Monitoring Critical Files



Critical File Monitor

A client system can be set up so the administrator is informed, by means of an alert, whenever a critical file on the managed system is created, changed or deleted. Users at the client system can also use the critical file monitoring on the local system.

The administrator specifies, on each client system, which files to monitor and the severity of the alert generated. Default files set up for OS/2 are:

- CONFIG.SYS
- STARTUP.CMD
- AUTOEXEC.BAT

The default files setup for Windows are:

- CONFIG.SYS
- AUTOEXEC.BAT
- WIN.INI
- SYSTEM.INI

The administrator can specify additional files to be monitored. For each file that is selected to be monitored, an Alert Severity level needs to be specified. See Figure 56, which shows how to set up a monitor for changes to the PROTOCOL.INI file.

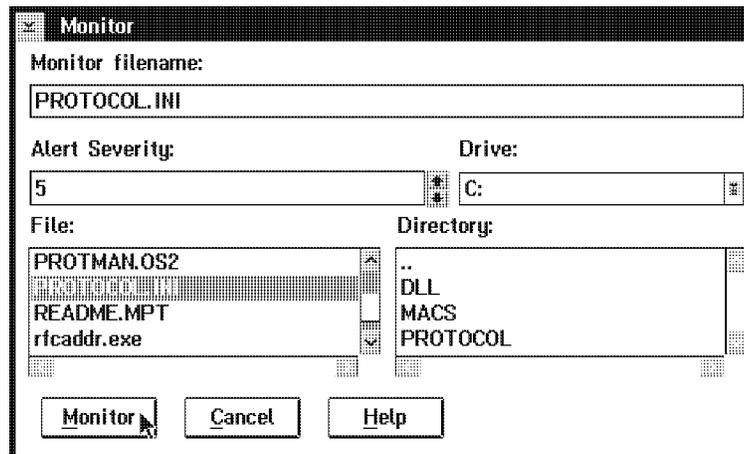


Figure 56. Specifying Files in the Critical File Monitor

Figure 56 shows how to select other files to control from the remote server, also assigning the alert priority value.

Each time the file is changed the Alert Manager (see 1.10.5, “Alert Manager” on page 77) receives an alert form the Critical File Monitor system (see Figure 57 on page 69).

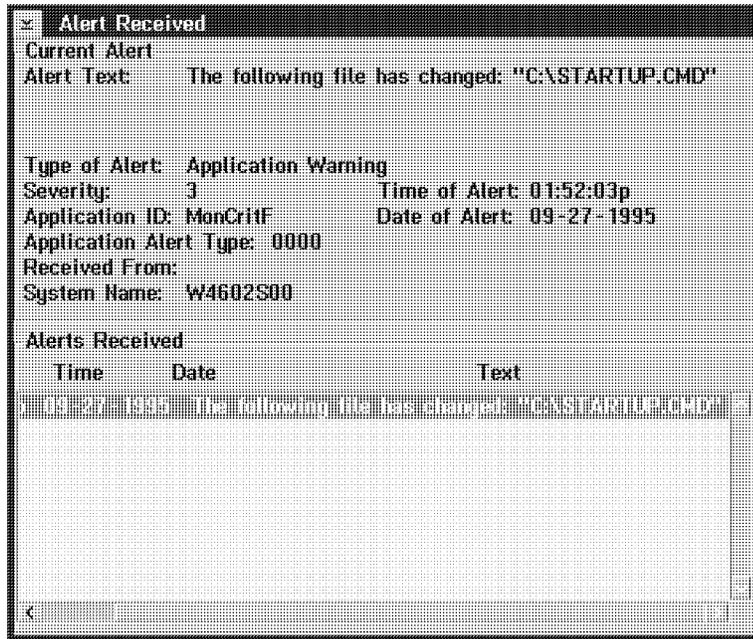


Figure 57. Alert Manager Message Generated by the Critical File Monitor

1.10.2 ECC (Error Checking and Correction) Memory Setup



ECC Memory Setup

This service is only be available on systems that have ECC memory installed. ECC memory is typically used in servers, and is more expensive. The services enable the user to monitor and manage ECC memory.

To configure the ECC Memory Setup (see Figure 58 on page 70):

1. Select the actions that you wish ECC Memory Setup to perform. Available options are:

- Single-Bit Error Scrubbing

This option instructs ECC Memory Setup to activate the automatic error correction features of the ECC memory in the system. This will immediately correct any single-bit errors that occur.

Note: This option may cause a slight performance impact on some systems, but ensures greater data integrity.

- Single-Bit Error Counting

This option instructs ECC Memory Setup to keep a running count of all single-bit errors that occur in the ECC memory.

- Single-Bit Error Threshold Non-Maskable Interrupt (NMI)

This option instructs ECC Memory Setup to cause a Non-Maskable Interrupt (NMI) if the number of single-bit errors exceeds the user-specified threshold. An NMI will often cause the system to immediately shut down; so this feature should only be enabled if the system contains special NMI handling hardware and software.

Note: If you have set the Single-bit Error Threshold option, you can also set the Single-bit Error Threshold value that will trigger the NMI.

2. Change the Single-Bit Error Count, if desired.

The Single-Bit Error Count field displays the number of single-bit errors that have been detected by ECC Memory Setup during the current session.

Note: The Single-Bit Error Count is for the current session *only*. The count is reset to zero upon restart. If you wish to carry a count over from a previous session, you must enter the error count manually from the configuration screen.

3. If you have chosen the Single-Bit Error Threshold NMI option, set a Single-Bit Error Threshold value.
4. Click on the **Save** button.

Note: All functions of ECC Memory Setup may also be accessed from your OS/2 command line. For more information, see the Command Line Help Reference and search the `ECCMEM` command syntax.

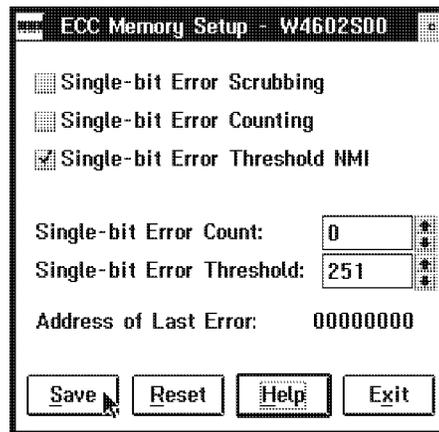


Figure 58. ECC Memory Setup

1.10.3 RAID Administration: RAID Manager



RAID Manager

RAID (Redundant Array of Inexpensive Disks) is a technology which allows several physical storage devices are grouped into an array, and can appear to the operating system as one physical drive. RAID technology also enables you to set up the RAID array drives into a variety of data configurations. These configurations (called RAID levels) provide varying levels of data integrity, protection and storage capacity. Some RAID levels provide greater data integrity through the use of data mirroring.

Ordinarily, you must take your RAID system offline in order to perform most RAID management tasks. However, with the RAID Manager service, you can easily gather information about your system's RAID adapter, physical drives in the RAID array, and the logical drives that are defined by the array. You can also perform a variety of important RAID management tasks quickly and easily. These tasks include:

- Adding and deleting logical drives
- Initializing and synchronizing logical drives
- Formatting and rebuilding RAID physical devices
- Configuring RAID adapters
- Gathering data about all RAID adapters, devices, logical drives, and enclosures

Note:

1. Irresponsible use of RAID Manager can seriously harm your system and its data. Use RAID Manager only if you are familiar with RAID arrays and RAID systems management.
2. This service is only available for use on systems that have a supported RAID adapter installed. For a list of supported RAID adapters, see 1.10.3.5, “Supported RAID Adapters” on page 75.

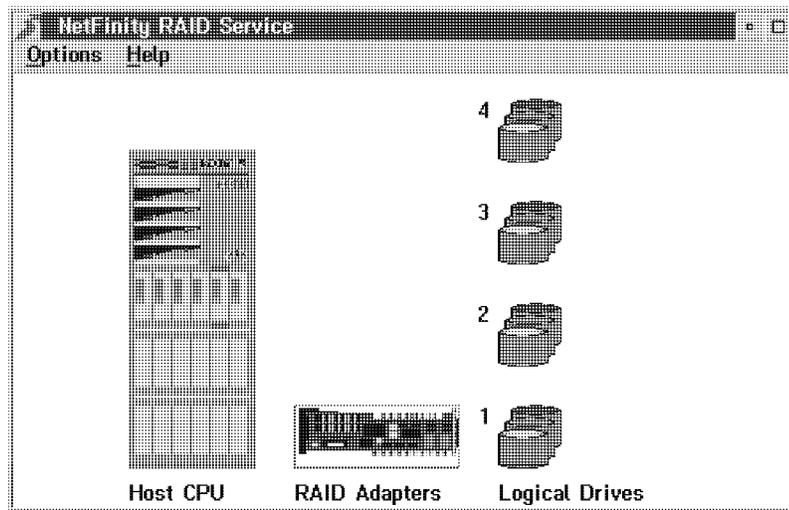


Figure 59. RAID Manager

1.10.3.1 Viewing RAID Device Information

The RAID Manager enables you to view general information on your RAID system's devices, including the RAID enclosure, physical RAID devices, RAID adapters, and logical RAID drives.

Viewing Enclosure Information: RAID Manager enables you to quickly gather information about any RAID enclosures attached to this system. Available information includes:

- Enclosure Model
- Enclosure Manufacturer
- Serial Number
- Number of RAID Adapters
- Enclosure Function

To view information about a RAID enclosure:

1. Use mouse button 2 to select the enclosure that you want to examine. This opens the enclosure's Context menu.
2. Select **View Enclosure** from the enclosure's Context menu.

Select **OK** to close the Enclosure Information window.

Using the RAID Manager

If you receive an error message about a *Raid Resource DLL* missing when starting the Raid Manager, you can try the following steps to correct the problem:

1. From the OS/2 Warp Server CD-ROM, copy the \CID\SERVER\SYSDVIEW2\SERVER_2\RRSRC.DLL file to \SYSDVIEW2\BIN directory on your system.
2. From the same directory, copy the RD*.INI files to the \SYSDVIEW2\BIN directory.
3. In the case of the IBM PC Server 320 or 520, you may need to copy the RD1x20.INI to RAIDSYS.INI, as appropriate.

Viewing Physical Device Information: RAID Manager enables you to gather a variety of information about the physical devices that are part of your RAID array. Available information includes:

- Device status
- Device number
- Channel number
- Device type
- Device size
- Maximum channels
- Sectors
- Device hot-pluggable
- Media status
- Manufacturer
- Model
- Serial number

To view information about a physical RAID device:

1. Use mouse button 2 to select the device that you want to examine. This opens the adapter's Context menu.
2. Select **View Device** from the device's Context menu.
3. Select **General Information**.

Select **OK** to close the Standard Device Information window.

Viewing Adapter Information: RAID Manager enables you to quickly gather information about any installed RAID adapters. Available information includes:

- Adapter Identifier
- Buses Available
- Attached Devices
- Device IO
- Host Bus
- Adapter Status
- Manufacturer
- Model
- Serial Number

To view information about a RAID adapter:

1. Use mouse button 2 to select the adapter that you want to examine. This opens the adapter's Context menu.
2. Select **View Adapter**.

Select **OK** to close the Adapter Information window.

Viewing Logical Drive Information: RAID Manager enables you to quickly gather information about any logical drives defined by your RAID adapters. Available information includes:

- Logical Drive Number
- Logical Drive Size
- Logical Drive Status
- Logical Drive RAID Level

To view information about a logical drive:

1. Use mouse button 2 to select the logical drive that you want to examine. This opens the logical drive's Context menu.
2. Select **View Logical Drive Information**.

Select **OK** to close the Logical Drive Information window.

1.10.3.2 RAID Device Management

RAID Manager enables you to manage the storage devices that make up your RAID array. Use RAID Manager to:

- Format the device
- Rebuild the device
- Spin-down the device
- Spin-up device

1.10.3.3 RAID Adapter Management

RAID Manager enables you to access and configure your RAID adapter. With RAID Manager, you can:

- Set Stripe Unit Size
- Set Rebuild Priority
- Set Parity Storage
- Set Read Ahead Settings

Setting the Stripe Unit Size: Stripe Unit Size is the amount of data written to each successive device in the logical drive. All of the units assembled form a stripe. This parameter is also known as the interleave depth. The minimum number of bytes that the adapter will read from a device is the Stripe Unit Size. The stripe unit can range from 8 Kbytes to 64 Kbytes.

The Stripe Unit Size is configurable on certain IBM adapters.

Knowing the average file size in your working environment and the frequency of file access can help set this parameter to maximize performance. If file access is high and file sizes are typically small, then a lower Stripe Unit Size is best. If file access is high and file sizes are typically large then a large, stripe unit is best. If disk access is seldom, then it is best to choose the default.

Setting Rebuild Priority: Because rebuilding is an intensive and sometimes time consuming operation, RAID Administration enables you to prioritize these operations. Low, Medium, and High priorities can be assigned to the operations.

Higher priority will enable the operation to complete more quickly, but will negatively affect normal processing.

Setting Parity Storage: The Parity Storage method can be set to further enhance your RAID array's performance.

Setting Read Ahead: Setting read ahead enables the RAID adapter to read data into its cache before the data is needed. This speeds up the next read request, enhancing the system's performance as a result.

1.10.3.4 RAID Logical Drive Management

RAID Manager enables you to alter a variety of logical drive parameters. The following logical drive management options are available:

Add Logical Drives:

1. Select **Add Logical Drive** from the Options pull-down menu.
2. This will open the Add Logical Drive window.
3. Select the physical devices that the logical drive's data will be striped across.
4. Select the amount of space that will be used on each selected physical device.
5. Select a RAID Level for the logical drive.
6. Select **Save** to define the logical drive.

Delete Logical Drives:

1. Select the logical drive you want to delete with mouse button 2. This will open the logical drive's Context menu.
2. Select **Configure**.
3. Select **Delete**.

Once you have selected Delete, the contents of the logical drive will be erased.

Note:

1. The changes will not take effect until after the machine is restarted.
2. Delete logical drives with care. Once a logical drive is deallocated, all data on that drive is lost.

Initialize Logical Drive: Select **Initialize** to write binary zeroes to all bits on the logical drive and recompute proper parity information. This operation is required for RAID Level 1 and RAID Level 5 logical drives.

Synchronize Logical Drive: Select **Synchronize** to recompute the parity information on a RAID Level 1 or RAID Level 5 logical drive. The data on the drive is not changed.

Check Drive Consistency: Select **Check Consistency** to read system and parity data and verify the parity data computed from the system data is identical to the parity data read from the disks. Only one consistency check may be performed at a time, and consistency checks cannot be performed on a RAID Level 0 logical drive.

Note: The Check Consistency function can be very time consuming, depending on the sizes of the drives involved. The RAID adapter will not accept any other Rebuild or Check Consistency functions during this time.

1.10.3.5 Supported RAID Adapters

The following RAID adapters are supported:

- IBM RAID Adapter
- IBM SCSI-2 Fast/Wide-Streaming RAID Adapter/A
- IBM SCSI-2 Fast PCI-Bus RAID Adapter

1.10.4 File Transfer



File Transfer

File Transfer enables a network administrator to send and receive individual or multiple files between a local system and a remote system. Also, it provides for simplified deleting of multiple files locally and remotely.

File Transfer also provides directory transfer capabilities, enabling a network administrator to transfer or delete entire directories, locally and remotely.

1.10.4.1 File Transfer Tips

1. File Transfer is a *remote only* service. This service will only be available for use when you are accessing a remote system. The File Transfer service object will *not* appear in your local Service Manager.
2. File Transfer uses an automatic file compression process to minimize the amount of time it takes to move files or directories across slower networks. However, if you are using a fast network, File Transfer will not use any compression because the time required to process the data for compression will actually increase the amount of time it takes to transfer the data. This process is automatic and requires no input. If you want to disable File Transfer's data compression capabilities, see 1.10.4.4, "Disabling Data Compression" on page 77.
3. The extended file names of any HPFS (High Performance File System) files that are transferred to a FAT (File Allocation Table) drive will be changed to an appropriate FAT file name.
4. Improper use of File Transfer can lead to data loss locally or remotely. If you are concerned about potential data loss, use Security Manager to limit use (for information about Security Manager, see 1.7, "Implementing Security" on page 40).

File Transfer Limitations for DOS target systems

DOS does not support path names of more than 63 characters. If you will be using File Transfer to transfer nested directories to a DOS or DOS/Windows Client running the SystemView Client, be sure the complete path name does not exceed the maximum 63-character length. If the total length of the path name exceeds 63 characters, some nested subdirectories and the files they contain will not be copied.

Figure 60 on page 76 shows a typical File Transfer window.

The top half of the File Transfer window represents your local system, and the bottom half represents the remote system you have accessed. The remote system's name is displayed above their remote system fields and in the window's title bar.

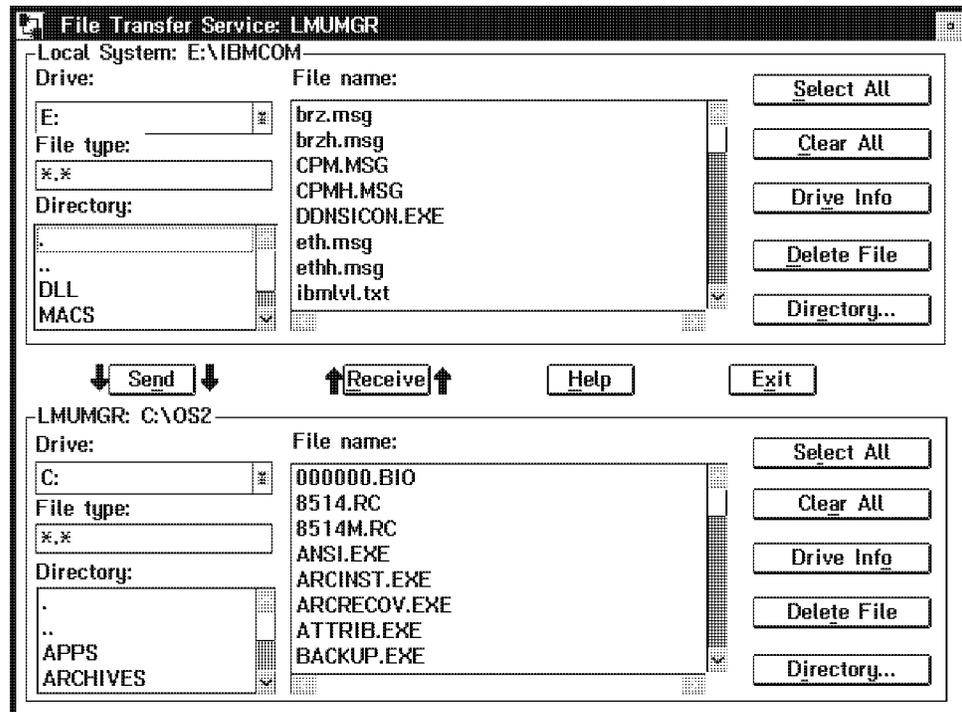


Figure 60. File Transfer Window

1.10.4.2 Local and Remote File Selection and Handling

To access individual drives and directories, select the desired drive or directory. File Transfer automatically updates all local or remote directory and file name displays as selections change.

The scope of the File name display can be narrowed by using the File type field. Select this field and adjust the file specifications as desired. All standard OS/2 wildcards are supported in this field.

To select single or multiple files for handling, select the individual files. Repeat this procedure to highlight multiple files. Multiple files can also be selected by dragging the mouse pointer across successive file names. Selections can be cleared by selecting **Clear All** at the right side of the field group.

To select all files within the displayed directory, select **Select All** at the right side of the field group. This will highlight all files displayed in the File name field.

Actions available for selected files are:

- Send
- Receive
- Delete

1.10.4.3 Local and Remote Directory Selection and Handling

Using File Transfer, you can select, transfer, or delete individual or multiple directories and directory trees. To access the directory utility program, select the **Directory** button next to the local or remote system that you want to access.

The available actions are:

- Transferring local directories
- Transferring remote directories
- Deleting local directories
- Deleting remote directories

1.10.4.4 Disabling Data Compression

To disable File Transfer's automatic data compression process, add the following statement in the CONFIG.SYS file:

```
SET NFFTCL=0
```

Once you have added this statement to your CONFIG.SYS file and have restarted your system, File Transfer will not use its automatic data compression capabilities under any circumstances.

1.10.5 Alert Manager



Alert Manager

SystemView Alert Manager enables you to receive and process application-generated alerts. A variety of actions can be taken in response to alerts, including alert logging, pop-up messages, forwarding the alert to another system, program execution, or an application-defined action. This service does the following:

- Simplifies application use and processing of alerts
- Allows applications to provide custom handlers and define conditions of their use
- Enables users to explicitly define conditions for use of standard handlers
- Allows new Alert Handlers to be added easily

SystemView Alert Manager includes standard Alert Handlers that do the following:

- Log the alert to a file
- Display the alert in a pop-up window
- Forward the alert to another workstation
- Execute a command
- Send a simple network management protocol (SNMP) version of the alert (not available on systems running SystemView Agent for DOS/Windows)
- Send an SNMP version of the alert to clear the alert condition (not available on systems running SystemView Agent for DOS/Windows)
- Play a waveform (WAV) sound file (requires multimedia support)

- Send a message to a digital pager through a modem (requires modem attached to system)
- Send the alert information to an alphanumeric pager through a modem (requires modem attached to system)
- Send the alert to another user using TCP/IP SENDMAIL (requires TCP/IP for OS/2 2.0 or later)
- Send the alert to Lotus Notes or cc:Mail using Vendor Independent Messaging (VIM) (requires VIM support)
- Export the alert information to a database
- Generate a Desktop Management Interface (DMI) indication, and send it to the DMI Service Layer (requires DMI support)
- Print the alert
- Add the alert to a text file
- Add an Error Condition to the system (see 1.10.5.3, “Error Conditions” on page 85)
- Remove the Error Condition from the system (see 1.10.5.3, “Error Conditions” on page 85)

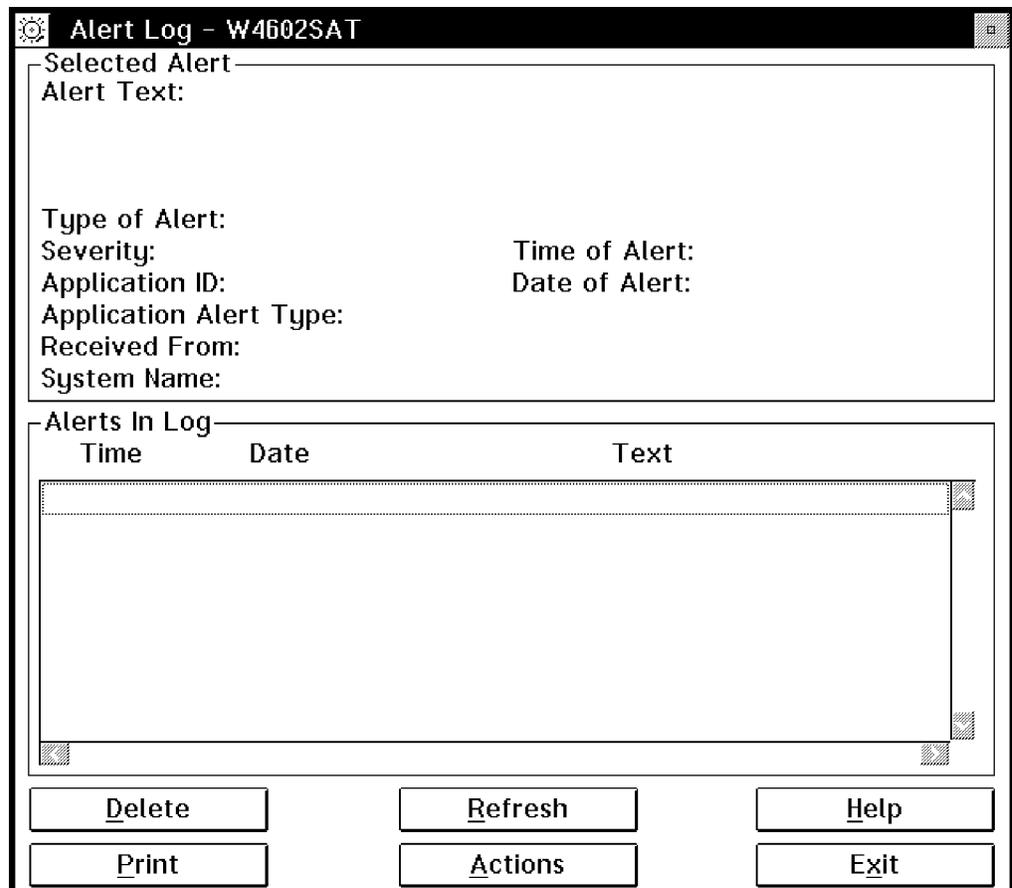


Figure 61. Alert Manager Main Window

1.10.5.1 Information on Individual Alerts

Select a specific alert from the alert log to display detailed information about the alert in the upper-half of the Alert Log window. You can select multiple alerts for the purposes of deleting multiple files or printing reports, but only the currently highlighted alert in the log will have its alert-specific information displayed at the top of the screen.

Information displayed about the selected alert includes:

Alert Text: The Alert Text includes the name of the alert, as well as any textual commentary included by the application that generated the alert.

Type of Alert: This is the application-specified alert type. A displayed alert consists of an Alert Sender name followed by an Alert Type.

The possible Alert Sender types are:

- System
- DASD
- Network
- Operating System
- Application
- Device
- Security

An Alert Sender might also be unspecified, in which case an Alert Sender value will not be displayed.

The possible Alert Type types are:

- Failure
- Error
- Warning
- Information

An Alert Type can also be unspecified, in which case an Alert Type value will not be displayed.

Severity: The alert Severity is a value from 0 to 7, with 0 being the most severe. For example, an alert Severity of 0 could be assigned to a disk failure, while a value of 7 could simply represent a system going offline at the end of a day. Alert Severity is determined by the application that generates the alert, and determines the actions that Alert Manager will then take, such as advising a user of a disk drive that is nearly full or launching applications to deal with disk errors or ECC memory failure.

Application ID: The Application ID is the name of the application that sent the specified alert to the log.

Application Alert Type: The Application Alert Type is a numeric value assigned to an individual alert by the application that generated it. This value is often used by the application itself.

Received From: Received From is the name of the system that generated the alert. Received From could be the local system or a remote system that has been instructed to relay alerts to the local error log.

System Name: This is the name of the system which sent the alert. The name is defined in the SystemView Configuration icon.

Time of Alert: The Time of Alert is the time of day when the alert was generated and logged.

Date of Alert: The Date of Alert is the calendar date on which the alert was generated.

1.10.5.2 Configuring Actions

Alert Manager enables you to configure automatic responses to alert conditions within your system. You can configure these responses (called actions) to respond to specific alerts, to alerts from a particular application, to alerts that have user-designated alert conditions, or to all alerts received.

Alert Manager includes standard actions that do the following:

1. **Log the alert to a file**

Puts the alert information into the Alert Log.

2. **Display the alert in a pop-up window**

Displays a small window with all alert-specific information.

3. **Forward the alert to another workstation**

Sends the alert to another user over a specified network. Once received, the alert is treated as though it were generated locally. When configuring this action, you will need to specify the Network Address of the workstation and the Network Type used by the workstation (NetBIOS, TCP/IP, or IPX). If you are unsure of the workstation's Network Type or Network Address, you can use Remote System Manager's Edit System action or system group Detail View (see Detail View) to check this information.

4. **Execute a command**

Executes a single command. This action includes special command strings (or macros) that enable you to imbed alert-specific data in the command. This data can then be used by the application that is started by the command line. These macros are:

Macro	Imbedded Information
%TXT	Alert Text
%TIM	Alert Time
%DAT	Alert Date
%SEV	Alert Severity
%SND	Alert Sender (for example, "NetBIOS::USER1")
%TYP	Alert Type
%APP	Alert Application ID
%AT	Alert Application-specific Type
%P1-%P9	Alert-specific text strings that are imbedded in the Alert Text. The content of these parameters is dependent on the alert itself.

5. **Send SNMP Alert**

Uses an SNMP agent to generate an SNMP version of the alert.

Note: This action requires IBM TCP/IP for OS/2 2.0 or later. OS/2 Warp Server contains IBM TCP/IP for OS/2 3.0. The SNMP Alert function is not available for local use on systems running SystemView Agent for Windows.

- a. NetFinity's management information base (MIB) file for use with NetWare SNMP management applications is found on NetFinity Services for NetWare, Diskette #1. It is named NETFIN.MIB. For information on how to use NETFIN.MIB with your SNMP-based systems management software, see the documentation that was supplied with your SNMP agent or with your systems-management product.
- b. NetFinity's management information base (MIB) file for use with OS/2 SNMP management applications is found in your NetFinity directory. It is named MIB2.TBL. You can append this file to your existing MIB2.TBL file, or replace your MIB2.TBL with this file.

6. Send an SNMP-Reset Alert

Uses an SNMP agent to generate an SNMP version of the alert that will indicate that the alert condition no longer exists.

Note: This action requires IBM TCP/IP for OS/2 2.0 or later. OS/2 Warp Server contains IBM TCP/IP for OS/2 3.0. The SNMP-Reset Alert is not available for local use on systems running SystemView Agent for Windows.

7. Play a WAV file (requires multimedia support)

Plays a specified waveform (WAV) audio file in response to the alert.

8. Send a message to a digital pager through a modem (requires a modem attached to the system)

Uses a modem attached to the system to dial out to a digital pager service. After the modem connects to the pager service, it will send all numeric data entered in the Digital Pager Display field. If your digital pager service requires that you press the pound sign (#) to send a page, be sure to type the # in the Digital Pager Display field after the numeric data.

9. Send the alert information to an alphanumeric pager through a modem (requires a modem attached to the system)

Uses a modem attached to the system to dial out to an alphanumeric pager service. After the modem connects to the alphanumeric pager service, it will send all alert information.

Note: This action will work only with pager services that use the telocator alphanumeric protocol (TAP). You must provide your pager's Pager ID.

10. Send the alert to another user using TCP/IP SENDMAIL (requires IBM TCP/IP for OS/2 2.0 or later)

Uses the TCP/IP SENDMAIL program to send the SystemView alert as a note to a specified email address.

11. Send the alert to Lotus Notes or cc:Mail via Vendor Independent Mail (VIM) (requires VIM support)

Uses the Vendor Independent Messaging (VIM) interface to generate a VIM-version of the alert that can be sent to any system that is VIM-compliant (including Lotus Notes, cc:Mail, and others).

12. Export the alert information to the NetFinity Database

Exports the alert information to a selected NetFinity Database.

13. **Generate a DMI indication and send it to the DMI Service Layer (requires DMI support)**

Converts the alert into a DMI indication which is then forwarded to the DMI Service Layer. Once it is received by the DMI Service Layer, it can be used by other DMI-compliant management applications.

14. **Print the alert**

Sends the alert to a printer attached to the system.

15. **Append the alert to a text file**

Adds the alert information to a specified ASCII text file.

16. **Add an Error Condition to the system**

Adds an Error Condition to the system's Error Condition Log. A system's Error Condition log is accessed with the Remote System Manager. For more information on Error Conditions, see 1.10.5.3, "Error Conditions" on page 85.

17. **Remove the Error Condition from the system**

Removes a previously generated Error Condition from the system's Error Condition log. A system's Error Condition Log is accessed with the Remote System Manager. For more information on Error Conditions, see Error Conditions.

Alert Actions: Select **Actions** from the Alert Log window to display the Alert Actions window. The Alert Actions window displays a list of all available and configured actions and enables you to select individually configured actions for editing, deleting, or to create completely new actions.

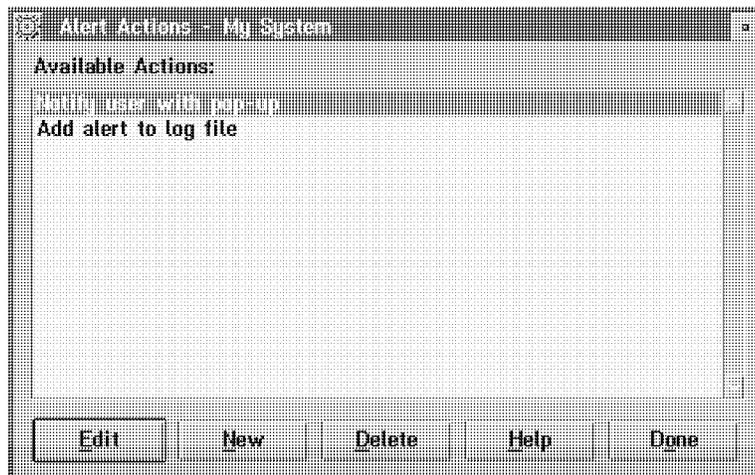


Figure 62. Alert Action Window: How the Alert is Processed

Alert Manager Action Editor: The Action Editor enables you to create and configure actions the Alert Manager will take in response to specific alerts. The Action Editor uses a series of user-defined Alert Conditions to determine which alerts will trigger a defined action.

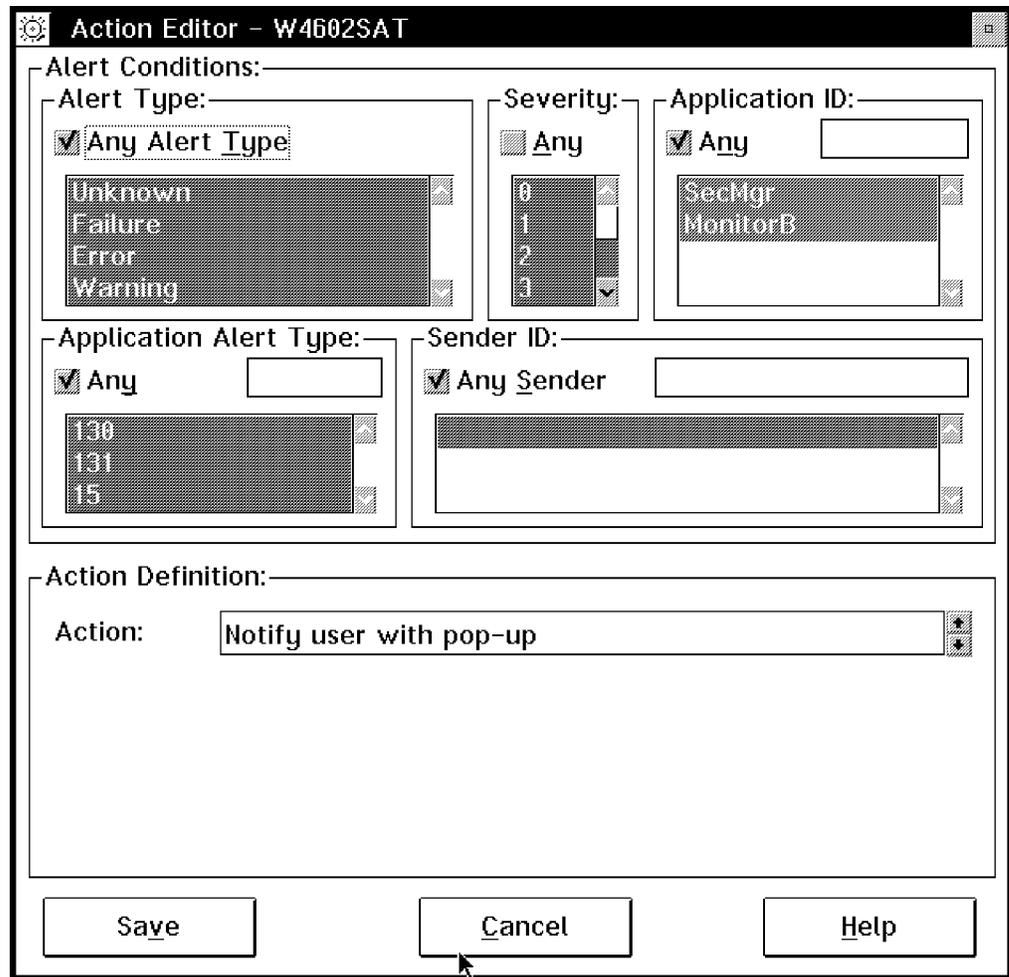


Figure 63. Alert Manager Action Editor Window

Configuring an action is a two-step process. First, you must set the Alert Conditions that the Alert Manager will look for. Then, you must set an Action Definition to define what action the Alert Manager will take in response to the received alert. Detailed descriptions of this process follow:

1. Set the Alert Conditions

When defining an action, you must first specify the Alert Conditions that must be met for the Alert Manager to execute a defined action. As alerts are received, the Alert Manager checks each of these conditions to see if they meet the specifications for a defined action. If all Alert Conditions are met, the defined action is executed.

There are five Alert Conditions that are used by the Alert Manager to determine appropriate action responses. For an alert to trigger an action, the alert must meet all of the alert conditions for the action. These five alert conditions are:

a. Alert Type

The Alert Type is a brief description of the generated alert. It describes the nature of the alert (unknown, failure, error, warning, information) and can also contain a general description of the source of the alert (system, disk, network, operating system, application, device, or security).

To screen incoming alerts for specific Alert Types, select one or more Alert Types from the selection list. If you do not want to screen for specific Alert Types, select the **Any** check box above the selection list.

b. Severity

The Severity is a number from 0 through 7 that indicates how serious a generated alert is. A severity of 0 represents a very serious alert, while a severity of 7 is relatively minor.

To screen incoming alerts for specific Severity values, select one or more Severity values from the selection list. If you do not want to screen for specific Severity values, select the **Any** check box above the selection list.

c. Application ID

The Application ID is the alphanumeric identifier of the application that generated the alert.

To screen incoming alerts for specific Application IDs, you can choose one or more from the Application ID selection list. If an Application ID you require is not available from the list, you can add it to the list by entering the ID in the entry field above the selection list and pressing **Enter**. If you do not want to screen for specific Application IDs, select the **Any** check box above the selection list.

d. Application Alert Type

The Application Alert Type is a numeric value assigned to an individual alert by the application that generated it. This value is often used by the application itself.

To screen incoming alerts for specific Application Alert Types, you can choose one or more from the Application Alert Type selection list. If an Application Alert Type that you require is not available from the list, you can add it to the list by entering it in the entry field above the selection list and pressing **Enter**. If you do not want to screen for specific Application Alert Types, select the **Any** check box above the selection list.

e. Sender ID

The Sender ID is the Network Address of the system that generated the alert.

To screen incoming alerts for specific Sender IDs, you can choose one or more from the Sender ID selection list. If a Sender ID that you require is not available from the list, you can add it to the list by entering it in the entry field above the selection list and pressing **Enter**. If you do not want to screen for specific Sender IDs, select the **Any** check box above the selection list.

2. Set an Action Definition

You must select a specific action handler, and supply any necessary information for the completion of the action.

a. Select an Action.

An Action is a program that carries out an action in response to an alert that meets the Alert Conditions that you have specified.

Use the spin buttons at the right of the Action field to see the available action handlers.

b. Enter additional information, if necessary.

If additional information is required, the parameter will be displayed in the Action field as <P#>, where # is the number of the parameter. An Action Definition parameter field appears for each required parameter, along with a brief description of the information that is required. Enter the appropriate information in each field.

3. Save the defined action

Once all Alert Conditions and Action Definition information has been entered, select **Save** to save the configured action. This action will now appear in the Available Actions window of the Alert Actions window. After you select **Save**, the Alert Manager window closes automatically.

1.10.5.3 Error Conditions

Select **Error Conditions** to open the system's Error Condition Log window. This selection will not be available if the Error Condition Log is empty.

Error Conditions are generated by the SystemView Alert Manager in response to SystemView alerts. Error Conditions simply alert the Remote System Manager that a notable event has occurred on one of the NetFinity systems in the network. When you configure the Alert Manager to generate an Error Condition in response to an alert, you must specify a name for the Error Condition. When the Alert Manager generates an Error Condition, it will place an Error Condition entry, using the name you specified, in the Error Condition Log of the system that generated the alert.

If a system currently has one or more entries in its Error Condition Log, its individual system object will be replaced by a generic system icon with a red *circle and slash* symbol. Any System Groups in the System Group Management window that contain this system will also change. This will help to alert you that the System Group contains one or more systems that have entries in their Error Condition Logs.

Error Conditions can be cleared in either of two ways:

1. Generate a Clear Error Condition message with the Alert Manager.

When the Alert Manager generates a Clear Error Condition message, it will clear only one identically named Error Condition from the log.

2. Select **Reset** from the Error Condition Log window.

This will clear all Error Conditions from the log.

Note: This function can only be performed on remote systems that are running NetFinity Manager or Services Version 3.0.

1.10.6 Power-On Error Detect



Power-On Error Detect

When IBM Micro Channel systems are powered-on, they perform a series on system hardware and configuration tests (called the Power-On Self Test or POST). If an error is detected, the system records the error and takes some appropriate action, such as loading its configuration utility program from the Systeeservices will be avail if no one is present when the utilities are loaded, or if

the system's user is unfamiliar with POST errors, the problem could go uncorrected for some time, leaving the system offline and unproductive.

However, if the Power-On Error Detect drivers are installed on an IBM Micro Channel system and an error is detected during POST, the system sends an SOS-style message out onto the LAN. This message contains valuable information about the POST error itself. Systems that have these drivers installed will also send a similar message out onto the LAN when their System Partitions are accessed during system startup (for example, when the user pressed Ctrl-Alt-Insert during startup).

The Power-On Error Detect service hears these messages on the LAN and enables you to quickly determine:

1. What system generated the POST error or System Partition access message.
2. What POST error (if any) was reported.
3. What caused the POST error.

The message also contains hardware configuration information that enables you to determine the possible cause of the problem before you've even left your desk, minimizing system downtime and loss of productivity with rapid problem determination and recovery.

For more information please see page 86 of the *IBM NetFinity Manager for OS/2 V3.0 - User's Guide*, S41H-6268.

1.10.7 Predictive Failure Analysis



Predictive Failure Analysis

Using the Predictive Failure Analysis (PFA) service, you can monitor all PFA-enabled disk drives installed locally on your system or on remote systems within your network. With this service, you will be instantly notified when a PFA-message is generated by a PFA-enabled drive. Also, you can configure this service to automatically generate an alert when a PFA message is received.

Note: PFA-messages generated by PFA-enabled disk drives that are in use as part of a RAID array cannot be detected by the Predictive Failure Analysis service. However, PFA-messages can be monitored and reported by using the System Monitor Service's attribute monitors for the PFA-enabled disk drive.

1.10.7.1 Predictive Failure Analysis Window

Each PFA-enabled physical drive is represented by an object in the Predictive Failure Analysis window. The Predictive Failure Analysis service uses two objects to help you quickly determine the status of each disk drive. These objects are:

Object	Description
Solid disk drive Normal	The drive has not reported any Predictive Failure Analysis messages.

Shattered disk drive Warning

The drive has reported one or more Predictive Failure Analysis messages and might be failing.

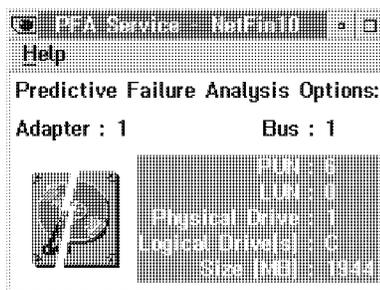


Figure 64. Predictive Failure Analysis

The PFA drive object shown represents a drive that has reported one or more Predictive Failure Analysis messages and might be failing.

Information that will help you identify the drive is listed beside its icon. This information includes:

Information	Description
Solid disk drive Normal	The Adapter is the value of the adapter card that the disk drive is connected to.
PUN and LUN	The physical unit number (PUN) and logical unit number (LUN) are values assigned to the hard disk drive to uniquely identify it within a system. Note: If an individual physical drive is partitioned into two or more logical drives, each logical drive will have the same PUN, LUN and physical drive value.
Physical Drive Values	The Physical Drive value is a numeric value assigned to each hard disk drive in your system. These values begin with 0 and increase with each additional hard disk drive installed (for example, if you have two hard drives in your system, their Physical Drive values will be 0 and 1).
Logical Drive Values	The Logical Drive value is a letter assigned to each hard disk drive or partition you create on a hard disk drive. For example, if you have a 1.0 GB drive, and you divide this drive into five partitions of 200 MB, they will have Logical Drive values of C, D, E, F, and G. However, each Logical Drive will share the same PUN, LUN and Physical Drive values. Note: If you are remotely managing a system running NetFinity Services for NetWare, the system will not report any logical drives.
Size	The Size value is the size of the physical drive. Note: Size does <i>not</i> represent space remaining on the individual drive.

To obtain more detailed information on an individual PFA-enabled drive, or to configure Predictive Failure Analysis service options for an individual drive, select the drive from the Predictive Failure Analysis window. This will open the PFA Options for Drive window (see 1.10.7.2, "PFA Options for Drive Window" on page 88 for more information).

1.10.7.2 PFA Options for Drive Window

Use the PFA Options for Drive window to view information about the selected PFA-enabled drive and to configure Predictive Failure Analysis service options specific to the selected drive (see Figure 65).

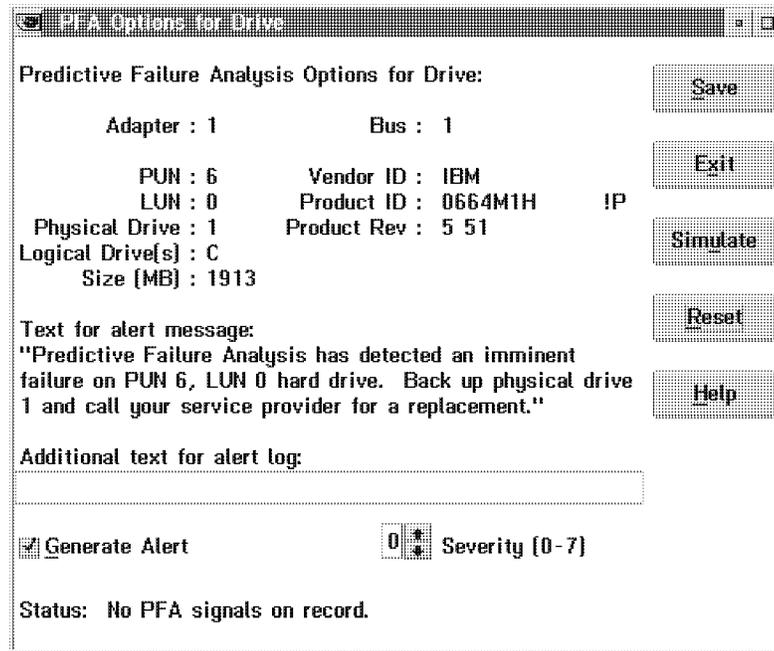


Figure 65. Working with Predictive Failure Analysis

Detailed Disk Drive Information: The PFA Options for Drive window duplicates the drive-specific information from the Predictive Failure Analysis window and also provides the following additional information:

Object	Description
Vendor ID	Name of the drive manufacturer reported by the disk drive.
Product ID	Drive-specific product number reported by the disk drive.
Product Rev	Product revision level reported by the disk drive.
Status	Shows the most recent information reported by the disk drive. If a PFA message has been generated by the disk drive, the Status data will show the day, date, and time at which the PFA message was generated.

Predictive Failure Analysis Options: The Drive window enables you to:

- Configure Predictive Failure Analysis' alert generation options for this drive.
- Simulate a Predictive Failure Analysis warning message for this drive.
- Reset the drive from *Warning* status to *Normal* status.

1. **Generating Alerts.** Select the Generate Alert check box to enable Predictive Failure Analysis to generate a SystemView alert whenever this disk drive generates a Predictive Failure Analysis message. You can customize some of the alert-specific information.
 - Alert Text. The standard Alert Text that will appear in the generated alert appears in the center of the window. If you would like to add information to this text, type it in the Additional text for alert log field.
 - Severity. Use the spin buttons beside the Severity field to set the alert severity value. This value can be an integer from 0 (most severe) to 7 (least severe).
2. **Simulating a Predictive Failure Analysis Message.** To simulate a Predictive Failure Analysis failure warning message for this drive, select **Simulate**. The Predictive Failure Analysis service will behave exactly as if an actual warning message had been received (it will change the drive status in the Predictive Failure Analysis window and in the PFA Options for Drive window, and will generate an alert if Alert Generation is selected). However, both the Status reported in the PFA Options for Drive window and the Alert Text will advise the reader that the PFA message was simulated and was not caused by a real PFA message.
3. **Resetting a Drive's Status.** Select **Reset** to change the drive's status from *Warning* to *Normal*.

1.10.8 Scheduling Events



Event Scheduler

The administrator can schedule various systems management events so they occur automatically. The administrator can create scheduled events, have them executed once or at specified intervals on one or more managed systems or on entire system groups, and maintain detailed logs of the results of these scheduled events. The administrator can also edit or delete previously created scheduled events as necessary. Scheduled events can automatically perform any of the following tasks:

- Perform hardware or software inventory on specified systems, and then:
 - Save the information as a history file
 - Print the information
 - Export the information to a database
- Distribute software to managed systems
- Transfer files and directories to or from managed systems or delete files from managed systems
- Execute commands on managed systems
- Access and manage the system partitions of managed systems
- Restart managed systems
- Export system monitor data to a database

The administrator can configure a scheduled event to run repeatedly at a specified time interval (hourly, daily, weekly, monthly, or yearly) for fully

automated systems-management functions (such as hardware and software inventory), or can run it once for special situations (such as Software Distribution or System Partition updating). The scheduler maintains a detailed log of all scheduled event results to ensure that automated tasks were executed correctly.

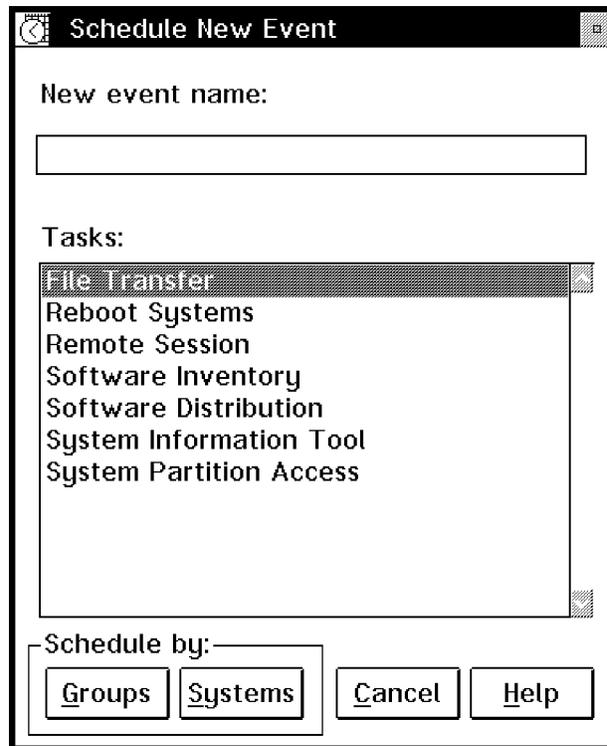


Figure 66. Scheduling a New Event

Figure 66 shows the window with the options for creating a new event.

Besides creating and scheduling events, the administrator can use event scheduling to:

- Delete a previously created scheduled event
- View a previously created scheduled event
- Edit a previously created scheduled event
- Refresh the list of scheduled events
- View the scheduler log

1.10.9 System Partition Access



System Partition Access

The SystemView System Partition Access allows for greatly simplified System Partition file handling of PS/2 computers, both locally and remotely. This service features:

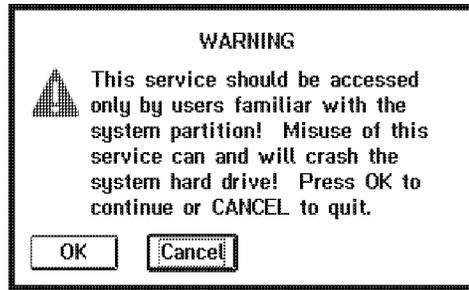


Figure 67. System Partition Access Misuse Warning

- Extensive file-level manipulation
- Initial Machine Load (IML) image updating
- Adapter Description Program (ADP), Adapter Description File (ADF), and Diagnostic Generation System (DGS) updating
- Set configuration program updating
- User-confirmation security to prevent accidental deletion of the System Partition

The System Partition is a group of preinstalled utility programs found on many PS/2 systems. If you are not using a PS/2 with a System Partition, you will not have access to, or a need for, this service.

Before you can use System Partition Access's features on another system, you must first select that system from a Remote System Manager System Group. Then, select the remote system's System Partition Access object. You are now ready to access the selected remote system's System Partition. Note that the top half of the System Partition Access window represents your local system, and the bottom half represents the remote system you have accessed. The remote system's System Name is displayed above the remote system fields and in the window's title bar.

Note: System Partition Access cannot access or manage the System Partitions on Enhanced Small Device Interface (ESDI) systems.

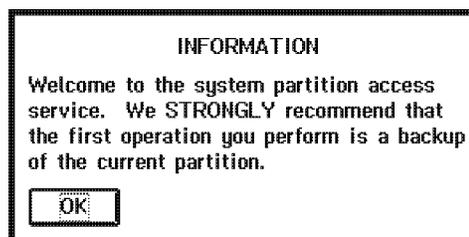


Figure 68. System Partition Access Backup Warning

1.10.9.1 Available System Partition Access Actions

SystemView System Partition Access offers a variety of System Partition file-manipulation actions. Available actions are:

- Copy from partition
- Copy to partition
- Delete directory

- Rename directory
- Delete file
- Rename file
- Partition backup
- Partition restore
- Delete partition
- Make directory
- Quit

1.10.10 Process Management



Process Manager

The SystemView Process Manager service enables you to view detailed information about all processes that are currently active on a system. Process Manager enables you to execute commands on the system, halt individual processes, monitor any process that you've specified and generate a SystemView Process Alert if the process is started, stops, or fails to start within a specified amount of time from startup.

1.10.10.1 Gathering Process Information

When you start Process Manager on your system or on a remote system, it will immediately gather information about all currently active processes on the system. This information is then displayed in the Process Manager window. Each process is signified by an icon depicting the type of process that is running (OS/2 window or full screen, Presentation Manager application, Windows application, NetWare Loadable Module (NLM), or DOS session), followed by data specific to the session type. The following information is available for each process:

- **Program Name** (All operating systems)
The name of this process, as well as the fully qualified path (if applicable) showing where the program resides on the system.
- **Process ID** (OS/2, Windows)
The operating system's internal identification value for this process.
- **Parent Process ID** (OS/2, Windows)
The operating system's internal identification value for the process or program that spawned this process.
- **Number of Threads** (OS/2, NetWare)
The number of program threads that this process is using.
- **Session ID** (OS/2 only)
The operating system's internal identification value for the session that is supporting this process.
- **Description** (NetWare only)
A brief description of the NetWare NLM (NetWare Loadable Modules).

- **Version** (NetWare only)
The NetWare NLM version number.
- **Date** (NetWare only)
The date of the NetWare NLM.

Note:

1. Available information about the process depends on the type of process and the operating system under which the process is running.
2. Windows and DOS processes running under OS/2 will appear as DOS sessions.

1.10.10.2 Running Commands

Process Manager enables you to send individual commands to the SystemView system that you are accessing. Unlike the Remote Session service, Process Manager will only enable you to issue a single command at a time, and you will not receive any textual feedback.

To run a command:

1. Select **Run command...** from the Process Manager window's Process pull-down menu.
2. Type in the Enter command line to be executed field the command that you want to execute on this system.
3. Select **Run** to execute the command.

Select **Cancel** at any time to close the Run Command window without executing a command.

1.10.10.3 Halting Processes

Attention

Use Process Manager's process-halting capabilities carefully. Process Manager enables you to halt almost any process that is running on a system. Irresponsible use of Process Manager can result in loss of data and could halt the operating system.

The method by which a process is halted depends on the operating system that the process is running under. For more information about the operating system, select **Operating System Information** from the System pull-down menu.

To halt a process that is running on a system:

1. Select the process that you want to halt.
2. Select **Process** from the Process Manager window's menu bar, or use mouse button two on the selected process to open the process's pop-up menu.
3. Select **the appropriate halt process** action for the system's operating system.
 - If the system is running OS/2, select one of these three process-halting actions:
 - Select **Send Ctrl-C** to send a `Ctrl-C` command to the selected process.
 - Select **Send Ctrl-Break** to send a `Ctrl-Break` command to the selected process.

- Select **Send Kill Process** to send a Kill Process command to the selected process.
- If the system is running Windows, select **Close Application** to halt the selected process.
- If the system is running NetWare, select **Send Unload Module** to halt the selected process.

1.10.10.4 Process Alerts

The Process Manager enables you to generate a SystemView alert when any specified process:

- Starts running
- Stops running
- Fails to start running within a specified amount of time after system startup

To configure Process Manager to generate an alert when a process starts, stops, or fails to start, select **Process Alerts...** from the Process pull-down menu. This opens the Process Alerts window. The alert condition field in the Process Alerts window contains a list of all currently configured Process Manager Alert conditions. Each Alert condition includes the name of the process that will trigger a SystemView Process Alert, and the conditions under which the alert will be generated.

From the Process Alerts window, you can:

- Add a Process Alert
- Edit a Process Alert
- Delete a Process Alert

Adding a Process Alert: Select **Add** to open the Add Process Alert window. This window enables you to configure a Process Alert for a specific process that will generate a SystemView Alert whenever the process:

- Starts running
- Stops running
- Fails to start running within a specified time

To add a new Process Alert:

1. Type in the Program Name field **the name of the process that you want to monitor**.
 - If you want to monitor a specific process that is run from a specific directory, type in the fully qualified path where the executable resides (for example, C:\APP\PROGRAM.EXE).
 - If you want to monitor any process with a specific name, type in only the name of the executable (for example, PROGRAM.EXE).
2. Type a severity value for the SystemView Alert that will be generated by Process Manager in the Alert Severity field.
3. Select one (or more) **Generate alert** checkboxes.
 - Select **Generate alert when program runs** to generate an alert if the specified process is started.
 - Select **Generate alert when program stops** to generate an alert if the specified process is stopped.

- Select **Generate alert if program not started** to generate an alert if the specified process does not start within a specified amount of time after system startup. The amount of time that Process Manager will wait before generating the alert is specified in the Execution time-out field.

4. Select **OK** to save this Process Alert.

Select **Cancel** at any time to close the Add Process Alert window without saving any changes.

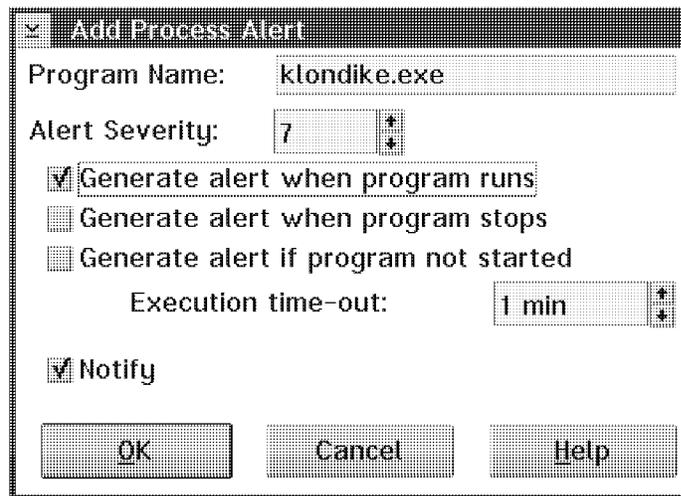


Figure 69. Process Management

1.10.11 Managing Systems Connected by Modem



Serial Control

The SystemView Serial Control service enables you to use your system's modem to remotely access another SystemView system.

Once properly configured, the Serial Control service will enable you to access and manage other modem-attached SystemView systems just as if they were attached to your LAN.

Also, if your system is not LAN-attached, the SystemView Serial Control service will enable your system administrator to manage your system that is using any of the SystemView applications without having to visit your office or interrupt your work.

Note: Your system *must* have a properly installed and configured modem that supports at least 9600 baud for the Serial Control service to function.

1.10.12 Remote Control Functions

Remote control functions are necessary when the network administrator, or anyone responsible for the network, needs to access a remote workstation from their machine and do the necessary corrections in order to make it work properly.

The Controller machine is the machine that the administrator uses to take control of the Remote machines, and the Remote, Target or Controlled machine is the system that is controlled remotely.

In some cases, it is only necessary to have a remote command interface from the Remote machine in order to correct some configuration file or start an application or move a file.

Or maybe we need only to have a view of the Remote machine, just to verify that it's working well.

In other cases, it is necessary to have total control of the workstation and be able to use mouse and keyboard, just as if you were seated in front of the Remote machine.

Sometimes it is also necessary to transfer a file from the Remote machine to the Controller and vice versa.

For each of these different situations, SystemView in Warp Server provides a particular functionality that best adjusts to one of these prerequisites. These can be:

- Remote Session
- Remote Workstation Control
- Screen View
- File Transfer

1.10.13 Remote Session



Remote Session

Using the Remote Session service, the administrator can establish a fully active remote command-line session with a managed system. This session is capable of all command-line functions that are available under the managed system's operating system.

Both users, managed and manager can see the command-line session and can enter commands.

Remote systems management icon

The icon of the Remote Session appears only when the administrator is accessing a managed system through the Remote System Manager.

Note: Remote Session returns only standard textual I/O. Entering a command that starts a graphic application on the managed system will cause the managed

system to appear to hang. If this occurs, it is necessary to close the Remote Session and begin again.

During the Remote Session, all local keystrokes are passed through to the managed system. However, some keystroke combinations are available to the SystemView manager. These combinations are:

Keystroke	Result
[Alt+Esc]	Switches to the next open window, Full-Screen session or object that is minimized on the desktop
[Alt+Shift+Tab]	Makes the desktop window active
[Ctrl+Alt+Del]	Restarts the operating system on the SystemView Manager
[Ctrl+Esc]	Displays the window list on the SystemView Manager
Print Screen	Prints the contents of the window on the managed system to the default local printer

Keystrokes other than those listed are treated as they would be under the managed system's default command shell. If the managed system is running OS/2, the default command shell is CMD.EXE. If the managed system is running Windows, the default command shell is the managed system's DOS COMMAND.COM, as shown in Figure 70:

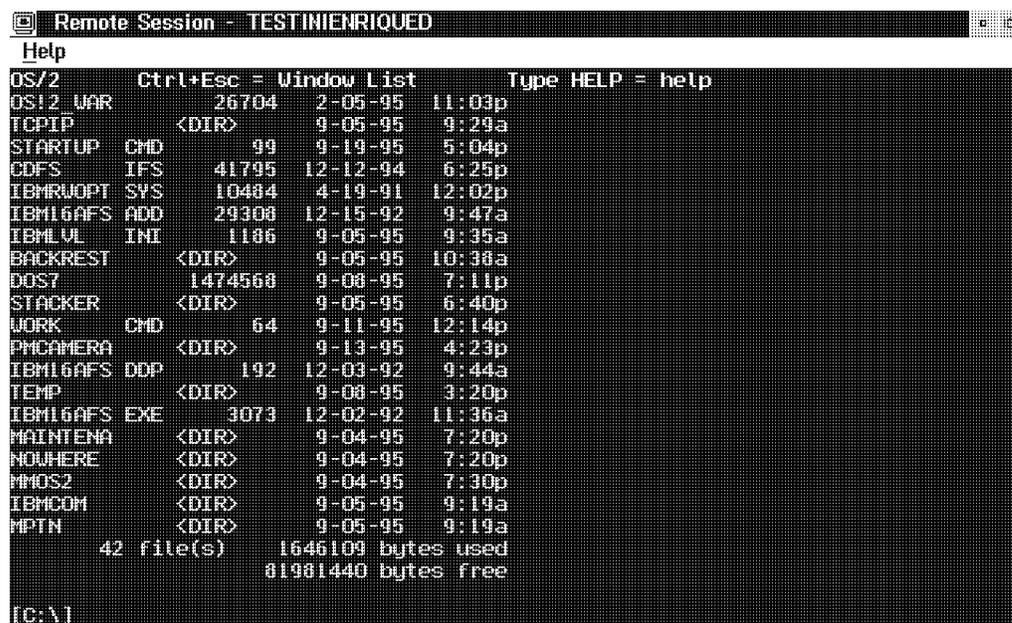


Figure 70. Viewing a Remote Machine's OS/2 Window

The Remote Session is closed the same way as a normal OS/2 or DOS window, by using the `Exit` command or by clicking twice in the upper-left check-box.

Figure 71 on page 98 shows one text application, such as `FDISK`, running on a remote server.

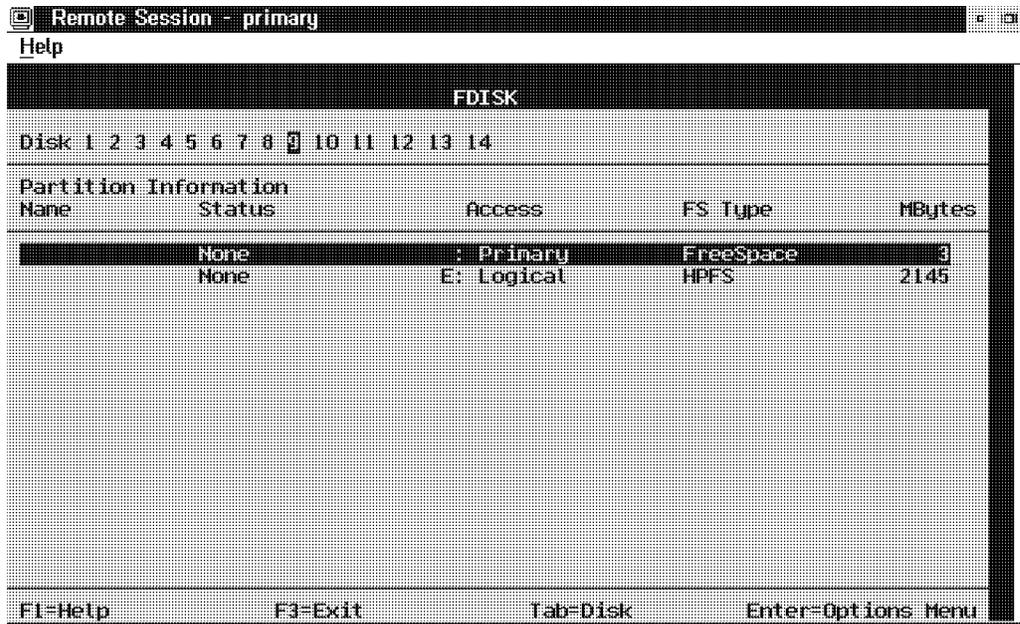


Figure 71. Text Mode Application: FDISK Example

If you run a Presentation Manager (PM) application from the Remote Session, the graphical output coming from that application will not be redirected to the manager, and then, the PM application will be displayed on the Remote machine. For this reason, you will see no output at the manager session. If you end or break the PM application (for example, using [Ctrl+C]), you will receive the shell command prompt again.

When you start a Remote Session at the managing workstation, the RCSHD.EXE (remote console shell daemon) program is started as a background task in the managed workstation.

The user at the managed workstation will see one entry in his window list pointing to that daemon. This daemon looks identical to the Remote Session the administrator has started, but in Full-Screen mode.

The user at the managed workstation can interoperate with every action the administrator actuates from the manager, and eventually, he can close the Remote Session the administrator has opened, by simply closing the RCSHD.EXE program.

1.10.14 Remote Workstation Control



Remote Workstation Control

Using the Remote Workstation Control functions of SystemView in Warp Server, one administrator at a SystemView Manager workstation can control the keyboard and mouse input and monitor the display output of a managed workstation without being physically present at the client.

Remote Workstation Control functions are useful if you need to:

1. Assist the user of the client workstation with running applications

2. Do remote problem determination and diagnosis
3. Have access to data and programs stored on a client workstation
4. Remotely monitor work in progress on client workstations (for example between teachers and students)

Figure 72 on page 101 shows an example of a Remote Workstation Control. The window with W4602S00 in the title bar (upper-left) is a part of the display coming from the Remote machine. The scroll bars allow us to access the different parts of the display. We can maximize, minimize or close this window as we do with a normal one.

Whatever we do inside these windows (having this window in foreground) is transmitted and executed on the remote workstation. For example, if we move the mouse inside, the mouse is also moved in the remote workstation. If the mouse is moved externally to that window, nothing happens in the Remote machine.

You can, for example:

- Click and double-click on an object
- Open a folder
- Open an OS/2 Windows or Full-Screen session
- Write inside or, for example, start an application PM- or non-PM-based
- Open a DOS Windows or Full-Screen session
- Write inside or, for example, start a DOS application from there
- Start WIN-OS/2 in window
- Move objects

But there are some things that you cannot do or things that you need to do in another way. For example:

1. You cannot use the following combination of keystrokes (see 1.10.14.3, "Change Keystrokes Mode Function" on page 102):
 - [Alt+Esc]
 - [Alt+Tab]
 - [Ctrl+Esc]

Note: Some tips for remote keyboard and mouse use:

- a. If you want to send to the client the keystrokes in the above list, make your choice from the Keystrokes pull-down menu, and continue working on the client.
 - b. The mouse affects the window that it points to. If the mouse points to a part of your own window, it works on your workstation. If it points to the display of the client screen, it works on the client.
2. You cannot restart the client machine from the Remote Workstation Controller.

In fact, using SystemView in Warp Server, you can reboot and eventually restart, the client machine in three ways:

- a. Using Remote Session (see 1.10.13, "Remote Session" on page 96) and executing the `SETBOOT /B` command of OS/2 (this option is not available for DOS clients and requires that Boot Manager is installed). Using this method, you cannot restart the system.

- b. Using the Remote Workstation Control and selecting **Shutdown** with the mouse and/or keyboard as in a normal OS/2 machine but from the Controller.
- c. Choosing **System Restart** from the pop-up menu in the Remote machine icon (see Figure 30 on page 39).

Before shutting down

Before shutting down and restarting a remote system, be sure that:

- The operating system startup process completes without interruption in any statement of CONFIG.SYS. If you are not sure, add to your CONFIG.SYS the following statement:

```
PAUSEONERROR=NO
```

- Check that SystemView Support Program is starting automatically when the machine starts. Usually, this program starts from the Startup Folder. In this case, check that the following statement doesn't appear in CONFIG.SYS:

```
SET RESTARTFOLDERS=NO
```

If you find this statement, simply remove it or REM it out; otherwise the SystemView Support Program selected to autostart from the Startup Folder won't be activated.

If you need to keep this statement in CONFIG.SYS, add in your STARTUP.CMD the following statement:

```
START x:\SYSVIEW2\BIN\NETFBASE.EXE
```

where x is the drive where SystemView in Warp Server is installed.

1.10.14.1 Comparison of SystemView Remote Workstation Control and DCAF Functions

Note: DCAF is Distributed Console Access Facility.

Remote Workstation Control included in SystemView in Warp Server is the result of the integration of the existing DCAF product to the new SystemView in Warp Server architecture.

For this reason, some features of DCAF were delegated to common, centralized functions already implemented in SystemView in Warp Server.

We will discuss some of the functions of the DCAF product that were not implemented in SystemView, and, for each case, the SystemView function that replaces the one that was dropped.

1. Gateway function in DCAF was dropped out for two reasons:
 - a. This release of SystemView in Warp Server doesn't support APPC as a communications protocol. The existing DCAF product requires APPC as a connection protocol for the gateway.

Note: APPC is Advanced Program-to-Program Communication.
 - b. One SystemView Manager can see and browse resources of another SystemView Manager on the same network; for example, the first SystemView Manager is part of a NetBIOS LAN, and the second

SystemView Manager is on the same LAN but can also reach resources of a TCP/IP LAN.

Then, the first SystemView Manager, through the second one, will be able to see and also browse resources of the TCP/IP LAN.

In other words, the second SystemView managed function is a gateway, allowing the first one to manage resources of a network that it cannot access directly.

So, we conclude, there is no need to implement a gateway function of the DCAF product when it is included in the SystemView environment.

- 2. Authenticator functions in DCAF were dropped because all security concerns were delegated to the Security Manager (for information about Security Manager, see 1.7, "Implementing Security" on page 40).
- 3. File Transfer is not available in the Remote Workstation Control because there is one special function already implemented in SystemView (for information about File Transfer, see 1.10.4, "File Transfer" on page 75).
- 4. The File Packager function of DCAF was not included because the Remote Workstation Control was integrated in SystemView in Warp Server, and SystemView in Warp Server does not have a similar function.

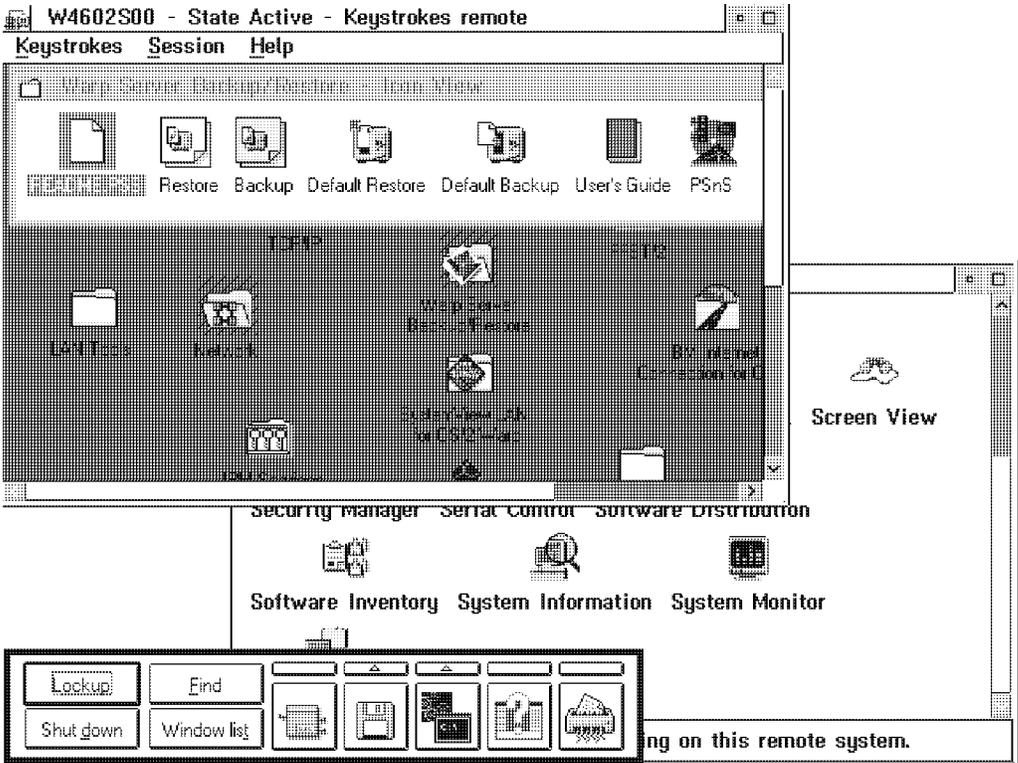


Figure 72. Remote Workstation Control Example

1.10.14.2 SystemView in Warp Server Remote Workstation Control Configuration

You can configure the following parameters:

- Start Remote Workstation Control sessions in Active state (see 1.10.14.4, “Session State” on page 103)
- Allow the target to terminate a session
- Refresh rate in milliseconds

For more information about these parameters, please see “Third page - Remote Control: Configuration Parameters for Remote Workstation Control” on page 22.

1.10.14.3 Change Keystrokes Mode Function

This choice, activated from the Keystrokes pop-up menu, is used only during an active session to determine which workstation, yours or the client, your input affects.

- **Keystrokes Local**— This option gives keyboard control back to the client user and allows you to work on your own keyboard.
- **Keystrokes Remote**— This choice allows you to work on the keyboard of your client. To work on your own keyboard, press the hot key combination and then switch to the Keystrokes Local.

Note: You can obtain the same effect by using the combination [Alt+T] to switch keystrokes back and forth between your own keyboard and the keyboard of the client.

The operating-system hot key combinations always affect your workstation and *not* the client.

The following table shows the relationship between the keystrokes or combination of keystrokes, the source, the effect caused and where this effect takes place.

<i>Table 5 (Page 1 of 2). Special Keystrokes and Mouse and their Effects in the Local or Target Machine</i>			
Keystrokes / Mouse	Coming from the Keyboard (Local Mode)	Coming from the Keyboard (Remote Mode)	Coming from the Pull-down Menu
[Alt+Esc]	[Alt+Esc] in the local machine	[Alt+Esc] in the local machine	[Alt+Esc] in the remote machine
[Alt+Tab]	[Alt+Tab] in the local machine	[Alt+Tab] in the local machine	[Alt+Tab] in the remote machine
[Ctrl+Esc]	[Ctrl+Esc] in the local machine	[Ctrl+Esc] in the local machine	[Ctrl+Esc] in the remote machine
[Ctrl+E]	[Alt+Esc] in the remote machine	[Ctrl+E] in the remote machine	Not supported
[Ctrl+U]	[Alt+Tab] in the remote machine	[Ctrl+U] in the remote machine	Not supported
[Ctrl+C]	[Ctrl+Esc] in the remote machine	[Ctrl+C] in the remote machine	Not supported
Other keystrokes	The same keystroke in the local machine	The same keystroke in the remote machine	Not supported

Table 5 (Page 2 of 2). Special Keystrokes and Mouse and their Effects in the Local or Target Machine

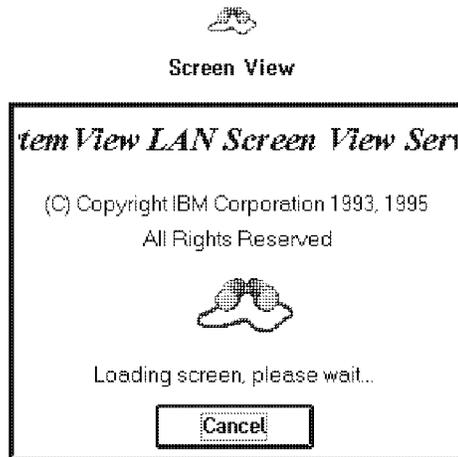
Keystrokes / Mouse	Coming from the Keyboard (Local Mode)	Coming from the Keyboard (Remote Mode)	Coming from the Pull-down Menu
Mouse	local machine	remote machine	Not supported
Note: <ul style="list-style-type: none"> • Use [Alt+Esc] to see your full screen or window sessions in rotation. • Use [Alt+Tab] to see the system menu for the OS/2 client full screen or window sessions in rotation. • Use [Ctrl+Esc] to see the OS/2 window list. 			

1.10.14.4 Session State

The session state represents the kind of access that you have to the client during a session. They can be:

- **Active**— You take control of the keyboard and mouse of the client, and you see the output in your monitor. You can use the shortcut key [Ctrl+A] instead.
- **Monitor**— You cannot control the keyboard and mouse of the client, but you can observe the screen and see the changes dynamically. You don't see the mouse pointer of the client, but you see the effects of what it does. You can use the shortcut key [Ctrl+M] instead.
- **Suspend**— Interrupts the session temporarily. The communications link with the client continues. You cannot control the client or view its screen. Your session window displays the client screen as it appears just before you suspend the session. You can use the shortcut key [Ctrl+S] instead.
- **Terminate**— Ends the session and the communication link with the client. You can use the shortcut key [Ctrl+T] instead.

1.10.15 Capturing a Managed System's Screen Image with Screen View



The administrator can view a snapshot of any managed system's current screen display through the Screen View service. The managed system's Desktop image is converted into a bitmap (BMP) file, compressed, and transmitted to the administrator's system, which then decodes the data and displays a scalable window of the managed system's display. The administrator can save screen images and load previously saved screen images for later viewing.

Note: Screen View cannot capture DOS Full-Screen sessions.

You can see one example in Figure 73.

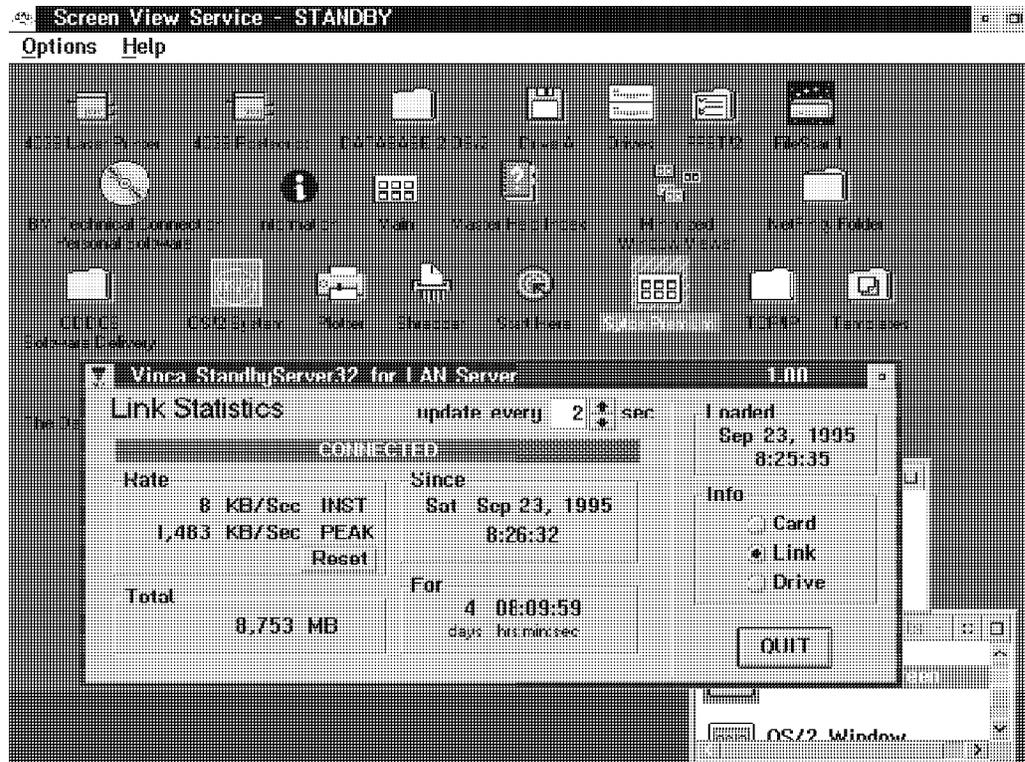


Figure 73. Screen View

The Screen View pop-up menu gives you the capability to:

- Capture a new screen
- Save the screen shot as a bitmap
- Load a screen-shot previously saved

1.11 SystemView Agent for OS/2

The SystemView Agent is a set of functions and agents that provide flexible management of the applications and resources in your system. Management applications gain access to applications and resources in your system through the SystemView Agent. The SystemView Agent has a number of subagents. Each subagent monitors its respective products and passes the information through the SystemView Agent to the managing application.

OS/2 Warp Server does not contain a management application. OS/2 Warp Server can be managed through the SystemView Agent by an SNMP manager such as NetView for OS/2 or NetView for AIX. In this section, we discuss the content of the SystemView Agent. For detailed installation and configuration information, refer to the online documentation installed with the SystemView Agent.

The SystemView Agent provides access to the following through its subagents:

- Resources and applications in your system that conform to the Desktop Management Interface (DMI)
- Resources and applications in your system that can be managed through the SNMP Distributed Protocol Interface (DPI)

1.11.1 SystemView Agent, DMI and DPI

The Desktop Management Interface (DMI) is a standard that has been published by the Desktop Management Task Force (DMTF). The DMTF is a vendor alliance which was formed to streamline the management of the diverse operating systems commonly found in an enterprise.

The SystemView Agent program provides access to system components that have been defined according to the DMI standard by acting as an SNMP agent. Although the DMI itself is protocol-independent, SystemView Agent can detect any DMI-enabled components in the system and translate the management information file (MIF) into SNMP objects that conform to the management information base (MIB) format. This MIF-to-MIB mapping is performed automatically by a DMI subagent provided with SystemView Agent.

The SystemView Agent program extends the use of the DMI by providing a MIF conversion utility and a MIF-to-MIB mapping function. Each MIF file in the system can be translated to an SNMP MIB with the conversion utility. SNMP-based management applications can then access attributes from these translated MIBs and perform standard SNMP Get and Set operations. If an SNMP management application changes an attribute in a translated MIB, SystemView Agent converts the request and forwards it to the DMI. When the response comes back and the appropriate MIF is updated, SystemView Agent translates the MIF information again and updates the associated MIB.

SystemView Agent's ability to perform this MIF-to-MIB mapping enables an SNMP management application to manage any component that implements the

DMI. SNMP Agent describes the relationship between an SNMP management application and the elements of the DMI.

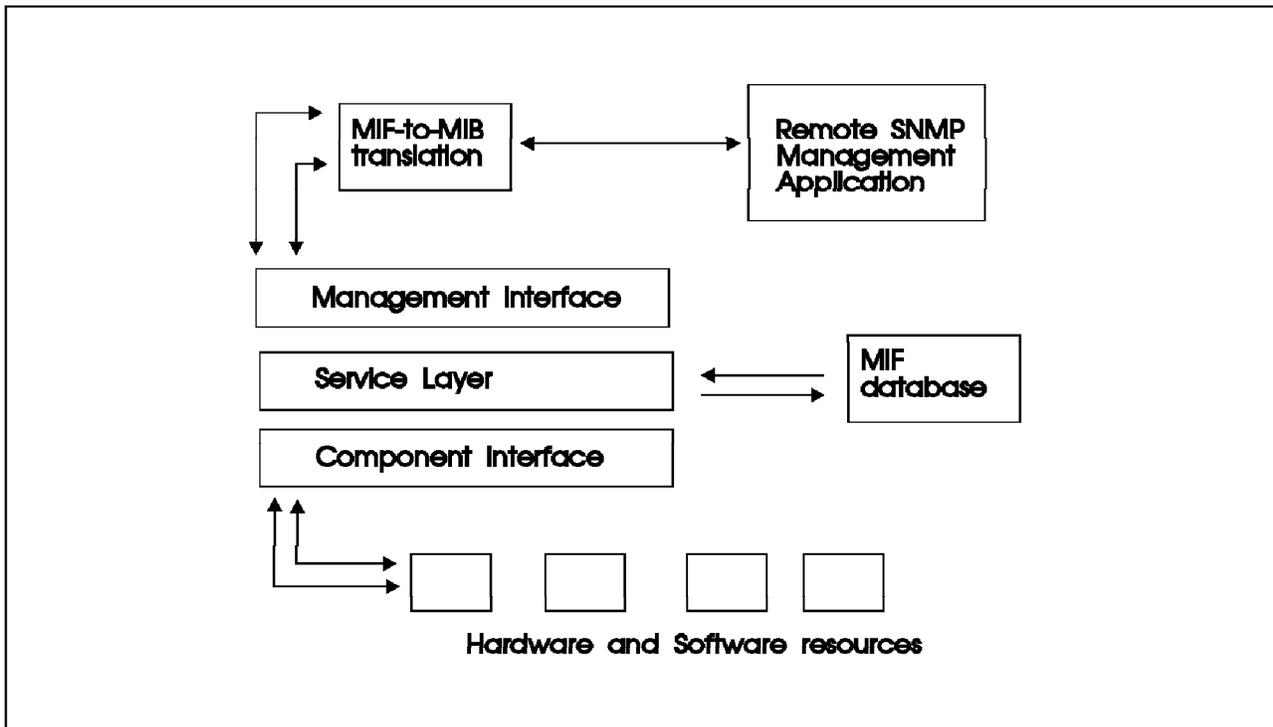


Figure 74. Using the DMI with an SNMP Management Application

The SystemView Agent also includes several subagents that can communicate with SNMP management applications. They include:

- OS/2 subagent (System Information Agent-SIA)

This allows for the management of OS/2 Nodes. With the OS/2 subagent, you can monitor:

- Logical storage areas
- Installed devices
- Local printers status
- File systems, partitions, and local disks status
- CPU utilization
- Installed software

- LAN Requester subagent

This agent allows SNMP managers to monitor and control the LAN Requester product. You can query information about the operational state, runtime configuration parameters and performance metrics. This includes data about service statistics, IBMLAN.INI configuration and read/write performance metrics. The control functions include activating or deactivating the LAN Requester services and setting selected runtime configuration parameters. Errors detected by the LAN Requester, which result in FFST alerts, are routed to SNMP managers as traps.

- LAN Server subagent

This subagent allows SNMP managers to monitor and control the LAN Server product. You can query information about the operational state, runtime configuration parameters and performance metrics. This includes data about service statistics, IBMLAN.INI configuration and performance metrics. The control functions included are activating and deactivating the LAN Server services and setting selected runtime configuration parameters.

Errors detected by the LAN Server product which result in First Failure Support Technology (FFST) alerts are routed to SNMP managers as traps. The LAN Requester subagent must be running to process the FFST alerts.

- Communications Manager/2 subagent

The Communications Manager/2 subagent allows SNMP managers to monitor and control the Communications Manager/2 product. You can query and control information about the product, operation state and SNA resources. The Communications Manager/2 subagent also provides error messages and information on configuration files.

- Database 2 for OS/2 subagent

The Database 2 for OS/2 subagent enables you to retrieve and modify the database configuration parameters, including the size of the lock list and the size of the database heap. You can also modify the Database Manager configuration parameters. All of the databases cataloged to the system are enumerated. You can control local databases with actions such as backup and restore.

1.12 License Management

In any network, a large number of licensed products are running at any one time. By effectively managing these licenses, administrators can determine how and when products are used and when additional licenses are required.

If software that has been enabled for license management is installed on managed systems, SystemView License Use Management Runtime for OS/2 (SystemView License Management) monitors usage of the licenses for that software. Software that is not enabled for license management cannot be monitored.

None of the products contained within OS/2 Warp Server is license enabled. The SystemView product, available separately, is itself enabled for license use management.

SystemView License Management can:

- Collect information on the use of license-enabled software, which will help the administrator determine how many licenses are needed
- Notifies the administrator, or takes other actions depending on the license-use management policy of the software vendor, when the number of licenses in use for an application is about to equal or exceed the number authorized
- Measures software use for purposes of establishing charges for software
- Produces reports and statistics

The license use management is made up of three components:

1. Development component

Used by software developers to enable their products for license use management. This is not part of SystemView License Management and is contained in a separate product called SystemView License Use Management Application Developer's Toolkit for OS/2 (also referred to as License Use Toolkit).

2. License Server component

This component must be installed on one or more workstations in the network. It contains the license information and controls the execution of the license-enabled products. It is also referred to as License Use Runtime Server.

3. Client component

This has to be installed on every workstation where a license-enabled product is installed. It is also referred to as License Use Runtime Client.

1.12.1 Licensing Models

SystemView License Management is able to manage licenses for products that use the nodelocked licensing and/or the server-based licensing model. There are four license types that fall into the above models.

1.12.1.1 Nodelocked Licensed Products

This model provides support for the Nodelock license type. A Nodelock license allows the use of a product at the particular node for which the license was created and for as long as the license remains valid. For example, when a user starts a product licensed in this way, the License Use Management Runtime (a part of the Client component) looks in a local file (called a Nodelock file) for a Nodelocked license password to run. If the file does not exist or does not contain a valid license, the product may fail or run for a limited period of time, depending on the policy of the vendor.

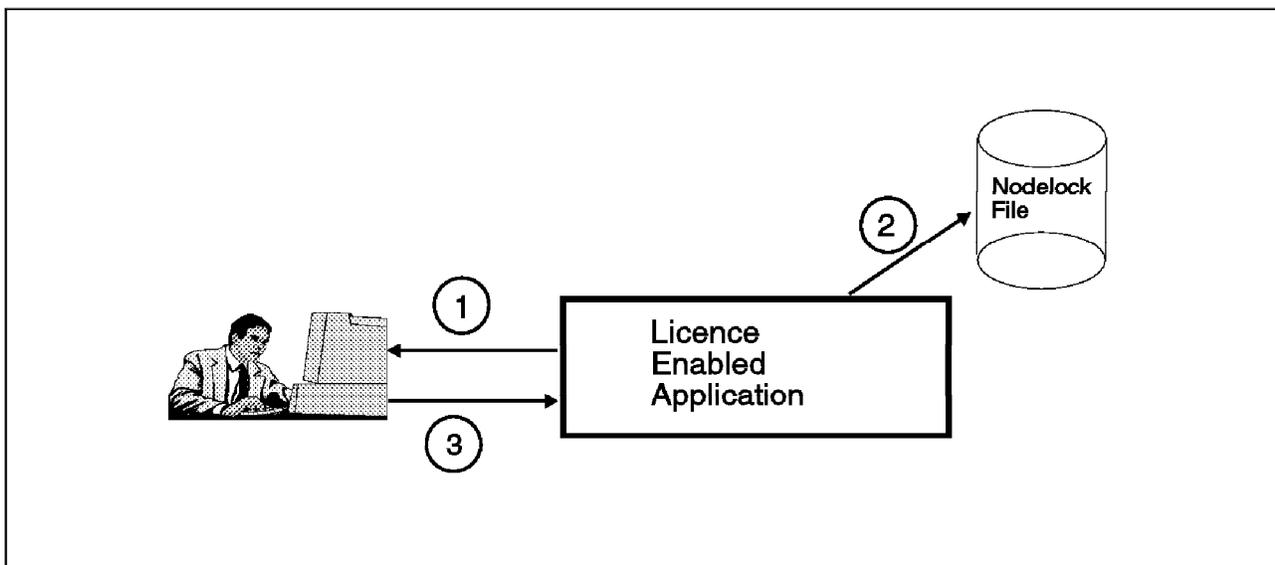


Figure 75. Using a Nodelocked License

In Figure 75, the following steps are executed for a Nodelocked- licensed application:

1. The user invokes the application.

2. The application checks for the Nodelock license. This license comes in the form of an electronic password which is contained in an enrollment certificate that the vendor gives you with the product. This license is linked, at time of license creation, to the unique identifier (target ID) of the system where you intend to run the licensed product.
3. The application runs, or returns information to user, depending on license request status.

Because a Nodelock license and the application that requires the license are always installed on the same machine, a Nodelocked product does not require the presence of a license server on the network.

1.12.1.2 Server-Based Licensed Products

Using this model, any potential user of a software product running on a network may contact a license server for the use of a license. This model provides support for the following license types:

- Concurrent Access

This is a server-based license type where a license is temporarily granted to run the product for which the license was created. When the license is in use, it remains unavailable to other requests. The license is eventually returned to the server, where it again becomes available.

- Use-Once

This is a license type that allows for a single use of a particular product within the period for which the license is valid. When the product stops running after being started, the use-once license ends.

Many vendors may use use-once licenses to safely distribute promotional or demonstration versions of their software.

- Dynamic Nodelocked

This license type is the same as a Nodelock license type, but differs in that it is not directly installed on the machine where the client is used.

The first time a user requests this license type, if available, it is granted to the client where it gets installed. For later uses, the client has its own Nodelocked license, and there is no need to request the license from the server.

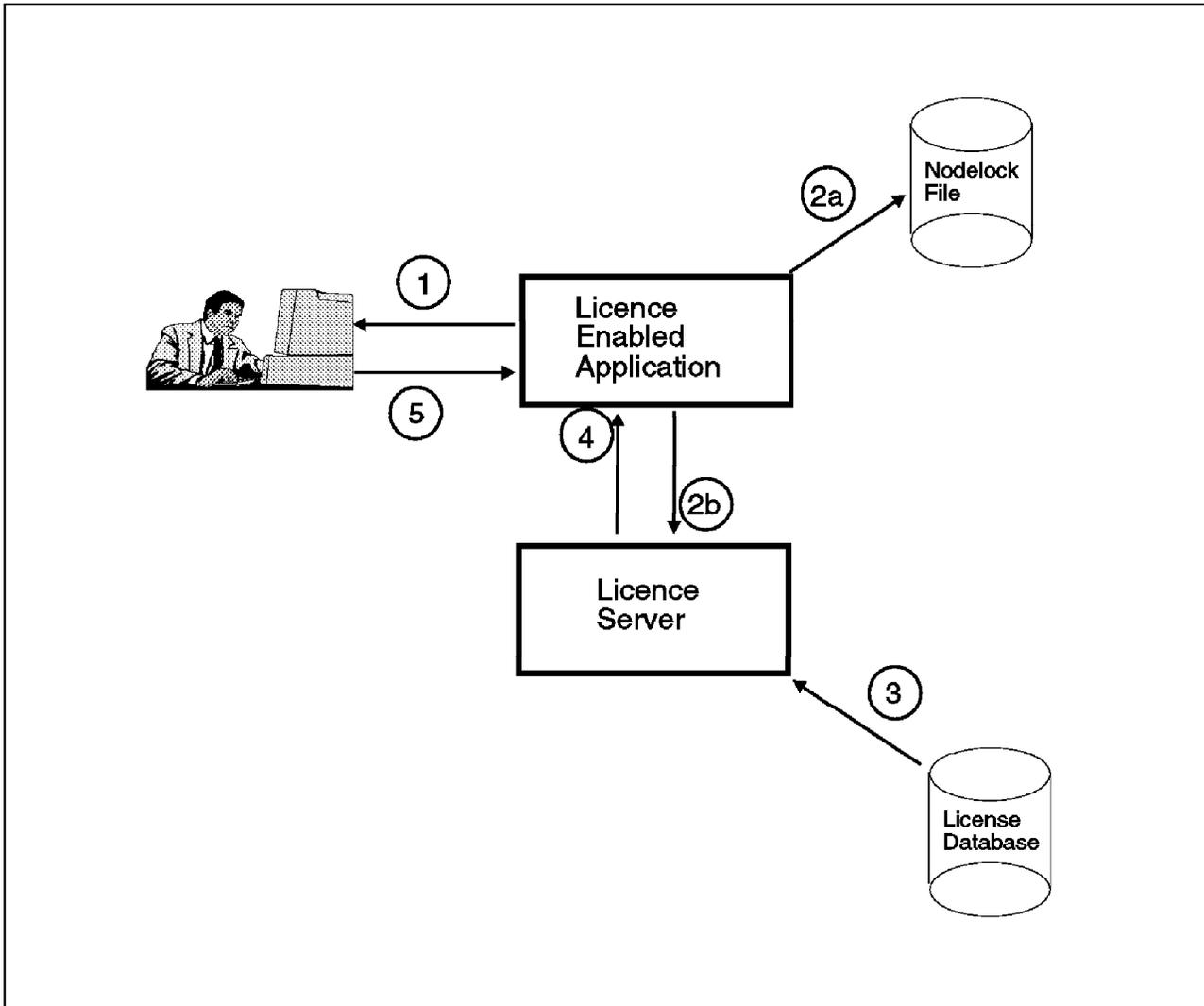


Figure 76. Using a Server-Based License

In Figure 76, the following steps are executed for a Nodelocked- licensed application:

1. The user invokes the application.
2. The application checks for the Nodelock license.
 - a. The application will first check locally to see if the Nodelock license file is available.
 - b. If the file is unavailable, the application requests the license from the license server.
3. The server checks the user rights and the license database.
4. The application runs, or returns information to user, depending on license request status.

In this model, when a user invokes a product licensed with a server-based license, the enabled product contacts the server and requests a license. If a valid license is available, the server grants the license and the product executes. As long as the product is running, that license remains unavailable. When the product stops, the license is returned to the server and again becomes available.

1.12.2 Security Levels

Using the above models, a vendor can impose one of the following predefined security levels:

- Restricted Registration Products (vendor-managed use)

This is the highest level of protection provided by SystemView License Management. With this level, you are technically bound to stay within the limits of the number of licenses you have purchased. When you purchase licenses, the vendor will ask you to supply the unique identifier of each machine where you intend to install the product licenses, the license type, and the number of licenses you want to make available. The vendor then uses this information to create a password that you use to install and activate the licenses that you have purchased. The passwords are contained in an enrolment certificate. The product cannot be used on another workstation.

- Unrestricted Registration Products (customer-managed use)

With this level, licenses are not associated with any particular workstation or server. Also the vendor does not set an upper limit on the number of licenses that you are entitled to use.

Typically, these products are shipped with a compound license password you use to install and distribute licenses to use the product. This compound password can contain an unlimited number of licenses and has an expiration date determined by the vendor. Vendors of unrestricted registration products may reserve the right to examine the log files on your server.

- Controlled Registration Products

With this intermediate level of security, a vendor may impose an upper limit to the number of licenses you initially distribute. As with unrestricted registration products, the licenses are contained within a single compound password from which you can create and distribute multiple licenses to use the product.

Before you use the product, you will need to contact the vendor. You must also exchange security information with the vendor before your compound password is activated. This allows the vendor to register customers. Once again, vendors may reserve the right to examine the log files on your server.

1.12.2.1 Summary of License Models

The following diagram summarizes the License Management models.

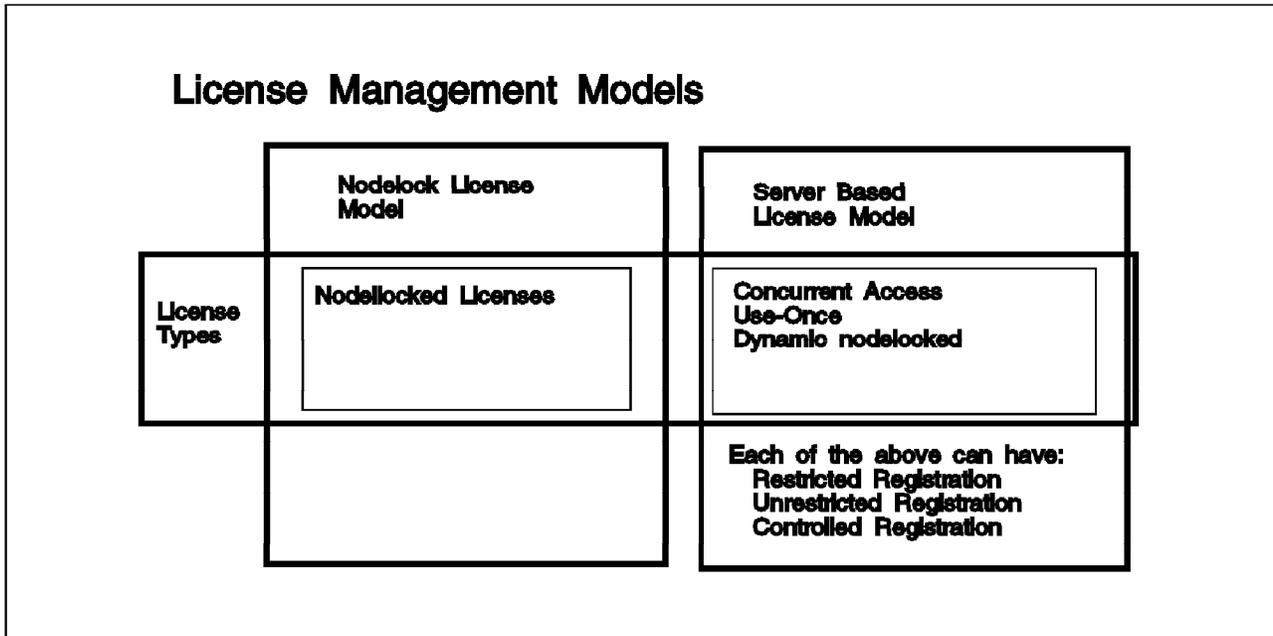


Figure 77. Summary of License Models

1.12.3 Planning for SystemView License Management

SystemView License Management makes use of the network computing system (NCS) which is a set of tools for heterogeneous distributed computing. The SystemView License Management or License Use Management Runtime component of either the server or the license client runs on top of the network computing kernel (NCK), that is included in the SystemView License Management components you install. In order for communication to occur between servers and between servers and clients, a number of processes are run. The processes in the NCK include:

- Remote Procedure Call (RPC) Runtime Library

This provides the calls that enable local programs to execute procedures on remote hosts. The RPC embedded in all license servers and enabled products provides a common mechanism to support the request and acquisition of licenses.

- Location Broker

This enables licensed products to locate license servers in the network. Two location brokers are run: a global location broker (GLB) and a local location broker (LLB).

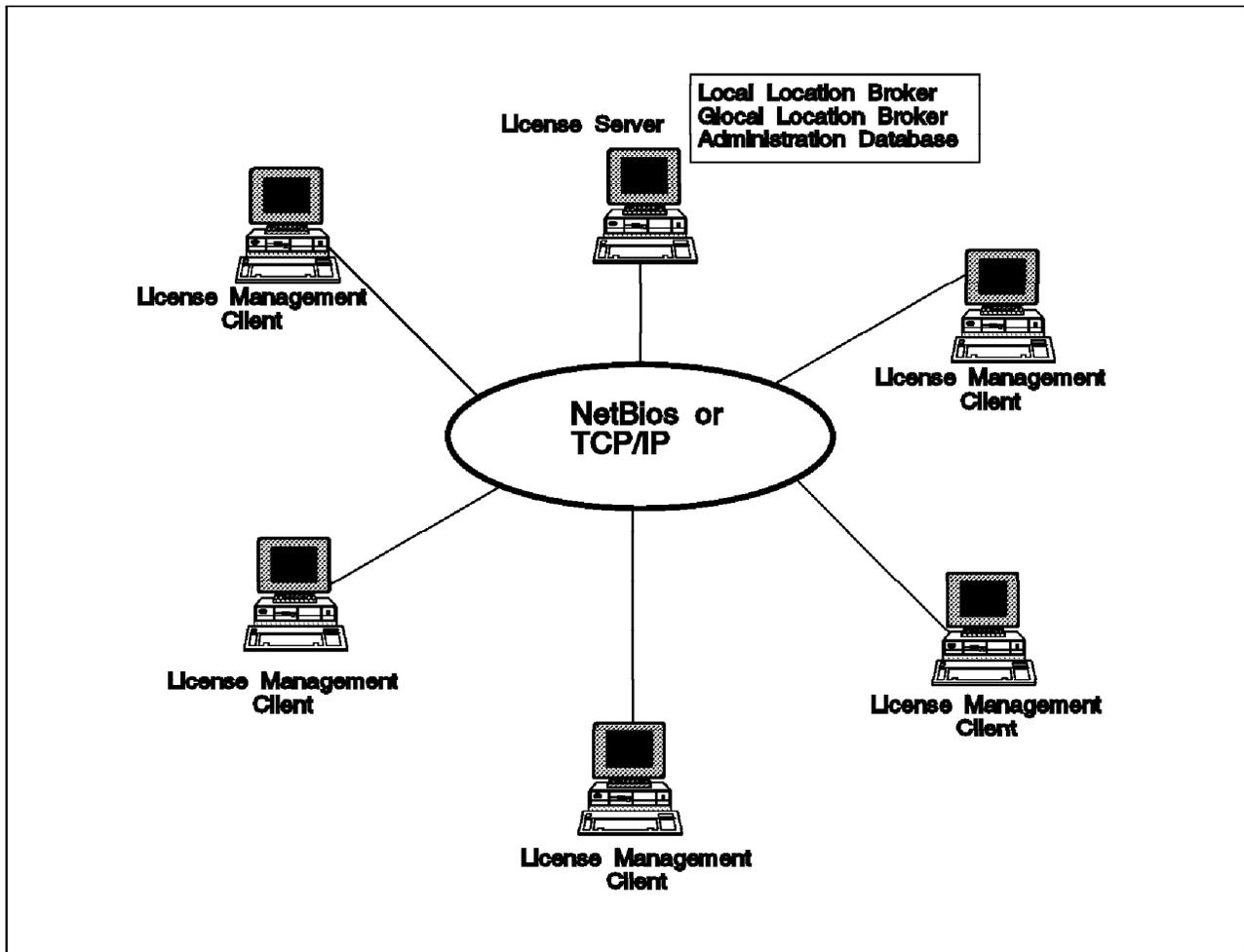


Figure 78. Simple NCS Cell - All Processes Run on One Server

Figure 78 shows a simple NCS cell where all the processes run on the same server. An NCS cell is a logical grouping of clients and servers. An enabled product that requires a license must have its request satisfied by a server in the same cell. Each client or server (known as nodes) cannot be in more than one cell. In Figure 78, all the license server components are running on one server. This is a simple, recommended configuration. Depending on the number of license servers and the number of clients, this could be installed over a number of machines.

The processes running on the server are:

- The Local location broker

This handles communication between the global location brokers and the actual servers. This must be run on each node that provides a license service. The process is called `i4l1bd`.
- The Global location broker

This process maintains a database of where all services reside on the network. At least one node in an NCS cell must run this service. You can replicate this process and have more than one running within a cell of the network. The process is called `i4g1bd`.
- The Administration database

This process is used for the administration of the license information database common to all servers in a cell. In order to keep the data consistent in the database, only one instance of this process will run in a cell at any one time. The process is called `i4gdb`.

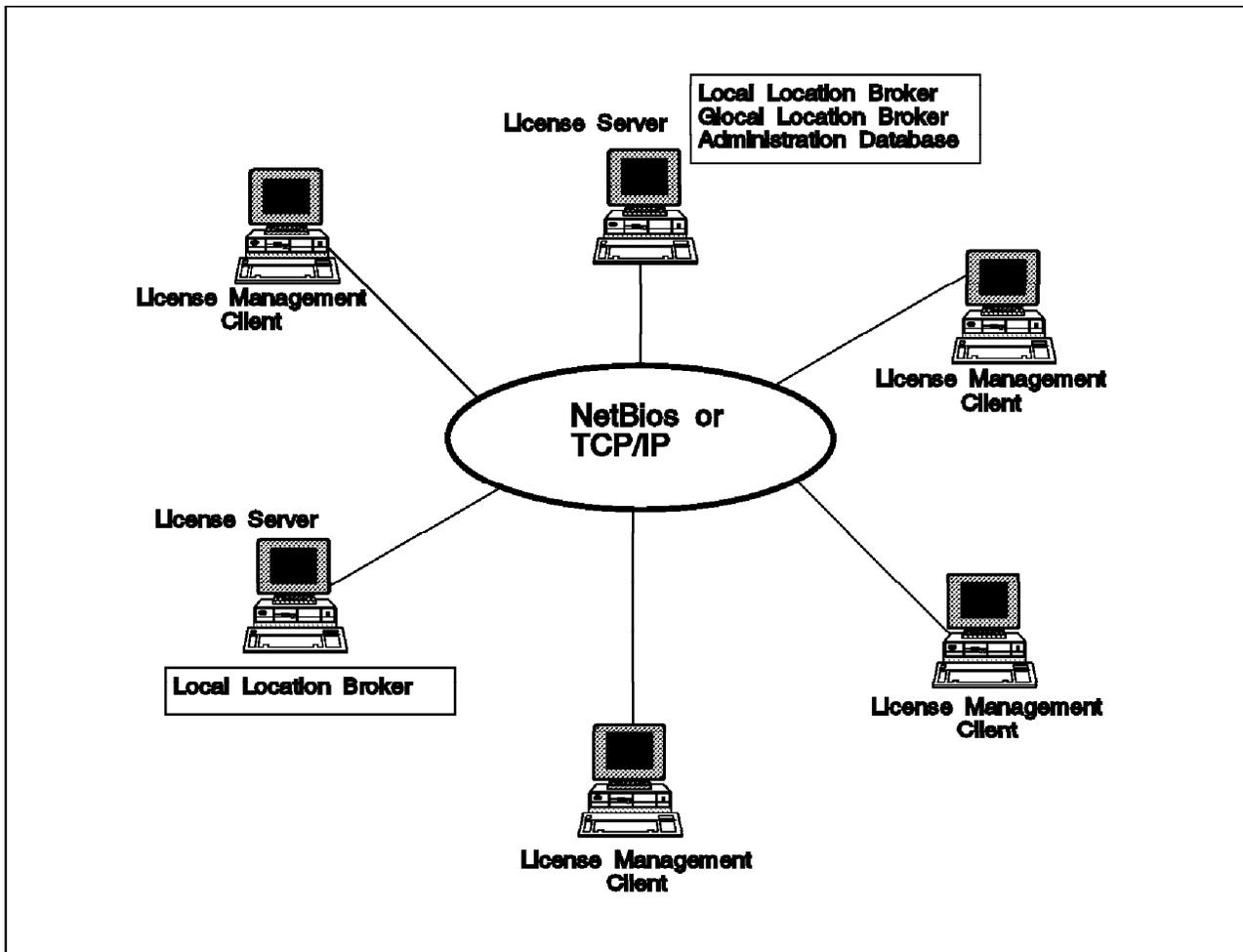


Figure 79. Cell with Two License Servers and Three Clients

Figure 79 shows a network with two license servers. Only one of them runs the GLB and administration database. The LLB is mandatory on all license servers.

1.13 Coexistence and Interoperability

SystemView in Warp Server is largely based on the NetFinity product. The architecture, transport, and graphical interface is very similar, if not exactly the same, for most of the SystemView services. In addition to the NetFinity services, a number of additional products have been integrated into SystemView in Warp Server, such as:

- Remote Workstation Control based on DCAF
- Software Distribution based on NetView Distribution Manager/6000, R.3.1.0
- License Management implemented using iForLS
- Application Sharing based on NetDoor/2

In many cases, you may already have one or more of the above products in production. Or, you may require the same function of the above products that have not been implemented in SystemView in Warp Server. In this section, we outline migration, coexistence, and interoperability of SystemView in Warp Server with the above products.

We define these three concepts as:

Concept	Definition
Migration	Capability to reuse customization done on existing products after the installation of SystemView in Warp Server
Coexistence	Installation and use of existing products and SystemView in Warp Server on the same workstation without interferences
Interoperability	Capability of SystemView in Warp Server to communicate and operate with existing products

1.13.1 NetFinity

SystemView in Warp Server uses many NetFinity functions, and the architecture of the underlying processes is much the same as NetFinity.

Interoperability: The SystemView in Warp Server core is essentially based on the NetFinity product and both products have full interoperability in a mixed environment. The following list describes the interoperability scenarios:

- A SystemView Manager can manage NetFinity and SystemView in Warp Server Clients sharing the same management group. In this environment, the:
 - Remote Workstation Control
 - Software Distribution
 - License Management

functions will *not* be supported on the NetFinity Clients because NetFinity does not support them.

- A NetFinity Manager can manage SystemView in Warp Server and NetFinity Clients sharing the same management group. In this environment, the:
 - Remote Workstation Control
 - Software Distribution
 - License Management

functions will *not* be supported because the NetFinity Manager doesn't support these functions.

- Both NetFinity managers and SystemView Managers can interoperate with each other.

Migration: When SystemView Manager is installed on a workstation where NetFinity Manager is already installed, all the customization (security, grouping, alerts, and so on) are migrated. The same happens when installing SystemView OS/2 Client on a workstation where NetFinity Services for OS/2 or for Windows are installed.

1.13.1.1 Coexistence

1. SystemView Manager *cannot* coexist in the same workstation where NetFinity Manager is installed (since the migration is performed).
2. The SystemView OS/2 and Windows clients cannot coexist with NetFinity Services OS/2 and Windows clients on the same workstation.

NetWare Server Management

Because NetFinity has a NetWare agent available, installing the NetFinity NetWare Client on the NetWare Server will allow management from a SystemView Manager. Not all management functions are available for NetWare Servers. This is due to a limitation in NetFinity NetWare Loadable Modules (NLMs).

1.13.2 License Management

The License Management feature of SystemView in Warp Server is provided by SystemView License Use Management Runtime for OS/2. The License Management is based on an existing iForLS product. Although this product is part of the SystemView in Warp Server installation, the base and graphical interfaces are independent of SystemView. Actually, no changes have been to the existing iForLS product.

As a result of this the question of migration, interoperability and coexistence are transparent.

1.13.3 NetView Distribution Manager/2 (NetView DM/2)

The Software Distribution functionality implemented in SystemView in Warp Server is based on a subset of NvDM/6000 R.3.1.0.

Note

SystemView in Warp Server Software Distribution is *not* based on NetView DM/2.

Many existing installations may be using the APPC support provided by NetView DM/2 to distribute software within enterprise networks. SystemView in Warp Server provides no such support. If you are using NetView DM/2 in this environment, be sure to understand this limitation before you move to SystemView in Warp Server

The following statements summarize the relationship between SystemView in Warp Server Software Distribution and NvDM/2:

Interoperability: There is *no* interoperability between SystemView in Warp Server Software Distribution and NetView DM/2. This means that SystemView in Warp Server Software Distribution Server cannot distribute software in NetView DM/2 clients and vice versa.

Software packages (change files) created with the existing elements of the NvDM Family *cannot* be reused/redistributed with SystemView in Warp Server.

1.13.3.1 Coexistence

Coexistence between SystemView in Warp Server Software Distribution and NetView DM/2 is possible in the following cases:

SystemView Manager (with the Software Distribution feature) can coexist with any of the following:

- NetView DM/2 CC Server
- NetView DM/2 CC Client for OS/2
- NetView DM/2 Remote Administrator

SystemView in Warp Server Client for OS/2 (with the Software Distribution feature) can coexist with any of the following:

- NetView DM/2 CC Server
- NetView DM/2 CC Client
- NetView DM/2 Remote Administrator

SystemView in Warp Server Client for Windows (with the Software Distribution feature) can coexist with:

- NetView DM/2 CC Client for Windows

All other coexistence environments are *not* supported. Namely, SystemView in Warp Server *cannot* coexist with:

- NvDM Agent for OS/2
- NvDM Agent for Windows (3.11)

1.13.3.2 Migration

No migration path is provided from any of the NetView DM family of products to SystemView in Warp Server for either the Manager or for the Client.

Recommendations

The following two scenarios could exist if you had the need to use NetView DM/2 for software distribution but still required some of the other OS/2 Warp Server functions:

1. If you need to install OS/2 Warp Server in an environment where machines are running NetView DM/2 and you need to distribute software on these machines, do not choose to install SystemView in Warp Server Software Distribution features during OS/2 Warp Server installation. You can install NetView DM/2 components in the OS/2 Warp Server machine instead, and maintain interoperability with the machines already installed in the network.

For this environment, it is recommended you use NetView DM/2 instead of SystemView in Warp Server Software Distribution.

Future direction about SystemView in Warp Server Software Distribution will assure interoperability with, and migration to, NetView DM/2; so, another choice could be to wait until the next release of SystemView in Warp Server will be announced.

2. If you have already installed OS/2 Warp Server with the SystemView in Warp Server Software Distribution feature, and you need to have the full functionality provided by the NetView DM/2 product, **you will need to remove the SystemView in Warp Server Software Distribution feature completely from this machine and install and configure NetView DM/2 instead.**

In the above process, your previous configuration of SystemView in Warp Server will be lost.

1.13.4 Distributed Console Access Facility (DCAF)

The Remote Workstation Control functionality implemented in SystemView in Warp Server is based on the IBM DCAF/2 (Distributed Console Access Facility) product. This product was adapted to coexist with the SystemView platform.

The DCAF product was tailored to use the NetFinity communication and graphical interface. Duplicate features, such as file transfer and security, were dropped from Remote Workstation Control, and the equivalent SystemView features can now be used.

See 1.10.14.1, "Comparison of SystemView Remote Workstation Control and DCAF Functions" on page 100 for further explanation.

1.13.4.1 Interoperability

Due to the changes in the communication interfaces, there is no interoperability between DCAF and Remote Workstation Control.

In other words:

- Remote Workstation Control of SystemView acting as a Controller cannot control a DCAF Target workstation (neither OS/2 nor DOS/Windows).
- Remote Workstation Control of SystemView cannot be a Target to a DCAF Controlling workstation.

1.13.4.2 Coexistence and Migration

Although interoperability is not possible between DCAF and SystemView in Warp Server machines, coexistence is. If you currently have DCAF implemented in your network, the following apply:

- A Remote Workstation Control implemented in SystemView Manager can coexist on the same machine with DCAF configured as a Controlling Workstation.
- A Remote Workstation Control implemented in SystemView Manager can coexist on the same machine with DCAF configured as a gateway.
- A Remote Workstation Control implemented in SystemView Manager cannot coexist on the same machine with DCAF configured as a Target Workstation.
- A Remote Workstation Control implemented in SystemView in Warp Server Client cannot coexist on the same machine with DCAF configured as a Target workstation.

The first possibility allows SystemView in Warp Server to integrate in a network with clients that have existing DCAF target installation and don't need to be migrated or converted to OS/2 Warp Server Clients containing SystemView Agents installed (see Figure 80).

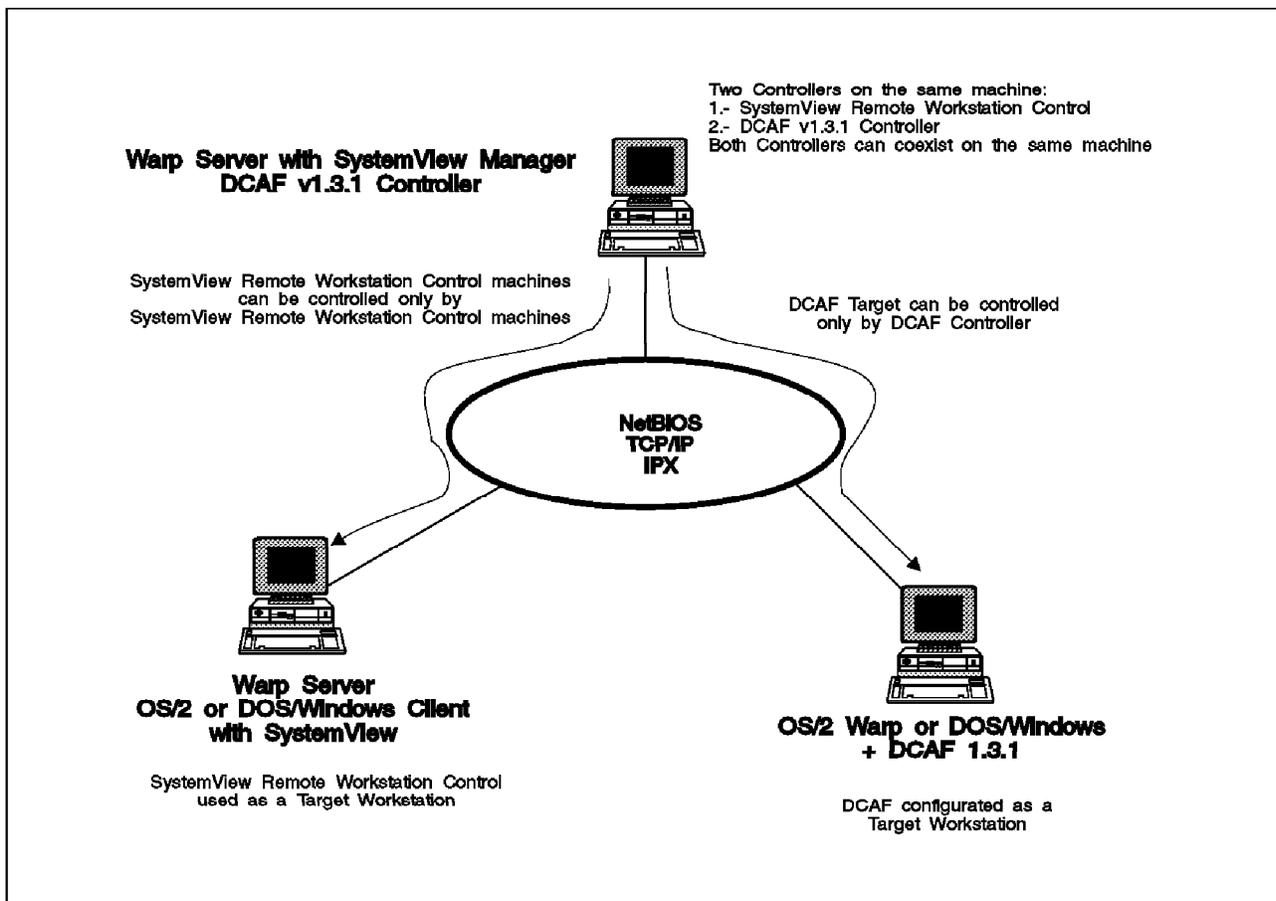


Figure 80. DCAF and SystemView: Rules for Coexistence and Interoperability

No migration is provided due to the fact that the customization options are limited and very different for both products.

1.14 Summary of the SystemView in Warp Server Functions

Function	Description	Administrator Only
Alert Manager	Receives and processes application-generated alerts.	No
Critical File Monitor	Warns whenever critical system files on the systems in the network are deleted or altered.	No
Power-On Error Detect	Detects POST errors or accesses the System Partition on Micro Channel machines.	No
Predictive Failure Analysis	Monitors all PFA-enabled disk drives installed on the system or on machines in the network.	No

Function	Description	Administrator Only
Remote System Management	Allows managing functions of remote machines in a LAN.	Yes
Remote Session	Establish a full-active, remote command-line window session with a remote client system.	Yes
Remote Workstation Control	Allows monitoring and control of a remote client system as if it was working at the remote client machine.	Yes
Screen View	Enables viewing a snapshot of any remote system's current screen display.	Yes
Serial Control	Enables you to use your system's modem to remotely access another SystemView system.	No
Event Scheduler	Automates many hardware and software systems-management tasks.	No
File Transfer	Allows transfer of files between two machines.	Yes

Function	Description	Administrator Only
CID Software Preparation	Create CID software objects for Software Distribution over the network.	No
Software Installation	Installs CID or non-CID software which has been defined into the catalog.	Yes
Software Preparation	Creates non-CID software objects for Software Distribution over the network.	No
Software Inventory	Allows software discovering over the network and keeps track of software products in a catalog.	Yes
Process Manager	Enables viewing detailed information about all processes currently active on the system and executes commands to halt and monitor individual processes.	No
License Manager	Allows license tracking and management for those applications which include such support	Yes

Function	Description	Administrator Only
System Information Tool	Gathers hardware and software configuration information.	No
ECC Memory Setup	Monitors and manages ECC memory.	No
RAID Manager	Gathers and shows information about the RAID adapter, physical drives in the RAID array, and the logical drives defined by the array.	No

<i>Table 9 (Page 2 of 2). Hardware Management and Inventory</i>		
Function	Description	Administrator Only
System Partition Access	Accesses a remote machine system partition (MCA machines) and allows multiple operations, such as backup partition, restore partition and so on.	No

<i>Table 10. Miscellaneous</i>		
Function	Description	Administrator Only
Security Manager	Implements security on SystemView in Warp Server machines in the network.	No
System Profile	Keeps track of various information on every machine in the network.	No
DMI	Provide or obtain hardware and software information, via GUI, in standardized format for systems which are DMI-compliant.	No

1.15 Related Publications

The following publications are suitable for further reading on the topics discussed in this chapter.

- *IBM NetFinity Manager for OS/2 Version 3.0*, S41H-6268
- *IBM NetFinity Services for OS/2 Version 3.0*, S41H-6270
- *SystemView Up and Running! V1.1*, SH19-4184
- *License Use Runtime Administrator's and User's Guide*, SH19-4187
- *Workgroup Management Using SystemView for OS/2*, SG24-2596

Chapter 2. Software Distribution Considerations

Over the past ten years, the number of workstations in organizations has grown steadily. During this time, operating systems and application software have become larger and more complex. In addition, many applications require data or configuration information to be supplied at installation time. All of the above factors make the task of installing and maintaining workstation software within such organizations very difficult. OS/2 and future IBM products have been designed with the above requirements in mind. IBM has designed a method to automate these processes by using redirected input/output on LAN-based client/server systems. It is called Configuration, Installation and Distribution (CID).

In this chapter we discuss the different methods available in OS/2 Warp Server of distributing software. This will include software that is CID-enabled as well as the distribution of non-CID enabled software.

2.1 Overview and Concepts

In this section, we describe some of the concepts that will be used in this chapter and provide an overview of the Software Distribution techniques that will be discussed. Since there are many Software Distribution techniques that are available we will attempt to draw attention to the differences.

In many cases, each environment has its own requirements. A decision to use one technique over the other will depend on the technique which works best in a given environment.

2.1.1 Installation Modes

The installation techniques used to install any kind of software product are classified into three modes:

2.1.1.1 Attended Installation

Attended installation is defined as that requiring a knowledgeable individual to be in attendance at the workstation where the software is being installed. This individual will need to respond to the various prompts that are displayed during the installation and configuration process.

2.1.1.2 Lightly Attended Installation

The phrase lightly attended installation refers to an environment where an individual must be present to initiate the installation process and potentially perform other simple or predefined tasks. However, this individual would require no specialized system knowledge.

2.1.1.3 Unattended Installation

An unattended installation has no requirement for an end user or administrator to be present at the time the system is being installed. In this instance, a Software Distribution Manager handles the initiation of the installation and everything else.

2.1.2 Configuration Installation and Distribution (CID)

The primary goals of CID are to:

- Eliminate human intervention at the Target workstation when preparing and executing the configuration, installation, migration, and maintenance processes that are necessary to operate this workstation.
- Enable the code executing at the Target workstation to perform all required configuration and installation tasks, including the integration of previous customizations.
- Provide the capability to centralize human intervention to an administrator at a central preparation site.

CID allows for products, including the OS/2 operating system and its subsystems, to be installed using a drive other than the A: drive. The Client, which is the system being installed, configured or maintained, accesses the product files through a redirected drive. This is called a Redirected Installation. The system that contains the source files (or installation diskette images) to be used during the installation or maintenance process is called the Code Server. Having the files on the Code Server saves the user from inserting the necessary diskettes manually. The source files for each product to be installed need to be placed on the server in a predefined format and structure. In most cases, utilities will be provided with applications to transfer the files from the product diskettes to the Code Server's product image directory.

CID also provides the capability to install different products without the user answering all the installation questions. At the same time, it provides the customization required by the end user for different installation needs. This is done through Response File support. Response Files are product-specific ASCII files that contain sequences of keyword-value pairs. They are interpreted during the installation and configuration process of a product. Simply put, they are responses to installation questions that a user installing the software would normally encounter.

CID conceptually defines six criteria for a software product to be CID enabled:

- Response Files
- Command-line driven execution
- Redirected drives
- Progress indication and logging facilities
- Standard return codes
- Transfer of product diskettes

With OS/2 Warp Server, there are three methods that can be used to distribute workstation software for CID and non-CID-enabled applications. They are described below:

2.1.3 Redirected Installation

When starting a normal software installation, a user inserts a diskette or CD-ROM into a drive and starts the installation program. The product will continue to install from the drive until all the diskettes required by the installation program have been processed or the installation ends.

A Redirected Installation defines the capability of the installation program to use a drive other than the diskette or CD-ROM drive, particularly the ability of the installation program to use a logical drive letter for installation.

Using this method, a workstation can access a server where the contents of the diskettes have been copied and perform the installation. This is the least complex method, but it requires the most interaction at the workstation.

Some of the ways of sharing a drive on a network are using:

- SRVIFS
- LAN Server
- Novell Netware
- TCP/IP - Network File System (NFS)

Clients that wish to use the remote drive provided by any of the services listed above would require the appropriate requester software. What follows is a brief explanation of each of the options:

2.1.3.1 SRVIFS

SRVIFS is a small NetBIOS-based file server and requester, that is shipped with OS/2 Warp Server. It is contained within the Multiprotocol Transport Services (MPTS) component. The main use of SRVIFS is to provide redirected file I/O support to enable client access to a Code Server. This is a subset of the function provided by the File and Print Services component of OS/2 Warp Server. Since SRVIFS requires a relatively small amount of disk space, it is particularly suited to being used during a boot diskette-based product installation.

2.1.3.2 LAN Server

Using the RIPL or File Services function provided with previous versions of LAN Server or OS/2 Warp Server, a network drive can be made available to client workstations.

2.1.3.3 Novell NetWare

A NetWare File Server network drive can be made available to client workstations. Client workstations will require the NetWare requester code.

2.1.3.4 TCP/IP NFS

TCP/IP provides a feature called Network File System (NFS) which can be used to share file resources across a network. Utilizing TCP/IP and NFS for redirected drive access provides a cross-systems environment. This allows different system types running operating systems other than OS/2 to take on the role of providing the remote drive. For example, the remote drive could be located on AIX, VM, MVS or OS/2. Client workstations or boot diskettes will require the appropriate requester software to connect to the remote drive.

TCP/IP NFS is not included in OS/2 Warp Server. It is available as a separate product.

2.1.4 CASSETUP

The Setup Utility (CASSETUP) for Redirected Installation is an applet that provides a Presentation Manager interface for installing and configuring a Code Server for Redirected Installation. The CASSETUP utility is contained in the MPTS component of OS/2 Warp Server. The Setup Utility also provides a user interface to assist administrators in creating bootable diskettes for use by clients to initialize and process Redirected Installation sessions.

The Setup Utility provides the following functions to assist administrators in preparing for Redirected Installation:

- A Presentation Manager interface for the installation and removal of Redirected Installation support. Redirected Installation support includes the LAN CID Utility and the Service Installable File System (SRVIFS).
- Installation and removal of diskette images for:
 - IBM OS/2 2.1 program
 - IBM OS/2 2.11 program
 - IBM OS/2 Warp Version 3.0 program
 - IBM OS/2 Warp Version 3.0 program with WIN-OS/2
 - IBM Service Paks
 - IBM Network Transport Services/2 (NTS/2) program
 - IBM LAN Server 4.0 program, including: IBM Multi-Protocol Transport Support (MPTS)
- A method of recording application diskette images that were previously loaded onto the server. This function allows you to use the utility with these images without having to reload them.
- Creation of a LAN CID Utility (CASPREP) and command file that will allow clients to install selected product images that were installed on the Code Server through the Setup Utility.
- Creating boot diskettes for use by clients to initialize and process Redirected Installation sessions.

2.1.5 SystemView in Warp Server Software Distribution

The SystemView in Warp Server Software Distribution is a client/server application. Any SystemView Manager can be set up as a Distribution Server (sometimes called the *change control server*, or *CC server*).

OS/2 and Windows-managed systems with the Software Distribution client component installed become distribution clients (called *change control clients* or *CC clients*) and can work in conjunction with the Distribution Server.

The Distribution Server maintains a database of client workstations, software objects, and the status of requests for software installation.

A catalog of software objects ready to be installed is maintained at the Distribution Server. Installation of the software at the Distribution Clients can happen in two ways:

- The administrator distributes software in the catalog to the Distribution Clients.

- End users at the Distribution Clients request installation of software that is in the catalog.

While it is possible to install more than one Distribution Server on a LAN, multiple Distribution Servers operate independently of one another.

2.1.6 Summary Table

Table 11 is a summary table which shows what type of software is installable using each of the methods described above. NetView Distribution Manager/2 is available as a separate product and is not included in OS/2 Warp Server.

		Operating System		CID Enabled Applications		Non-CID Enabled Applications	
		DOS/Win	OS/2	DOS/Win	OS/2	DOS/Win	OS/2
Redirected Drive	SRVIFS	No	Yes	No	Yes	No	Yes
	LAN Server	Yes	Yes (1)	Yes	Yes	Yes	Yes
	NetWare	Yes	Yes	Yes	Yes	Yes	Yes
	TCP/IP (NFS)	Yes	Yes	Yes	Yes	Yes	Yes
CASSETUP	SRVIFS	No	Yes	No	Yes	No	No
SystemView in Warp Server Software Distribution		No	No	Yes	Yes	Yes	Yes
NetView DM/2		Yes	Yes	Yes	Yes	Yes	Yes
Note:							
1. Except using LAN Server							

2.2 Using a Redirected Drive

In this section, we describe different methods to obtain one or more drives from a Code Server by using different transport protocols and utilities.

Once you have accessed a Code Server through its redirected drives, you'll be able to run multiple tasks, for example:

- Get access to the code files of the product that you want to install. Usually, the product can be installed from a single directory containing all the product files (for example, most Lotus products allow installation from a single directory in a CD-ROM or a hard drive).
- Get access to customized Response Files for the Client Installation (assuming that the product to be installed accepts a predefined response files as input).
- Write log files that allow error discovery and troubleshooting (if the product to be installed writes a log file as output).
- Execute some utility or application that may help us during the installation.
- Browse Code Server files and directories and make some changes on them.

Redirected drives have the following advantages:

- You can install an application easier and faster than using diskettes.
- Many people at the same time can install the same application.
- Configuration, installation and removal of necessary files that allow access to the Code Server is easy and is supported from many standard protocols.

2.2.1 Methods for Obtaining Redirected Drives

In this section, we briefly describe some methods based on standard transport protocols such as NetBIOS, TCP/IP and IPX, and provide some examples and implementations.

2.2.1.1 Use of SRVIFS

SRVIFS is a small application that implements a reduced NetBIOS client/server environment using OS/2 as its operating system.

We will describe step-by-step how to install and configure a server and how a client can be attached to the server resources.

1st. Step. Determine if NetBIOS is installed on your machine:

In most cases, NetBIOS is already configured and running in your machine because, for example, you have a LAN Requester or a LAN Server already installed.

If you don't have NetBIOS already installed in your client or server, you will need to install it.

Note: In most cases, you choose to install the SRVIFS server in a workstation that already has NetBIOS running. If you need to distribute, for example, communication software to OS/2 workstations that were not attached to the network previously, you will need to install the NetBIOS support. Another example is installing a product from scratch using boot diskettes, which offers two alternatives:

- Install the LAN Adapter and Protocol Support
- Install THINLAPS

In order to transfer NetBIOS and the network drivers onto the target system, the Code Server administrator uses a utility called THINLAPS. For detailed information about THINLAPS, please read the section 4.1.2.3 "THINLAPS" on page 92 of the redbook titled *OS/2 Installation Techniques: The CID Guide*, SG24-4295.

THINLAPS will install a seed LAN transport system on the target system and update the CONFIG.SYS accordingly.

A PROTOCOL.INI file is created on the target system based on a valid Network Information File (.NIF). The name of the .NIF is supplied as a parameter.

Let's go to the OS/2 Warp Server CD-ROM and start THINLAPS from the directory:

```
\CID\SERVER\MPTS
```

Now you need to run the THINLAPS program. For details about this program and syntax, please refer to Chapter 11, page 306 in the Redbook titled *OS/2 Installation Techniques: The CID Guide*, SG24-4295.

For example, you can type:

```
THINLAPS f:\cid\server\mpts e: ibmtok.nif
```

Where e: is the drive where THINLAPS will be installed, and f: is the CD-ROM drive.

The result is shown in Figure 81:

```
PKUNZIP (R) FAST! Extract Utility Ver 1.11-OS/2 Prot Mode 9-01-92
Copr. 1989-1992 PKWARE Inc. All Rights Reserved. PKUNZIP/h for help
PKUNZIP Reg. U.S. Pat. and Tm. Off. IBM LICENSED VERSION
Searching ZIP: f:\cid\server\mpts\IBMCOM\MACS\MACS.ZIP
Exploding: e:\ibmtok.nif
PKUNZIP (R) FAST! Extract Utility Ver 1.11-OS/2 Prot Mode 9-01-92
Copr. 1989-1992 PKWARE Inc. All Rights Reserved. PKUNZIP/h for help
PKUNZIP Reg. U.S. Pat. and Tm. Off. IBM LICENSED VERSION
Searching ZIP: f:\cid\server\mpts\IBMCOM\IBMCOM.ZIP
Exploding: e:\lt2.msg
PKUNZIP (R) FAST! Extract Utility Ver 1.11-OS/2 Prot Mode 9-01-92
Copr. 1989-1992 PKWARE Inc. All Rights Reserved. PKUNZIP/h for help
PKUNZIP Reg. U.S. Pat. and Tm. Off. IBM LICENSED VERSION
Searching ZIP: f:\cid\server\mpts\IBMCOM\MACS\MACS.ZIP
Exploding: e:\ibmtok.os2
PKUNZIP (R) FAST! Extract Utility Ver 1.11-OS/2 Prot Mode 9-01-92
Copr. 1989-1992 PKWARE Inc. All Rights Reserved. PKUNZIP/h for help
PKUNZIP Reg. U.S. Pat. and Tm. Off. IBM LICENSED VERSION
Searching ZIP: f:\cid\server\mpts\IBMCOM\IBMCOM.ZIP
Exploding: e:\PROTMAN.OS2
PKUNZIP (R) FAST! Extract Utility Ver 1.11-OS/2 Prot Mode 9-01-92
Copr. 1989-1992 PKWARE Inc. All Rights Reserved. PKUNZIP/h for help
PKUNZIP Reg. U.S. Pat. and Tm. Off. IBM LICENSED VERSION
Searching ZIP: f:\cid\server\mpts\IBMCOM\IBMCOM.ZIP
Exploding: e:\pro.msg
PKUNZIP (R) FAST! Extract Utility Ver 1.11-OS/2 Prot Mode 9-01-92
Copr. 1989-1992 PKWARE Inc. All Rights Reserved. PKUNZIP/h for help
PKUNZIP Reg. U.S. Pat. and Tm. Off. IBM LICENSED VERSION
Searching ZIP: f:\cid\server\mpts\IBMCOM\IBMCOM.ZIP
Exploding: e:\LANMSGDD.OS2
PKUNZIP (R) FAST! Extract Utility Ver 1.11-OS/2 Prot Mode 9-01-92
Copr. 1989-1992 PKWARE Inc. All Rights Reserved. PKUNZIP/h for help
PKUNZIP Reg. U.S. Pat. and Tm. Off. IBM LICENSED VERSION
Searching ZIP: f:\cid\server\mpts\IBMCOM\IBMCOM.ZIP
Exploding: e:\LANMSGEX.EXE
PKUNZIP (R) FAST! Extract Utility Ver 1.11-OS/2 Prot Mode 9-01-92
Copr. 1989-1992 PKWARE Inc. All Rights Reserved. PKUNZIP/h for help
PKUNZIP Reg. U.S. Pat. and Tm. Off. IBM LICENSED VERSION
Searching ZIP: f:\cid\server\mpts\IBMCOM\DLL\DLL.ZIP
Exploding: e:\acsnetb.dll
PKUNZIP (R) FAST! Extract Utility Ver 1.11-OS/2 Prot Mode 9-01-92
Copr. 1989-1992 PKWARE Inc. All Rights Reserved. PKUNZIP/h for help
PKUNZIP Reg. U.S. Pat. and Tm. Off. IBM LICENSED VERSION
Searching ZIP: f:\cid\server\mpts\IBMCOM\PROTOCOL\PROTOCOL.ZIP
Exploding: e:\netbeui.nif
PKUNZIP (R) FAST! Extract Utility Ver 1.11-OS/2 Prot Mode 9-01-92
Copr. 1989-1992 PKWARE Inc. All Rights Reserved. PKUNZIP/h for help
PKUNZIP Reg. U.S. Pat. and Tm. Off. IBM LICENSED VERSION
Searching ZIP: f:\cid\server\mpts\IBMCOM\PROTOCOL\PROTOCOL.ZIP
Exploding: e:\NETBEUI.OS2
```

Figure 81 (Part 1 of 2). Output of THINLAPS execution

```

PKUNZIP (R) FAST! Extract Utility Ver 1.11-OS/2 Prot Mode 9-01-92
Copr. 1989-1992 PKWARE Inc. All Rights Reserved. PKUNZIP/h for help
PKUNZIP Reg. U.S. Pat. and Tm. Off. IBM LICENSED VERSION
Searching ZIP: f:/cid/server/mpts/IBMCOM/PROTOCOL/PROTOCOL.ZIP
Exploding: e:/NetBIOS.OS2
PKUNZIP (R) FAST! Extract Utility Ver 1.11-OS/2 Prot Mode 9-01-92
Copr. 1989-1992 PKWARE Inc. All Rights Reserved. PKUNZIP/h for help
PKUNZIP Reg. U.S. Pat. and Tm. Off. IBM LICENSED VERSION
Searching ZIP: f:/cid/server/mpts/IBMCOM/PROTOCOL/PROTOCOL.ZIP
Exploding: e:/NETBIND.EXE
THINLAPS completed successfully.

```

Figure 81 (Part 2 of 2). Output of THINLAPS execution

Transport protocol support files are copied in the root of the drive selected for THINLAPS installation. You can see these files emphasized in Figure 82.

```

The volume label in drive E is OS2.
The Volume Serial Number is A6D4:0814.
Directory of E:\

10-10-95  7:27p  <DIR>      0  .
10-10-95  7:27p  <DIR>      0  ..
9-11-95  2:35p  3349      0  acsnetb.dll
9-19-95  11:44a    433      0  AUTOEXEC.BAT
10-10-95  7:27p  3433     42  CONFIG.SYS
10-10-95  6:48p  <DIR>    869  Desktop
9-19-95  11:45a    1396     0  IBMLVL.INI
6-01-95  1:00p  17736     0  ibmtok.os2
9-19-95  10:08a  <DIR>      0  IBMVESA
9-11-95  2:45p  3572      0  LANMSGDD.OS2
9-11-95  2:45p  2580      0  LANMSGDL.DLL
9-11-95  2:45p  1099      0  LANMSGEX.EXE
9-11-95  2:45p  12814     0  LT0.MSG
9-11-95  2:43p  2860      0  lt2.msg
9-19-95  10:22a  <DIR>    331  Maintenance Desktop
10-10-95  6:48p  <DIR>      0  MMOS2
9-11-95  2:34p  114532     0  NETBEUI.OS2
9-11-95  2:44p  13657     0  NETBIND.EXE
9-11-95  2:35p  15892     0  NetBIOS.OS2
9-19-95  11:45a  <DIR>      0  NETWARE
10-05-95  11:36a  <DIR>    296  Nowhere
9-19-95  11:35a  <DIR>    296  Nowhere1
10-10-95  6:49p  <DIR>      0  OS2
9-11-95  2:44p  2234      0  pro.msg
9-11-95  2:44p  22276     0  PROTMAN.OS2
10-10-95  7:27p    533      0  PROTOCOL.INI
9-19-95  10:06a  <DIR>      0  PSFONTS
2-05-95  11:03p  26704     0  README
9-19-95  11:34a  <DIR>      0  SPOOL
10-10-95  4:29p  <DIR>      0  SRVIFS
10-10-95  4:29p    150     0  startup.cmd
9-19-95  10:08a  <DIR>      0  XVA$DMQS

```

Figure 82. THINLAPS Files Are Copied into the Root

The THINLAPS installation adds information in the CONFIG.SYS file (see Figure 83 on page 131).

```

.
.
.
.
SET PATH= .....;E:\SRVIFS;
SET DPATH= .....;E:\SRVIFS;
.
.
.
.
rem *** Start of ThinLAPS additions ***
device = lanmsgdd.os2
device = protman.os2
device = netbeui.os2
device = netbios.os2
DEVICE=IBMTOK.OS2
call = netbind.exe
run = lanmsgex.exe
rem *** End of ThinLAPS additions ***
.
.
.

```

Figure 83. THINLAPS Changes to CONFIG.SYS

It also creates a PROTOCOL.INI file on the drive selected for installation (see Figure 84).

```

[protman]
  drivename = protman$

[netbeui_nif]
  drivename = netbeui$
  bindings = mac

; If running on an ethernet network, remove the semicolon from the
; "ETHERAND_TYPE =" statement to change the protocol convention from
; IEEE 802.3 to DIX 2.0.
; ETHERAND_TYPE = "D"

[mac]
  drivename = IBMTOK$
;  EARLYRELEASE
;  ADAPTER = ""
;  NETADDRESS = ""
;  RAM = 0x
  MAXTRANSMITS = 6
  RECVBUFS = 2
  RECVBUFSIZE = 256
  XMITBUFS = 1
;  XMITBUFSIZE =
;  ENABLEBRIDGE
;  BRIDGERAM =

```

Figure 84. THINLAPS PROTOCOL.INI File Creation

2nd. Step. Installing a SRVIFS Server

1. **Where do you find the necessary files in the OS/2 Warp Server CD-ROM?** In the directory \CID\SRVIFS, you will find all necessary files for installing and configuring a SRVIFS server. In fact, you will find the following files (see Figure 85 on page 132):

```

The volume label in drive F is WARP SERVER.
The Volume Serial Number is C15E:0D30.
Directory of F:\CID\SRVIFS

9-18-95 12:00p <DIR> 0 .
9-18-95 12:00p <DIR> 0 ..
9-11-95 2:48p 28972 0 IFSDEL.EXE
9-11-95 2:37p 50640 0 SERVICE.EXE
9-11-95 2:37p 14008 0 SRVATTCH.EXE
9-11-95 2:37p 1076 0 SRVIFS.SYS
9-11-95 2:37p 24692 0 SRVIFSC.IFS
8-21-95 8:22p 169 0 SYSLEVEL.SIF
9-11-95 2:48p 32342 0 THINIFS.EXE
9-11-95 2:48p 43268 0 THINSRV.EXE
9-11-95 2:48p 8511 0 XI1.MSG
9-11-95 2:48p 28894 0 XI1H.MSG
12 file(s) 232572 bytes used
0 bytes free

```

Figure 85. Directory \CID\SRVIFS. Required files for SRVIFS server

2. Configuring the SRVIFS server Response File

Now you need to configure a SRVIFS server Response File.

OS/2 Warp Server provides a template of a SRVIFS Response File that you can modify according to your needs.

In fact, unzipping the file:

```
\CID\SERVER\IBMLS\IBM500N5\SAMPLE\SAMPLE.ZIP
```

we obtain the following files (see Figure 86):

```

The volume label in drive C is OS2.
The Volume Serial Number is 1F24:9195.
Directory of C:\SAMPLE

. <DIR> 10-10-95 3:28p
.. <DIR> 10-10-95 3:28p
LAPSRSP RSP 285 5-09-95 4:29p
LAPSRSP0 RSP 412 5-09-95 3:48p
LAPSRSP1 RSP 1028 5-09-95 3:48p
LAPSRSP2 RSP 939 5-09-95 3:48p
LAPSRSP3 RSP 1238 5-09-95 3:48p
LAPSRSP4 RSP 1617 5-09-95 3:48p
LAPSRSP5 RSP 454 5-09-95 3:48p
LAPSRSP6 RSP 903 5-09-95 3:48p
LAPSRSP7 RSP 1202 5-09-95 3:48p
LAPSRSP8 RSP 316 5-09-95 3:48p
LAPSRSP9 RSP 297 5-09-95 3:48p
MPTSRSP1 RSP 2530 5-09-95 4:29p
MPTSRSP2 RSP 1064 5-09-95 4:29p
MPTSRSP3 RSP 3070 5-09-95 4:29p
SERVICE INI 359 5-09-95 3:50p
SERVICE LST 431 5-09-95 3:50p
18 file(s) 16145 bytes used
30912512 bytes free

```

Figure 86. Sample SRVIFS Response Files

The file called SERVICE.INI is a sample of a Response File for the SRVIFS server. The file called SERVICE.LST is a sample of the authorization list file for the SERVICE.INI file. A configured example of SERVICE.INI is shown in Figure 87 on page 133. In Figure 88 on page 133, you can see an example of SERVICE.LST.

```

;
!
@
#
Adapter      = 0
MaxClients   = 5
MaxFiles     = 102
Name         = ENRIQUE
Groupname    = No
ClientWorkers = 6
Authlist     = E:\SRVIFS\SERVICE.LST
;
Path         = E:\OS2
perclient    = No
PermitWrite  = Yes
;
alias= readonly,single,cid,c:\cid
alias= readonly,single,img,c:\cid\img
alias= readwrite,perclient,csd,c:\cid\csd

```

Figure 87. SERVICE.INI Sample File

Note: The server name (srvname) must be a unique name not used by other NetBIOS applications, such as LAN Server/Requester, and must not exceed eight bytes (characters or numbers).

In the above example, the authorization list file is located in the E:\SRVIFS directory, and E:\OS2 is the fully qualified path that will appear as the root of the redirected drive to the SRVIFS redirector's.

We have configured three different aliases: CID, IMG and CSD, corresponding to three different directories in the C drive of the Code Server.

```

* This is a sample authorization list file for service.ini file
* This file should have one requester name per line. The requester
* name should be 1-8 characters long followed by at least 1 space.
* For each requester, the name may optionally be followed by a
* Universal Administered address of the LAN adapter. This optional
* feature provides an additional layer of security.
*
client1
client2
client3.10005a882805

```

Figure 88. SERVICE.LST Example

If you need more information about each keyword of the SERVICE.INI file, please see Appendix L for the SERVICE.INI file keywords on page 571 in the redbook titled *OS/2 Installation Techniques: The CID Guide*, SG24-4295.

3. Installing the SRVIFS server

The next step is to create a directory in the drive where the SRVIFS server is installed. We can call it, for example, SRVIFS:

```
E:\SRVIFS
```

Now, you need to run the THINSRV program. For details about this program and syntax, please see Chapter 11, page 302, of the redbook titled *OS/2 Installation Techniques: The CID Guide*, SG24-4295.

For example, type:

```
THINSRV /R:e:\srvifs\service.ini /T:e:\srvifs /S:f:\cid\srvifs /TU:e:\srvifs\thinsrv.log
```

After completion, the following output is displayed:

```
[F:\CID\SRVIFS]thinsrv /R:E:\SRVIFS\SERVICE.INI /T:E:\SRVIFS /S:F:\CID
/TU:E:\ /L1:E:\SRVIFS\THINSRV.LOG
THINSRV completed successfully.
```

— ALIAS statements —

THINSRV checks the content of SERVICE.INI, and if it finds some inconsistency, it will fail. For example, if you don't create physically on the Code Server the directories specified in the ALIAS statements in SERVICE.INI, THINSRV will show the following error message:

```
[F:\CID\SRVIFS]thinsrv /R:E:\SRVIFS\SERVICE.INI /T:E:\SRVIFS
/S:F:\CID\SRVIFS /TU:E:\ /L1:E:\SRVIFS\THINSRV.LOG
XI10021: Invalid value for "PATH =" statement or path on "ALIAS =
" statement on line 17 in Response File.
XI10021: Invalid value for "PATH =" statement or path on "ALIAS =
" statement on line 18 in Response File.
XI10021: Invalid value for "PATH =" statement or path on "ALIAS =
" statement on line 19 in Response File.
XI10042: THINSRV did not complete successfully.

[F:\CID\SRVIFS]
```

Once finished, THINSRV produces the following changes on the system:

- a. SRVIFS is installed on directory E:\SRVIFS
- b. The line:

```
START E:\SRVIFS\SERVICE.EXE /INI=SERVICE
```

was added in the file STARTUP.CMD.

- c. PATH and DPATH statements are updated in CONFIG.SYS

```
PATH= ..... ;E:\SRVIFS;
DPATH= ..... ;E:\SRVIFS;
```

Now, the Code Server is ready to be used.

After rebooting the server, the SERVICE.EXE will start automatically.

Note: If you need some suggestions on how to install the remote installation tree in the Code Server, please see the section 2.3.1, "Setting Up a Code Server" on page 145.

3rd. Step. Installing the SRVIFS client: The SRVIFS client can run in:

- A machine with OS/2 already installed that needs to be connected with the SRVIFS Code Server
- An OS/2 boot diskette needed to install an operating system, CSD or application that requires installation from boot

The same considerations about protocol support (see "1st. Step. Determine if NetBIOS is installed on your machine" on page 128) are valid for the SRVIFS client.

If you need to create OS/2 Boot Diskettes: If you are configuring the LAN CID Utility (LCU) redirector on a target system, you must skip this section and jump to the section "Attachment to the Code Server using THINIFS" on page 135.

If you need to create OS/2 boot diskettes, you will need to use the SEDISK utility.

Note: The SEDISK utility is documented in section 15.1.2, page 379, of the redbook titled *OS/2 Installation Techniques: The CID Guide*, SG24-4295.

SEDISK is located in the directory \CID\EXE\OS2 in the OS/2 Warp Server CD-ROM.

SEDISK also needs access to the OS/2 installation tree on the OS/2 Warp Server CD-ROM. You can find this tree under the \OS2IMAGE directory.

So, being in the \CID\EXE\OS2 directory, execute the following command:

```
SEDISK /S:f:\os2image /T:a:
```

and you'll obtain the following output:

```
Insert a formatted diskette into drive A:.  
Press <Enter> to continue.  
All data on the diskette will be erased.  
Do you want to continue? (Y/N)  
Deleting all files on A:, please wait.  
Copying files, please wait.
```

```
Insert a formatted diskette into drive A:.  
Press <Enter> to continue.  
All data on the diskette will be erased.  
Do you want to continue? (Y/N)  
Deleting all files on A:, please wait.  
Copying files, please wait.  
F:\OS2IMAGE\DISK_4\BUNDLE  
- A:\REFPART.SYS  
    0 file(s) copied.  
    1 file(s) unpacked.
```

SEDISK has completed successfully.

Attachment to the Code Server using THINIFS: THINIFS is a utility that transfers the SRVIFS redirector code to the target system (another machine or a boot diskette).

Note: If you need a detailed explanation about this utility, please refer to 4.1.3.1 "THINIFS" on page 94 of the *OS/2 Installation Techniques: The CID Guide*, SG24-4295, and also to section 11.6.3 "Install LCU Redirector (THINIFS)" of the same book.

THINIFS is located in the directory \CID\SRVIFS of the OS/2 Warp Server CD-ROM (see Figure 85 on page 132).

Because you don't have the CD-ROM drive attached on the target machine (the CD-ROM is attached on the Code Server), you cannot install the LCU redirector on the target machine using the network.

If you need to install the LCU redirector in the hard disk of the target machine, you must:

1. At the Code Server, run THINIFS and configure the OS/2 boot diskette, disk 1, and in a second instance,
2. Apply the modifications that THINIFS performed to the OS/2 boot diskette, disk 1, to the fixed disk of the target system, also copying the LCU redirector files.


```
.
.
.
.
rem *** Start of ThinLAPS additions ***
device = lanmsgdd.os2
device = protman.os2
device = netbeui.os2
device = netbios.os2
device = IBMTOK.OS2
call = netbind.exe
run = lanmsgex.exe
rem *** End of ThinLAPS additions ***
.
.
.
.
.
DEVICE=a:\SRVIFS.SYS
IFS=a:\SRVIFSC.IFS client1
CALL=a:\SRVATTCH.EXE x: \\ENRIQUE\cid
.
.
.
.
```

Figure 90. THINIFS Boot Diskette CONFIG.SYS Changes

Note:

1. THINIFS can be executed several times, one time for every redirected drive you need to get from the Code Server.
2. The OS/2 boot diskette, disk 1, is the second of the OS/2 boot diskettes. The first one is called OS/2 Boot Installation Diskette and is not modified by THINIFS.

Finally, if you need to install the LCU redirector in a Target machine with OS/2 installed, you need to copy the files added by THINLAPS and THINIFS to the diskette along with the information in CONFIG.SYS.

2.2.1.2 Using LAN Server

If you have already installed LAN Server contained in OS/2 Warp Server in your machine, you probably don't need to install a SRVIFS server to implement a redirected drive to a Code Server.

In fact, you must configure the LAN Server resources (for more information, see the redbook titled *Inside OS/2 Warp Server, Volume 1*, SG24-4602) according to the applications that are going to be installed from the Code Server.

Regarding the Server:

1. Create the Code Server Tree.
Note: If you need some suggestions of how to install the remote installation tree in the Code Server, please see section 2.3.1, "Setting Up a Code Server" on page 145.
2. Create user IDs and passwords.
3. Create aliases.
4. Assign logical drives and aliases for the users to these resources.

Regarding the Client: The client can be DOS or OS/2.

- DOS Client: it must run DLS (DOS LAN Services)
- OS/2 Client: it must run OS/2 LAN Requester + LAPS (LAN Adapter and Protocol Support) with NetBIOS configured.

This method is adequate for installing applications. It is not recommended for installing operating systems or applications that require booting from diskettes because DLS and OS/2 LAN Requester are difficult to install and run from diskettes.

However, you will see in the example of 2.2.2.1, "Installation of DOS, Windows and DOS LAN Services Using LAN Server 5.0" on page 143 how to configure a DOS boot diskette that allows installation of DOS 7.00 + Windows + DLS on a pristine system.

2.2.1.3 SRVIFS and LAN Server Comparison

At this point, we can compare the SRVIFS method with the LAN Server method.

SRVIFS	LAN Server
Normally requires a manual installation (unless you have installed and are using CASSETUP or other utilities that automatically installs the SRVIFS support)	Easy to install and configure.
Requires minimal DASD space and memory	Requires considerable DASD space and memory.
No support for DOS clients.	Supports DOS client.
Easy to install on client boot diskettes.	Difficult installation on client boot diskettes.

2.2.1.4 Using TCP/IP NFS Server Functions



Start NFS

In this section, we will explain how to use a TCP/IP server as a Code Server using the Network File System (NFS) feature of TCP/IP for OS/2 and redirected drives.

Use of this facility allows a workstation to be installed from the following systems that provide NFS server capability, like:

- OS/2 systems (TCP/IP for OS/2 + NFS feature)
- AIX systems (IBM RISC System/6000)
- UNIX systems which support an NFS server capability

Installation of the TCP/IP Code Server

Note: In all cases, we assume that we have installed OS/2 Warp Server in the Code Server.

1. Install Warp Server choosing the TCP/IP component and OS/2 with REXX support.
2. Install the TCP/IP for OS/2 2.0 NFS Kit. Choose:

- NFS Kit
- NFS TCP/IP CID Install

See Figure 91.

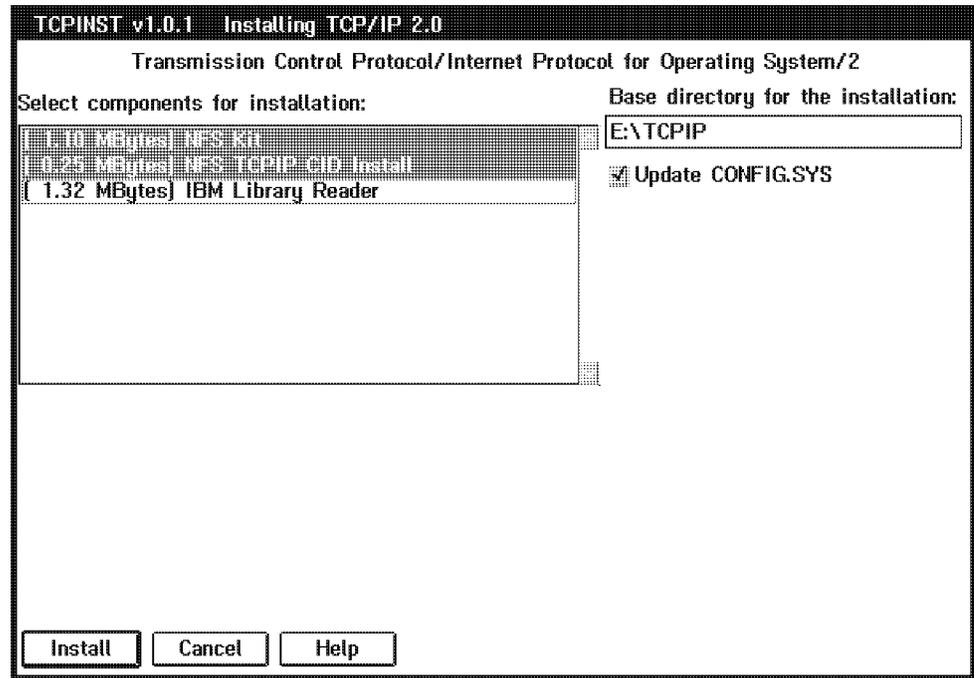


Figure 91. Installing TCP/IP for OS/2 NFS Kit

3. Install the latest NFS fixpak. In our example, we install fix UN57064 for NFS Kit. Choose:

- CSD UN57064 for NFS Kit
- CSD UN57064 for NFS CID Install

See Figure 92 on page 140.

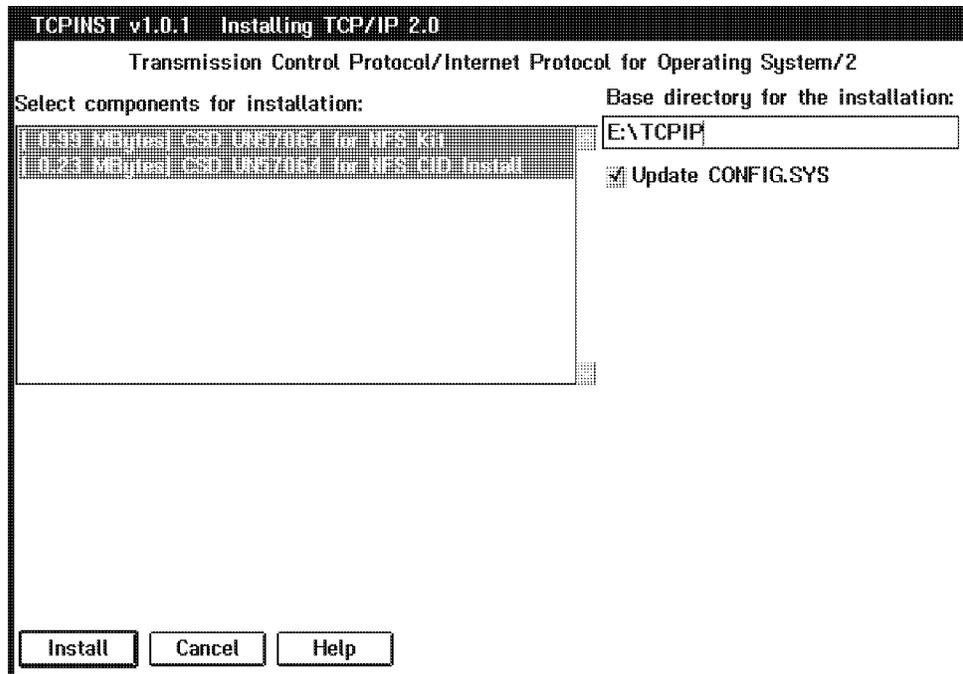


Figure 92. Installation of TCP/IP for OS/2 NFS CSD Kit

4. Create the Tree Directory structure

Note: If you need some suggestions of how to install the remote installation tree in the Code Server, please see the section 2.3.1, "Setting Up a Code Server" on page 145.

5. Configure the TCP/IP Code Server with the following parameters:

- Code Server IP Address
- Code Server Hostname
- Subnet Mask, if necessary
- Routing information, if necessary
- Configure Name Resolution Services (file HOSTS), if necessary
- Name Server Addresses (the TCP/IP network has to have a configured Name Server somewhere)

Note: In the OS/2 environment, some functions require using names instead of IP addresses. Mounting an NFS drive requires the use of names, and for this reason, the Name Server address *must be* configured in the TCP/IP Code Server configuration.

- Local domain name or LAN Domain searchlist, if necessary
- Configure the Mountable Client Directories EXPORTS file:
 - Selecting directories
 - Enabling clients
 - Selecting profiles
- User ID and a group ID for the client
- Select NFSD and PORTMAP services to start in automatic mode or start **NFSD.EXE** and **PORTMAP** from the command line

Note: For information about how to configure these parameters, see page 246, "Expanding OS/2 Warp Server TCP/IP Capabilities" of the redbook titled *Inside OS/2 Warp Server, Volume 1*, SG24-4602.

6. Reboot the machine.

Installing the TCP/IP NFS Client

1. If the client machine is another OS/2 machine, then:
 - Repeat steps 1, 2 and 3 for the installation of the Code Server.
 - Skip step 4.
 - Do step 5 (Configuration of the TCP/IP NFS Client) considering:
 - IP Address, Hostname must be different than the Code Server (the Hostname must be the same one configured in the EXPORTS file)
 - You don't have to configure the EXPORTS file in the client machine.
 - To automate the mounting operation, you can configure the Mount/Mvslogin Startup Commands FSTAB option in the NFS Configuration Section.

Mount Command Syntax

```
NFS client mount command:
Function: This command allows one to attach an NFS server
          disk to the local file system.
Syntax:  mount <options> <drive> <hostname>:<mountpoint>
          <drive>           Local drive.
          <hostname>       Host to attach to.
          <mountpoint>    Directory to attach to and any server
                           specific parameters.
Options: -a               Set archive option.
          -c               Set CR/LF translation option.
          -s               Set lock option.
          -lUSERNAME      Set username.
          -pPASSWORD      Set password.
          -u[UID]         Set UID.
          -g[GID]         Set GID.
          -v[PASSWORD]    Set VM-style password.
Examples: mount z: catch22:/homes/catch22
          mount -u312 -g1 k aix03:/home/andrew
          mount -v v vm1:myid.191,ro
          mount -c -lbill -psecret m: jupiter:/usr/bill
```

2. If the client machine is a DOS machine, you will need to install and configure TCP/IP for DOS/Windows and NFS.
3. If you need to install from OS/2 boot diskettes, you need to run a file called MAKENFSU.CMD.

Note: Once you install TCP/IP NFS for OS/2 2.0 (CID Support), you will find a file called MAKENFS.CMD in the directory where you decided to install NFS (usually \TCPIP). This file is not updated for the version of TCP/IP and MPTS contained in OS/2 Warp Server. In fact, in this new version, the TCP/IP protocol stack was integrated into MPTS. As a result, changes need to be made to this command file. We have adapted this file to the new version of MPTS. Now this file is called MAKENFSU.CMD.

MAKENFSU prompts you for the following information:

- The drive where you have installed MPTS.

Attention—LAN Adapter

PROTOCOL.INI is installed on the diskette which is based on your PROTOCOL.INI. It assumes that you want to use the same type of network adapter and address. You should ensure that PROTOCOL.INI is compatible with the workstations on which you plan to use the bootable installation diskettes. You should also ensure that you use a universal address to avoid incidents of duplicate addresses on the LAN.

- The full path name of your TCP/IP base directory. This is the base directory of the server that contains the version of TCP/IP the server is running.
- The full path name of your NFS base directory. The default is the path you entered previously for the TCP/IP base directory.
- The Code Server Hostname.
- The Code Server IP Address.

2.2.1.5 Using NetWare as a Code Server

If the customer network is IPX-based, it will probably be more convenient to configure a NetWare Server as a Code Server.

Attention

We assume the reader of this redbook is familiar with NetWare Server configuration and management and Novell NetWare Requester for OS/2 and DOS.

If you need information about installing and configuring the Novell NetWare Requester for OS/2 please see page 33, "Netware File and Print Gateway Services", in the redbook *Inside OS/2 Warp Server, Volume 1*, SG24-4602.

You must configure the NetWare Server resources according to the applications that are going to be installed from the Code Server.

You must:

1. Create the Code Server Tree.

Note: If you need some suggestions on how to install the remote installation tree in the Code Server, please see the section 2.3.1, "Setting Up a Code Server" on page 145.

2. Create user IDs and passwords.
3. Create trustee rights.
4. Create login script files and map drives.

Regarding the Client: The client can be DOS or OS/2.

- If it's DOS, it must have been configured for IPX (or IPXODI) support.
- If it's OS/2, it must run the Novell NetWare Requester for OS/2 2.01 and above.

This method can be used for installing applications.

If you need to install the client on boot diskettes because you need to install an operating system or an application that requires booting disks, you will find:

- The DOS Client boot disk is quite easy to create.
- A few OS/2 boot diskettes containing the Novell NetWare Requester for OS/2 requires much work and it has many caveats. For this reason, it is not recommended.

Note: If you need information about how to create OS/2 boot diskettes containing the Novell NetWare Requester for OS/2, you can read Chapter 12, page 321, of the redbook titled *OS/2 Installation Techniques: The CID Guide*, SG24-4295.

2.2.2 Installing Operating Systems Using Redirected Drives

Note: In this discussion, we assume that operating systems (such as DOS and OS/2) need to be booted from diskettes to be installed, upgraded or fixed. We assume also that operating systems cannot be deinstalled.

There are two important aspects that we need to discuss in this section, and those are:

1. How easy or difficult is it to obtain boot diskettes using each method of redirecting drives: This is discussed in Table 13.
2. What happens if the installation requires a further boot from a hard disk: In every case, you need to provide some manual intervention in order to have the client attached to the Code Server after booting from the hard disk.

	SRVIFS	LAN Server	TCP/IP	NetWare
Advantages	Easy to install and fits in the OS/2 boot diskette, disk 1.	No need to install a separate piece of software for the Code Server.	Code Server can be a UNIX/AIX machine.	DOS Client boot diskette is quite easy to obtain.
Disadvantages	Doesn't support DOS.	Doesn't support the OS/2 Client in the OS/2 boot diskette, disk 1.	Difficult to fit everything (protocol support, Base TCP/IP, and NFS component) in a single DOS boot diskette.	OS/2 Client boot disk 1 can be obtained with some restrictions.

2.2.2.1 Installation of DOS, Windows and DOS LAN Services Using LAN Server 5.0

Warp Server's remote client install provides a mini-DLS solution to install DOS LAN Services, SystemView Client and Remote Access Client. However, there is no official way to automatically install DOS, Windows and DLS from a LAN Server.

2.2.3 Non-CID-Enabled Applications

These applications need an attended installation, and that means the user has to answer all questions and panels during the installation process.

With a redirected drive, we can avoid using a diskette drive for installation. Of course, the application must allow being installed from a single directory or directory tree in a Code Server.

Compared to the operating system installation, in many cases, installing an application does not require creation of boot diskettes; so, item 1 (see 2.2.2, "Installing Operating Systems Using Redirected Drives" on page 143) is no longer valid.

Most applications are installed at once and don't require rebooting the system to continue installing.

For these reasons, in order to install a non-CID application, every method to obtain a redirected drive is suitable. The only limitation is that you cannot install DOS applications using SRVIFS.

2.2.4 CID-Enabled Applications

These applications allow lightly attended installation because the installation program is able to read and interpret a Response File containing all the parameters the application needs for installation.

Sometimes, the installation program is able to write a log file which is useful for troubleshooting and error finding.

The only difference with the non-CID application is, now the installer is less involved in the installation process, and the installation can be delegated to a less-skilled person.

2.3 Using CASSETUP



CASSETUP is basically a PM-based utility that automates several CID functions.

We will see in this section how to configure a Code Server and build LCU boot diskettes using CASSETUP.

At the same time, we will explain how to use CASSETUP and the existing OS/2 Warp Server CD-ROM CID configuration to install the products contained in the CD-ROM through CASSETUP.

2.3.1 Setting Up a Code Server

There are common tasks a LAN administrator has to perform besides deciding which Software Distribution Management to use.

2.3.1.1 Code Server Directory Structure

Directory Structure

Before you implement your Software Distribution environment, no matter what kind of Software Distribution Manager you are going to use, you must first consider what type of directory structure you want on the Code Server.

The directory structure determines where the product images, and other files that are needed for remote installation, are located so that the LAN CID Utility, CASSETUP or NetView DM/2 can find them.

In the example, as shown in Figure 93 on page 146, the directory structure can be used by NetView DM/2, CASSETUP and LCU.

In this redbook, we assume that you plan to follow the recommended directory structure. If you have created, or if you want to create, a directory structure other than the recommended directory structure, insert your own directory names whenever necessary.

```

d:\-
- SHAREA -
  - CLIENT          /* Client Command Files          */
  - DLL             /* Dynamic Link Libraries for LCU  */
    - V211          /* OS/2 2.11 related               */
    - V30           /* OS/2 Warp Version 3 related     */
  - EXE             /* Executable Files for LCU        */
    - MPTS          /* MPTS related                     */
    - V211          /* OS/2 2.11 related               */
    - V30           /* OS/2 Warp Version 3 related     */
  - PROFILES        /* NetView DM/2 Change File Profiles */
  - IMG -          /* Product Diskette Images      */
    - DLS           /* DOS LAN Services                 */
    - LCU           /* LAN CID Utility                  */
    - LS40A         /* OS/2 LAN Server 5.0 Advanced     */
    - LSP136        /* DOS LAN Support Program V1.36    */
    - MPTS          /* Multiprotocol Transport Services */
    - NVDM2V21     /* NetView DM/2 V.2.1 Extended     */
    - OS2V211      /* OS/2 V.2.11                     */
    - OS2V30       /* OS/2 Warp V3                    */
    - IBMDOS63     /* IBM PC DOS 6.3                  */
    - SRVIFS       /* Mini-Server/Requester Utility   */
  - RSP -          /* Product-Specific Response Files */
    - DLS           /* DOS LAN Services                 */
    - LSA40         /* OS/2 LAN Server 5.0 Advanced     */
    - LSP136        /* DOS LAN Support Program V1.36    */
    - MPTS          /* Multiprotocol Transport Services */
    - NVDM2V21     /* NetView DM/2 V.2.1 Extended     */
    - OS2V211      /* OS/2 V.2.11                     */
    - OS2V30       /* OS/2 Warp V3                    */
    - IBMDOS63     /* IBM PC DOS 6.3                  */
- SHAREB -
  - LOG -          /* Log and History files        */
    - DLS           /* DOS LAN Services                 */
    - LCU           /* LAN CID Utility                  */
    - LS40A         /* OS/2 LAN Server 5.0 Advanced     */
    - LSP136        /* DOS LAN Support Program V1.36    */
    - MPTS          /* Multiprotocol Transport Services */
    - NVDM2V21     /* NetView DM/2 V.2.1 Extended     */
    - OS2V211      /* OS/2 V.2.11                     */
    - OS2V30       /* OS/2 Warp V3                    */
    - IBMDOS63     /* IBM PC DOS 6.3                  */
    - SRVIFS       /* Mini-Server/Requester Utility   */
- FSDATA

```

Figure 93. Code Server Directory Structure Example

Drive letter d:

In figures, examples and syntax diagrams that are shown in this chapter, the drive letter **d:** (always written in lowercase) is the Code Server's drive letter.

The following is a description of the directories found in the recommended directory structure and the intended contents of the directories.

<i>Table 14. Description of the Recommended Directory Structure</i>	
Directory Name	Description
SHAREA	The user-defined name of the root directory for all but the log directories in the recommended structure.
SHAREB	The user-defined name of the root directory for the log directory in the recommended structure.
CLIENT	The client directory containing the command files that LAN CID Utility is to use for the Redirected Installations on the clients. These can be specific client command files, default command files, or both.
DLL	CASSETUP and LAN CID Utility need additional OS/2- and REXX-related dynamic link libraries in order to work properly. For each OS/2 version, there is another subdirectory to this path and directory.
EXE	CASSETUP and LAN CID Utility need additional OS/2 and REXX executable files in order to work properly. For each OS/2 version, there is another subdirectory to this path and directory.
PROFILES	Change file profiles for NetView DM/2. These are product-specific files that contain the syntax of the remote installation program and are needed to build a CDM software catalog.
FSDATA	File services for NetView DM/2. These are the product-specific change files. (Files are called change files because Software Distribution is part of IBM's NetView family. The discipline's name is change management)
IMG	The product images directory containing a subdirectory for each product.
RSP	The Response Files directory containing a subdirectory for each product. The individual product subdirectories hold the general Response Files, the individual client Response Files and the default Response Files for that product. Not all programs use Response Files. For example; the LAN CID Utility installation program (CASINSTL) and the SRVIFS requester installation program (THINIFS) do not.
LOG	The log directory containing a subdirectory for each product.

OS/2 Warp Server CD-ROM CID Directory Structure

Some Assumptions

Let's assume for the exercise that:

1. OS/2 Warp Server boot drive is D:
2. MPTS is installed on drive D:
3. Complementary Code Server Tree is created in D:
4. Code Server files are installed in D:
5. OS/2 Warp Server CD-ROM is in drive F:

The OS/2 Warp Server CD-ROM CID Directory Structure is not organized in the same way the standard CID Directory Structure (like that shown in Figure 93 on page 146).

Figure 94 on page 148 shows the directories in the OS/2 Warp Server CD-ROM that can be involved in a CID process. Looking at the OS/2 Warp Server CD-ROM CID Tree, you can also see the products that can be installed using the CD-ROM.


```

d:\-
- SHAREA -
  - CLIENT          /* Client Command Files          */
  - DLL -          /* Dynamic Link Libraries for LCU */
    - OS2F305      /* OS/2 Warp Version 3 related    */
  - EXE -          /* Executable Files for LCU       */
    - MPTS50       /* MPTS related                    */
    - OS2F305      /* OS/2 Warp Version 3 related    */
  - IMG -          /* Product Diskette Images      */
    - LCU          /* LAN CID Utility                 */
    - NVDM2V21     /* NetView DM/2 V.2.1 Extended    */
    - SAMPLE       /*                                  */
    - APPLETS      /*                                  */
    - SRVIFS       /* Mini-Server/Requester Utility  */
  - RSP -          /* Product Specific Response Files */
    - MPTS50       /* Multiprotocol Transport Services */
    - NVDM2V21     /* NetView DM/2 V.2.1 Extended    */
    - OS2F305      /* OS/2 Warp V3                   */
- SHAREB -
  - LOG -          /* Log and History files          */
    - LCU          /* LAN CID Utility                 */
    - MPTS50       /* Multiprotocol Transport Services */
    - NVDM2V21     /* NetView DM/2 V.2.1 Extended    */
    - OS2F305      /* OS/2 Warp V3                   */
- FSDATA

```

Figure 95. OS/2 Warp Server CD-ROM CID Directory Structure

The first step creates the appropriate directory structure on the hard disk and copies the necessary files from the CD-ROM.

Execute the following commands:

```

D:
CD \
MD SHAREA
MD SHAREA\CLIENT
MD SHAREA\DLL
MD SHAREA\DLL\OS2F305
MD SHAREA\EXE
MD SHAREA\EXE\OS2F305
MD SHAREA\EXE\MPTS50
MD SHAREA\IMG
MD SHAREA\IMG\LCU
MD SHAREA\IMG\NVDM2V21
MD SHAREA\IMG\SRVIFS
MD SHAREA\RSP
MD SHAREA\RSP\OS2F305
MD SHAREA\RSP\MPTS50
MD SHAREA\RSP\NVDM2V21

MD SHAREB
MD SHAREB\LOG
MD SHAREB\LOG\LCU
MD SHAREB\LOG\OS2F305
MD SHAREB\LOG\MPTS50
MD SHAREB\LOG\NVDM2V21

COPY F:\CID\DLL\OS2\*. * D:\SHAREA\DLL\OS2F305
COPY F:\CID\EXE\OS2\*. * D:\SHAREA\EXE\OS2F305
COPY F:\CID\LCU\*. * D:\SHAREA\IMG\LCU
F:\CID\SERVER\MPTS\LAPSRSP D:\IBMCOM\PROTOCOL.INI D:\SHAREA\RSP\MPTS50\DEFAULT.RSP /T:D: /:
CT
COPY F:\OS2IMAGE\SAMPLE.RSP D:\SHAREA\RSP\OS2F305\DEFAULT.RSP

COPY D:\OS2\FDISK.COM D:\SHAREA\EXE\OS2F305
COPY D:\OS2\CHKDSK.COM D:\SHAREA\EXE\OS2F305
COPY D:\OS2\DLL\NLS.DLL D:\SHAREA\DLL\OS2F305

```

Figure 96. Creating the CID Directory Structure

We have created two main directories:

- SHAREA
- SHAREB

Under SHAREA, we create the following subdirectories:

- CLIENT
- DLL
- EXE
- IMG
- RSP

Under SHAREB we create:

- LOG

Directories IMG, RSP and LOG need one subdirectory per product to be installed.

Directories EXE and DLL need to have a subdirectory for each different version of OS/2 to be installed.

Directory EXE needs to have a subdirectory for each different version of MPTS to be installed.

The last COPY statements transfer some important files from the CD-ROM and from the existing operating system to the Code Server hard disk that are needed for the CID installation process.

2.3.1.2 Setting Up a Code Server with the CASSETUP Utility

CASSETUP provides a single graphical interface for several common tasks involved in installing CID-enabled products over the network.

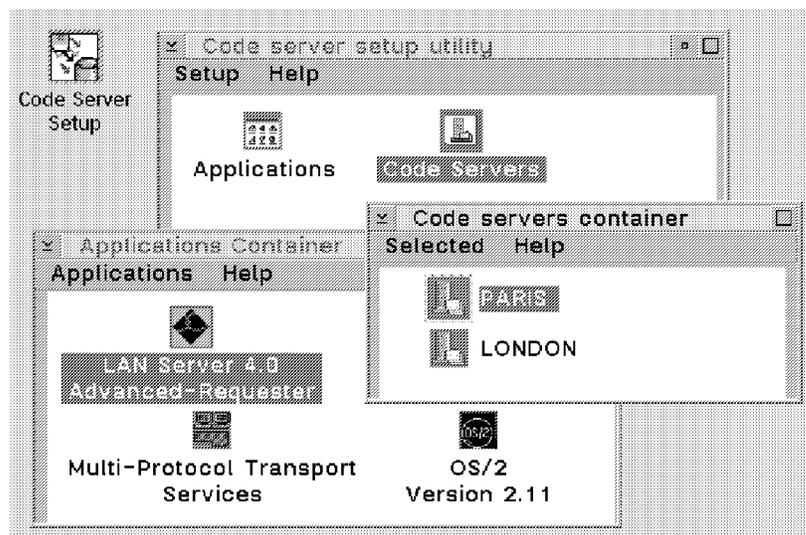


Figure 97. CASSETUP Code Server Setup Utility

CASSETUP allows you to:

- Install the means of redirection SRVIFS (a simple server)
- Run the LAN CID Utility (LCU)
- Load product diskette images from diskettes or CD-ROM onto a Code Server
- Build LCU boot diskettes for diskette-initiated clients
- Create CASPREP files which can be used to generate the client-specific LCU command files

CASSETUP generally can handle all kinds of CID-enabled applications. To add an application to the suite that CASSETUP understands, you just add an application (.PRO) profile to the CASSETUP directory. As described in the following pages, the CASSETUP directory in our following example is D: CASSETUP.

Similarly, to build boot diskettes of different OS/2 versions, you just create a diskette-built (.SCR) script file by using the existing script files as templates.

2.3.1.3 Installation of CASSETUP Utility

Before you proceed with the next steps, make sure you have created the recommended directory structure discussed in 2.3.1.1, "Code Server Directory Structure" on page 145.

1. Create a directory, for example, D: CASSETUP.
2. Unzip the CASSETUP.ZIP file from the OS/2 Warp Server CD-ROM disk.

```
--PKUNZIP2-----  
--F: \CID\SERVER\IBMLS\IBM500N5\APPLETS\CASSETUP.ZIP--D: \CASSETUP--
```

3. Generally, two modifications to CASSETUP files should be made.

- a. First, change a REXX statement in the CASENG3.CMD file. Using an ASCII editor, like EPM, go to line 627, and change the following statement:

```
logpath = lcudrive
```

to:

```
logpath = logdrive
```

Unless you make this change, all clients being remotely installed will have read/write access to the product image tree.

- b. Second, make the following changes to the CASENG6.CMD file. Load this file using an ASCII editor, and go to line 1003. Look for the following section:

```
TheCmd = TheCmd || '/l1:'glob.lcualias.0Drive':\'
IF glob.lcupath <> "" THEN
TheCmd = TheCmd || STRIP(glob.lcupath,'b','\') || "\"
TheCmd = TheCmd || 'LOG\lcu\"client\".log '
TheCmd = TheCmd || '/l2:'glob.lcualias.0Drive':\'
IF glob.lcupath <> "" THEN
TheCmd = TheCmd || STRIP(glob.lcupath,'b','\') || "\"
TheCmd = TheCmd || 'LOG\lcu\srvifs_req.log '
TheCmd = TheCmd || '/req:"client"'
```

and make the following changes to this section:

```
TheCmd = TheCmd || '/l1:'glob.logalias.0Drive':\'
IF glob.lcupath <> "" THEN
TheCmd = TheCmd || STRIP(glob.lcupath,'b','\') || "\"
TheCmd = TheCmd || 'LOG\lcu\"client\".log '
TheCmd = TheCmd || '/l2:'glob.logalias.0Drive':\'
IF glob.lcupath <> "" THEN
TheCmd = TheCmd || STRIP(glob.lcupath,'b','\') || "\"
TheCmd = TheCmd || 'LOG\lcu\srvifs_req.log '
TheCmd = TheCmd || '/req:"client"'
```

Unless you make this change, logfiles cannot be written since lcu drive is a read/only area, whereas log drive is not.

4. From the D: CASSETUP directory, issue the following installation command from an OS/2 command line:

```
--CASINST-----
```

A Code Server Setup icon will appear on your desktop when the installation of CASSETUP is complete, and will display the following:

After Code Server Setup

```
-----  
Date: 30 October 1995      Time: 11:58:01  
Code Server Utility Installation  
-----  
--- Establishing Execution profile  
--- Creating Workplace shell object  
Code Server Setup WorkPlace object created  
-----  
Code Server installation ended  
Updating config.sys...  
    1 file(s) copied.  
    1 file(s) copied.  
Your original config.sys was backed up in file D:\config.477  
Your config.sys has been updated.  Reboot before running CASSETUP.
```

5. Shut down and reboot your workstation as prompted.

Earlier Versions of CASSETUP

If you plan to use CASSETUP under OS/2 Warp, make sure you have the version of CASSETUP that comes with OS/2 Warp Server. A preceding version will hang when started on an OS/2 Warp machine. The update files, known as APAR IC08609 and IC08610, are:

```
CASSETUP.EXE      (10/28/94 version or later)  
OS230.PRO  
30NNTS.SCR
```

2.3.1.4 Modify CASSETUP.STR Storage Information File

Before you actually load the CASSETUP Code Server setup utility, we recommend you adapt the storage information file, CASSETUP.STR, to your CID environment. Alternatively, you may use the application features of CASSETUP to modify default values.

Change to the d: CASSETUP directory, and edit the file CASSETUP.STR by using an ASCII editor, such as EPM.

For the example of the installation of the CID connection server using the OS/2 Warp Server CD-ROM, let's consider the proposed directory structure shown in Figure 93 on page 146. Alter the entries as highlighted and shown in Figure 98 on page 154.

```

*****
**          Code Server Setup Utility
** Date last written: 30 Oct 1995
** Time last written: 17:55:55
*****
Server.
  srvname=ENRIQUE          /* Name of the SRVIFS Server
  srvgroup=0
  imgalias=IMAGES        /* Default Image Alias
  nifpath=
  srviceon=CASSETUP:\108  /* Type of ICON
  srvtitle=Enrique's Code Server /* SRVIFS Server Description
  firstflag=1
Alias.
  aliasname=LOGFILES      -----* This alias define a resource that
                           ] resides on the Code Server hard disk.
  aliasdrive=D:           ] Is used by CASSETUP to
  aliaspath=\SHAREB      ] write LOG files during
  aliasro=0               ] remote installation.
endalias.
Alias.
  aliasname=IMAGES        -----* This alias define a resource that
                           ] resides on the OS/2 Warp Server CD-ROM.
  aliasdrive=F:           ] Is used by CASSETUP to
  aliaspath=\             ] locate OS/2 Warp image
  aliasro=1               ] files in OS2IMAGE directory.
endalias.
Alias.
  aliasname=IMAGES1       -----* This alias define a resource that
                           ] resides on the OS/2 Warp Server CD-ROM.
  aliasdrive=F:           ] Is used by CASSETUP to
  aliaspath=\CID\SERVER   ] locate the Server Product image
  aliasro=1               ] files in different directories.
endalias.
Alias.
  aliasname=IMAGES2       -----* This alias define a resource that
                           ] resides on the OS/2 Warp Server CD-ROM.
  aliasdrive=F:           ] Is used by CASSETUP to
  aliaspath=\CID\CLIENT  ] locate the Client Product image
  aliasro=1               ] files in different directories.
endalias.
Alias.
  aliasname=IMAGES3       -----* This alias define a resource that
                           ] resides on the Code Server hard disk.
  aliasdrive=D:           ] Is used by CASSETUP to
  aliaspath=\SHAREA      ] locate the Software Product image
  aliasro=1               ] files in IMG directory.
endalias.
Alias.
  aliasname=OTHFILES      -----* This alias define a resource that
                           ] resides on the Code Server hard disk.
  aliasdrive=D:           ] Is used by CASSETUP to
  aliaspath=\SHAREA      ] locate information other that image
  aliasro=0               ] files in DLL, EXE, RSP and CLIENT
endalias.
-----* directories.
Srvifs.
  srvifsflag=1
  maxfiles=100
  maxsessions=5
  maxthreads=10
  adapterno=0
  clientdrive=d
  cidpath=
  diraccess=
  perclient=0
  serverpath=D:\SRVIFS
  LCUpath=
  LOGAlias=LOGFILES
  RSPAlias=OTHFILES
  CMDAlias=OTHFILES
  WRKAlias=OTHFILES
  DLLAlias=OTHFILES
  LCUAlias=OTHFILES
  Cmddir=CLIENT
Endsrvifs.
Endserver.

```

Figure 98. CASSETUP Storage File CASSETUP.STR

Note: The server name (srvname) must be a unique name not used by other NetBIOS applications, such as LAN Server/Requester, and must not exceed eight bytes (characters or numbers).

Reminder—Directory Structure

Make sure all directories mentioned in the CASSETUP.STR file exist. Otherwise, some parts of the installation may fail. For example, you may receive an error message like the one shown in Figure 99.

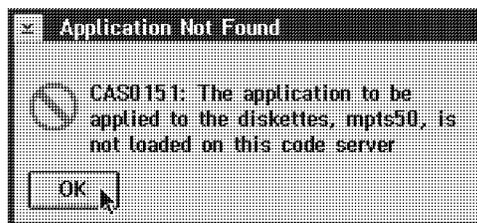


Figure 99. Error Message: MPTS50 Directory Not Created

2.3.1.5 Selecting Application Profiles

The Code Server utility comes with a series of application profile (.PRO) files which are installed by the CASINST command.

These are examples of application profiles for different CID-enabled products:

LS40A.PRO	OS/2 LAN Server 4.0 Advanced (whole product)
LS40E.PRO	OS/2 LAN Server 4.0 Entry (whole product)
LS40AREQ.PRO	OS/2 LAN Server 4.0 Advanced (Requester part)
LS40AREQ.PRO	OS/2 LAN Server 4.0 Entry (Requester part)
LS40CDA.PRO	OS/2 LAN Server 4.0 Advanced (whole product) from CI
LS40CDE.PRO	OS/2 LAN Server 4.0 Entry (whole product) from CD
MPTS10.PRO	Multiprotocol Transport Services
MPTS10CD.PRO	Multiprotocol Transport Services from CD
OS221.PRO	OS/2 2.1
OS2211.PRO	OS/2 2.11
OS221SP.PRO	OS/2 2.1 Service Pak XR06200
OS2F30.PRO	OS/2 Warp Version 3.0 (Full version)
OS2F30CD.PRO	OS/2 Warp Version 3.0 (Full version from CD)
OS2W30.PRO	OS/2 Warp Version 3.0 (For Windows version)
OS2W30CD.PRO	OS/2 Warp Version 3.0 (For Windows version from CD)

The following profiles appear in the D:\CASSETUP directory after they are unzipped from the CASSETUP.ZIP file contained in the OS/2 Warp Server CD-ROM:

LS50AREQ.PRO	LAN Server 5.0 Advanced Requester
LS50EREQ.PRO	LAN Server 5.0 Entry Requester
LS50WSA.PRO	LAN Server 5.0 Advanced Server
LS50WSE.PRO	LAN Server 5.0 Entry Server
MPTS50WS.PRO	Multiprotocol Transport Services 5.0
OS2WS.PRO	OS/2 Warp 3.0 (Full version from CD)

1. Creating Additional Application Profiles or Modifying the Existing Ones: If you want to distribute OS/2 Warp Version 3, you can easily modify its application profile by doing the following:

- In the CASSETUP directory, copy the template file OS2WS.PRO to OS2WS.000.
- Edit the OS2WS.PRO file, and change the following values as shown emphasized in Figure 100.

```

* CASSETUP application profile for: OS/2 Warp 3.0 (WIN-OS2 version)
*****
* APPLICATION DESCRIPTION SECTION *
*****
APPNAME = OS/2 Warp Server with WIN-OS/2Version 3.05 CD-ROM
APPNICK = OS2F305
PROGTYPE = 1
ICON = CASSETUP:#111
OS = 1
PACKAGE = 1
* FIXTO =
* FIXLEVEL =
LOADPREREQS = <LCU>
*****
* IMAGE LOAD SECTION *
* (elements in this section describe how the application's *
* install image is put onto a Code Server -- usually by being *
* copied from install diskettes or CD-ROM) *
*****
APPDIR =OS2IMAGE
WORKDIR = EXE\OS2F305
DLLDIR = DLL\OS2F305
RESPDIR = RSP\OS2F305
LOGDIR = LOG\OS2F305
METHOD = 2
NUMDSKT = 1
IMAGELOAD.0 = 0
IMAGELOAD.1 = XCOPY $$\OS2IMAGE $T /s /e /v /h /o /t /r
IMAGELOAD.2 = GetOSCID $T $W
IMAGELOAD.3 = GetRExx $T $D
IMAGELOAD.4 = GetBoot $T $W
SETUP.0 = 1
SETUP.1 = OS/2 Warp Server 3.05 CD-ROM
SETUP.1.0MarkerFile = OS2IMAGE\DISK_0\OS2KRNL1
SETUP.1.0 = 0
*****
* INSTALL SECTION *
* (elements in this section deal with how the application is *
* remotely installed). *
*****
INSTCMD = $W\seinst /b:$B /s:$S /t:$T /l1:$L\"client\".log /r:
DEFRESPFILE = default.rsp
MaintSysReq = 1
*****
* MAINTENANCE SYSTEM SECTION *
* (applications that have a PROGTYPE of 1 (OS), 2 (transport) *
* or 3 (redirector) have associated commands that allow them *
* to be installed as part of Maintenance Systems. This section *
* describes those commands. *
*****
MSCmd.0 = 2
MSCmd.1 = $W\semaint /s:$S /t:$M /b:$B /l1:$L\"client\".log
MSCmd.1.0CmdName = semaint
MSCmd.2 = $W\sedisk /S:$S /T:$T
MSCMD.2.0CmdName = sedisk
MaintSysBuild = 1

```

Figure 100. CASSETUP Profile for OS/2 Warp Version 3 (OS230.PRO)

You need to specify the directory for the OS/2 Warp 3.0 Image files in:

APPDIR =**OS2IMAGE**

Specify that you don't need to download the images of the product into the Code Server, with:

IMAGELOAD.0 = 0

Figure 101 shows the CASSETUP profile file for MPTS 5.0. You will also find emphasized the changes you need to do to this file.

```
*****
*          APPLICATION DESCRIPTION SECTION          *
*****
APPNAME = Multi-Protocol TransportServices 5.0 from Warp Server
APPNICK = mpts50
PROGTYPE = 2
ICON = CASSETUP:#107
OS = 1
PACKAGE = 1
* FIXTO =
* FIXLEVEL =
*****
*          IMAGE LOAD SECTION                      *
* (elements in this section describe how the application's *
* install image is put onto a Code Server -- usually by being *
* copied from install diskettes or CD-ROM) *
*****
APPDIR = MPTS
WORKDIR = EXE\mpts50
DLLDIR = DLL\mpts50
RESPDIR = RSP\mpts50
LOGDIR = LOG\mpts50
METHOD = 2
NUMDSKT = 1
IMAGELOAD.0 = 0
g fixed.
IMAGELOAD.1 = XCOPY $$\CID\SERVER\MPTS $T /s
SETUP.0 = 1
SETUP.1 = MPTS 5.0 WARP SERVER CD-ROM
SETUP.1.0MarkerFile = CID\SERVER\MPTS\MPTS.EXE
* SETUP.1.1Volser = WARP SERVER
SETUP.1.0 = 0
*****
*          INSTALL SECTION                        *
* (elements in this section deal with how the application is *
* remotely installed). *
*****
INSTCMD = $$\mpts /e:prod /s:$S /t:$B /l1:$L\"client\".log /r:
INSTCMDM = $$\mpts /e:maint /s:$S /t:$B /l1:$L\"client\".log /r:
DEFRESPFILE = default.rsp
MaintSysReq = 0
*****
*          MAINTENANCE SYSTEM SECTION            *
* (applications that have a PROGTYPE of 1 (OS), 2 (transport) *
* or 3 (redirector) have associated commands that allow them *
* to be installed as part of Maintenance Systems. This section *
* describes those commands. *
*****
MSCmd.0 = 2
MSCmd.1 = $$\mpts /e:prep /s:$S /t:$M /tu:$B /l1:$L\"client\".log /r:
MSCmd.1.0DefRespFile = default.rsp
MSCmd.1.0CmdName = mpts_prep
MSCmd.2 = $$\thinlaps . $T $N
MaintSysBuild = 1
```

Figure 101. CASSETUP Profile for MPTS 5.0 (MPTS50WS.PRO)

You need to specify the directory for the Multiprotocol Transport Services 5.0 Image files in:

APPDIR = **MPTS**

Specify that you don't need to download the images of the product into the Code Server, with:

IMAGELOAD.0 = 0

Now, suppose that we need to distribute an application that doesn't have a template in the D:\CASSETUP directory. We can use a similar one as a model and modify it.

The following example shows how to generate a profile file for SystemView in Warp Server. We used the profile file, OS2WS, for our template for OS/2 Warp V3.0, and typed:

```
COPY OS2WS.PRO SYSVIEW2.PRO
```

Please see Figure 102 on page 159. All changes we have made are emphasized.

```

* CASSETUP application profile for: OS/2 Warp 3.0 (WIN-OS2 version)
*****
*          APPLICATION DESCRIPTION SECTION          *
*****
APPNAME = SystemView in Warp Server Manager
APPNICK = SYSVIEW2
PROGTYPE = 4
ICON = CASSETUP:#111
OS = 1
PACKAGE = 1
* FIXTO =
* FIXLEVEL =
LOADPREREQS = <LCU>
*****
*          IMAGE LOAD SECTION          *
* (elements in this section describe how the application's *
* install image is put onto a Code Server -- usually by being *
* copied from install diskettes or CD-ROM) *
*****
APPDIR =SYSVIEW2\SERVER_2
WORKDIR = EXE\SYSVIEW2
DLLDIR = DLL\SYSVIEW2
RESPDIR = RSP\SYSVIEW2
LOGDIR = LOG\SYSVIEW2
METHOD = 2
NUMDSKT = 1
IMAGELOAD.0 = 0
IMAGELOAD.1 = XCOPY $$\OS2IMAGE $T /s /e /v /h /o /t /r
IMAGELOAD.2 = GetOScid $T $W
IMAGELOAD.3 = GetRExx $T $D
IMAGELOAD.4 = GetBoot $T $W
SETUP.0 = 1
SETUP.1 = OS/2 Warp Server 3.05 CD-ROM
SETUP.1.0MarkerFile = OS2IMAGE\DISK_0\OS2KRNL1
SETUP.1.0 = 0
*****
*          INSTALL SECTION          *
* (elements in this section deal with how the application is *
* remotely installed). *
*****
INSTCMD = $$\svinst /X /A:I /S:$$ /T:$T
/11:$L\C.11 /12:$L\C.12
/13:$L\C.13 /r:DEFRESFILE = default.rsp
MaintSysReq = 0
*****
*          MAINTENANCE SYSTEM SECTION          *
* (applications that have a PROGTYPE of 1 (OS), 2 (transport) *
* or 3 (redirector) have associated commands that allow them *
* to be installed as part of Maintenance Systems. This section *
* describes those commands. *
*****
MSCmd.0 = 2
MSCmd.1 = $W\semaint /s:$$ /t:$M /b:$B /11:$L"client".log
MSCmd.1.0CmdName = semaint
MSCmd.2 = $W\sedisk /S:$$ /T:$T
MSCMD.2.0CmdName = sedisk
MaintSysBuild = 1

```

Figure 102. CASSETUP Profile for SystemView in Warp Server Manager (SYSVIEW2.PRO)

SVINST /X is the command for SystemView in Warp Server remote installation. We have specified the keyword:

```

INSTCMD = $$\svinst /X /A:I /S:$$ /T:$T /11:$L\C.11
/12:$L\C.12 /13:$L\C.13 /r:

```

in the profile file, where **\$\$**, **\$T**, **\$L**, **\$C** are replaced for, respectively, the source, the target, the log, and the client directories.

Remote Installation

For a detailed description of the keywords for the SVINST command, refer to the redbook titled *SystemView Up and Running*, SH19-4184.

You must set the keyword `MaintSysReq` to **0** because the system doesn't require maintenance service.

You must specify the directory for the SystemView in Warp Server Manager Image files in:

```
APPDIR = SYSVIEW2\SERVER_2
```

Specify that you don't need to download the images of the product into the Code Server, with:

```
IMAGeload.0 = 0
```

2. Creating Additional Boot Diskette Script Files: In order to create a set of OS/2 Warp Version 3 boot diskettes, you need to add the following boot diskette script file:

- In the `CASSETUP` directory, copy the file `30WMPTS.SCR` to `30MPTSWS.SCR`.
- Edit the `30MPTSWS.SCR` file, and change values as shown in Figure 103.

```
Title: OS/2 Warp Server and MPTS 5.0
Desc:
Build boot diskettes with OS/2 Warp Server and MPTS 5.0
EndDesc:
  * This is a comment line
  * The next line causes a prompt for a diskette to be
  * issued:
*Prompt: Programs Diskette #1
  * This next line allows us to put up a warning message if needed
*Warn: If the version of OS/2 running on this Code Server is 2.2 or higher, Boot Diskette
creation will probably fail. Press OK to continue.
  * The next line does a verify step. If it fails, the
  * previous line is executed again. You can choose to
  * verify either the volume label or a file or nofiles
  * by the arguments VOLSER label, FILE filename, or
  * BLANK
*Verify: FILE anyfile.txt
  * The next lines executes steps:
OS: 2 os2f305
TRANSPORT: 2 mpts50 $N=NIFFILESPEC
  * lines of this sort have a type followed by a colon,
  * then an integer then a label. The label is the
  * nickname of an application loaded on the code server
  * using CASSETUP. The integer is the
  * ordinal of the maintenance-system building command
  * in the profile. The rest of the line defines
  * symbolic substitutions. The left side is the string
  * to be replaced on the command line; the right is
  * the name of an environment variable that contains
  * the data to be substituted.
```

Figure 103. Boot Diskette Profile for OS/2 Warp V3 (30WMPTS.SCR)

DOS Remote IPL

Using CASSETUP, you cannot remotely install LAN Server 5.0 with the DOS Remote IPL feature. This is due to CASSETUP's own transfer procedure. It does not use the LANINST command of OS/2 LAN Server 5.0 to transfer product diskettes for remote installation. Therefore, you will not be prompted for any DOS version to be supported with OS/2 LAN Server 5.0.

2.3.1.6 Working with the CASSETUP Utility

Prior to starting the CASSETUP utility, you must enable your Code Server for remote installation. That means you must have MPTS loaded on your Code Server, and configured with the NetBIOS network protocol. For more information, refer to page 133, "Installing Adapter and Protocol Services", in the redbook titled *Inside OS/2 Warp Server, Volume 1*, SG24-4602.

Start the CASSETUP utility by double-clicking on its Code Server Setup icon. While loading, it reads profile and storage information you adapted, selected, and added in the steps before. From the Code Server Setup utility folder, open the **Applications** and **Code Servers** objects.

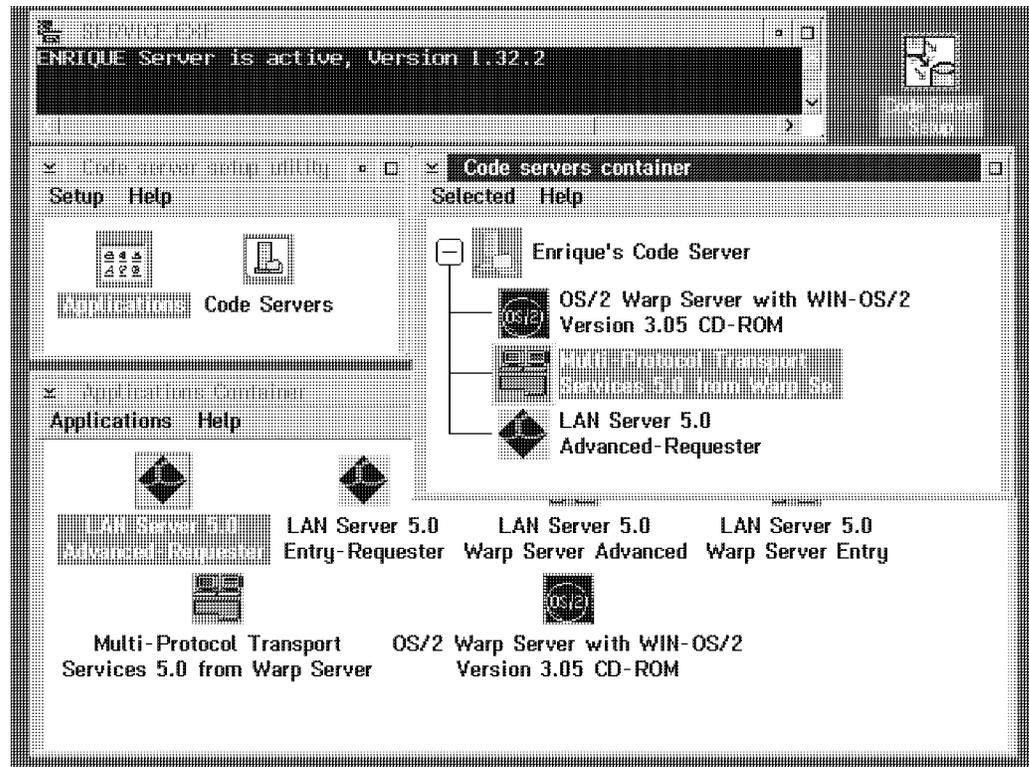


Figure 104. CASSETUP Containers

1. Load LAN CID Utility and SRVIFS.
 - a. Within the Code Servers container, pull down the **Selected** menu.

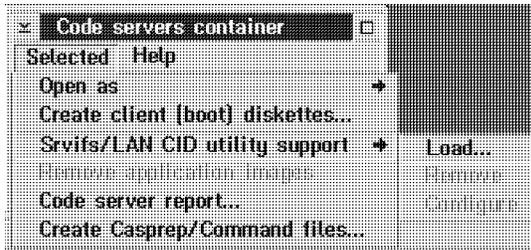


Figure 105. Code Servers Container Selected Menu

- b. Select **Srvifs/LAN CID utility support**.
- c. Then Select **Load...**

The Load Srvifs/LAN CID utility support window will be opened. This window is shown in Figure 106.

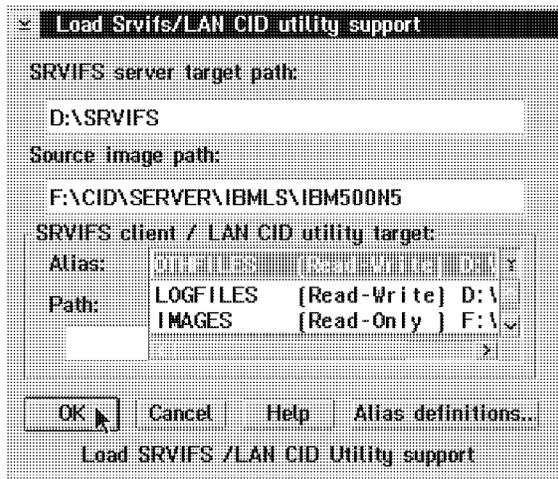


Figure 106. Load Srvifs/LAN CID Utility Support Window of CASSETUP

- d. Select the **OK** button to start the installation process (you do not need to insert a path since the IMAGES alias already points to the F: directory).

LAN CID Utility and SRVIFS are being installed on the Code Server. After successful completion, the following information window will pop up on your screen to prompt you to stop the Code Server utility and to restart the workstation:

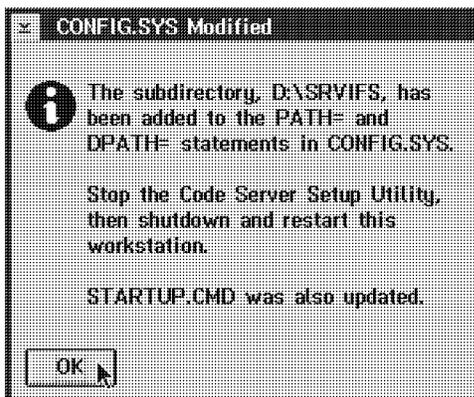


Figure 107. Load Srvifs/LAN CID Utility Support - CONFIG.SYS Modified Window

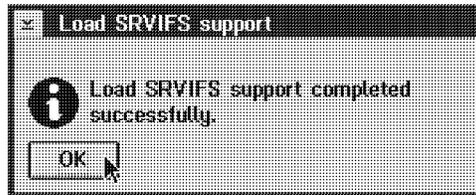


Figure 108. SRVIFS Support Completed Successfully

According to the changes made to the CASSETUP.STR file, the following initialization SERVICE.INI file was created for SRVIFS:

```
Name = ENRIQUE
GroupName = no
Adapter = 0
MaxClients = 5
MaxFiles = 100
ClientWorkers = 10
Path = D:\SHAREA
PermitWrite = no
PerClient = no
ALIAS=READWRITE, SINGLE, LOGFILES, D:\SHAREB
ALIAS=READONLY, SINGLE, IMAGES, F:\
ALIAS=READONLY, SINGLE, IMAGES1, F:\CID\SERVER
ALIAS=READONLY, SINGLE, IMAGES2, F:\CID\CLIENT
ALIAS=READONLY, SINGLE, IMAGES3, D:\SHAREA
ALIAS=READWRITE, SINGLE, OTHFILES, D:\SHAREA
```

After restart of the workstation, SRVIFS-Server will be started from the STARTUP.CMD.

Note: If you want to change a parameter in CASSETUP.STR after the SRVIFS/LAN CID utility support was installed, you need to select **Configure** from the Selected pull-down menu (see Figure 105 on page 162). This will update SERVICE.INI accordingly. At the conclusion, you will get a message such as the one shown in Figure 109.

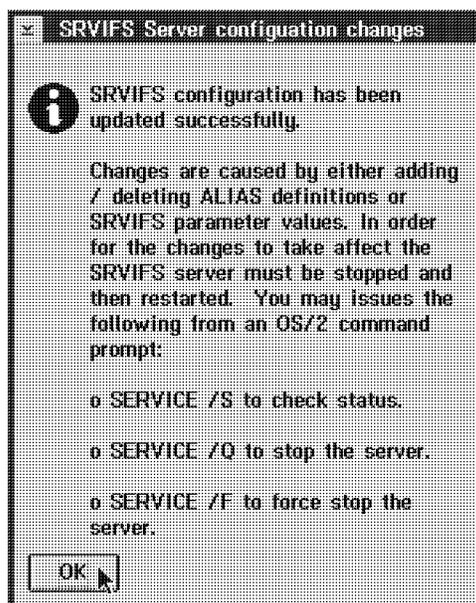


Figure 109. Updating CASSETUP.STR

2. Upload and register the products.

- a. From the applications window (suite), drag the desired product object you want to make available for remote installation to the Code Server's icon in the Code Server's window (suite). For example, drag the OS/2 Warp Version 3 object, and drop it to the server's object, ENRIQUE.

The Application Image Load window will be opened as shown in Figure 110.

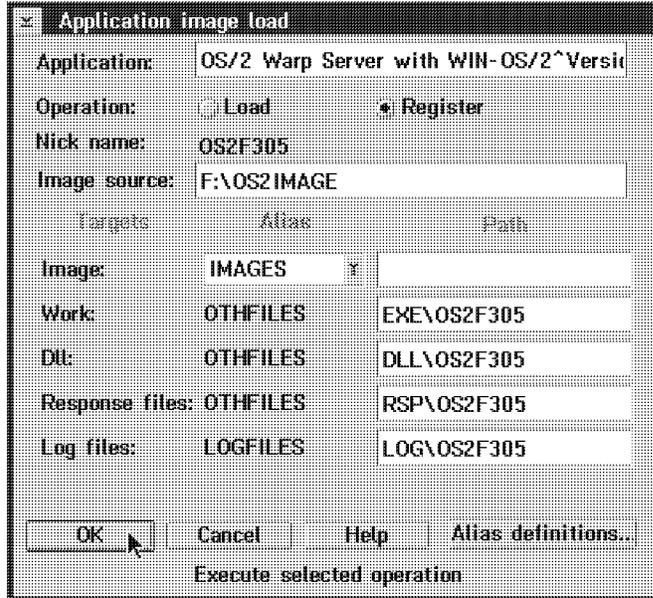


Figure 110. Definition for OS/2 Warp V3

Figure 111 shows the Application image load window for the MPTS 5.0.

Note, the image alias has changed (IMAGES for IMAGES1), and we must also specify MPTS as the subdirectory for image files.

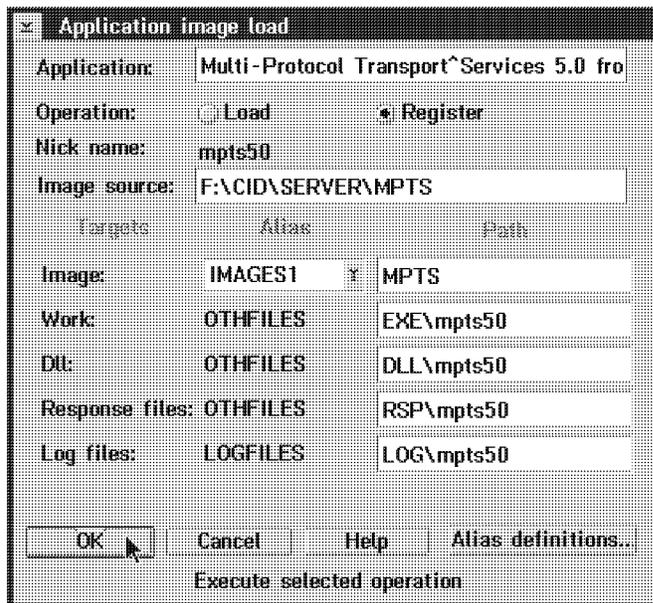


Figure 111. Definition for MPTS

Figure 112 on page 165 shows the Application image load window for the LAN Requester Advanced.

Files are located in the same directory as the server (IBMLS), and the alias is IMAGES1.

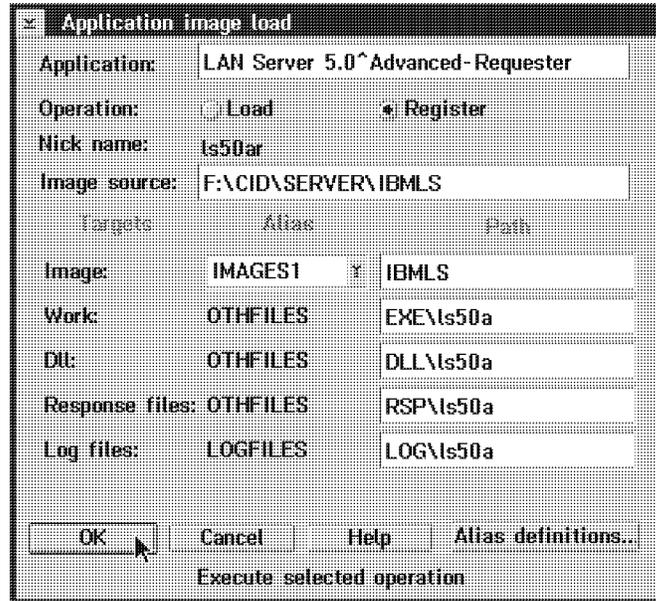


Figure 112. Definition for LAN Requester

Figure 113 shows the Application image load window for the LAN Server Advanced.

Files are located in the same directory, IBMLS, and the alias is IMAGES1.

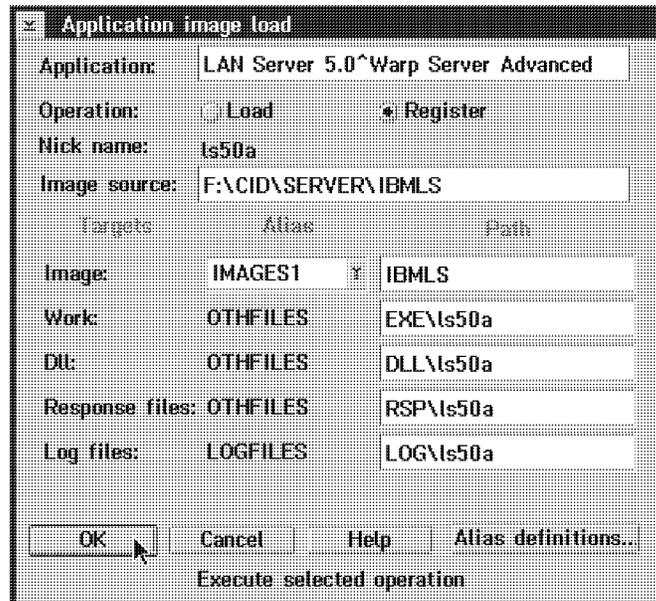


Figure 113. Definition for LAN Server

Figure 114 on page 166 shows the Application image load window for the SystemView in Warp Server Manager.

Files are located in the same directory, SYSVIEW2\SERVER_2, and the alias is IMAGES1.

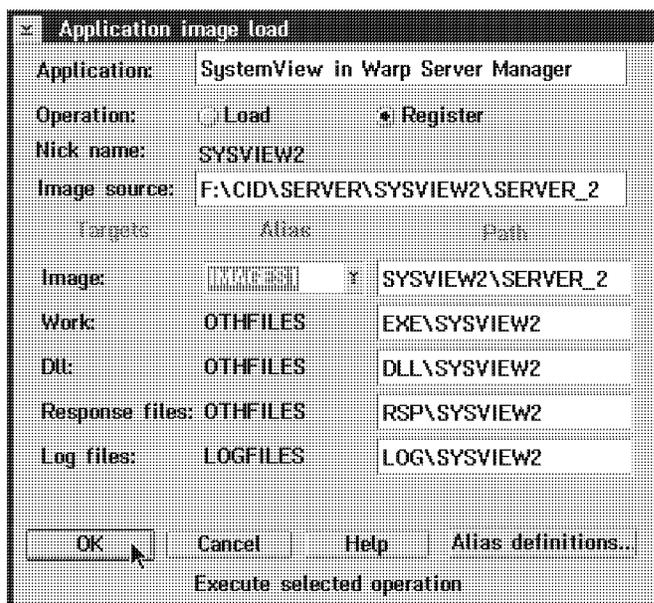


Figure 114. Definition for SystemView

The Operation attribute allows you to choose between **Load** and **Register**. Select either:

- **Load** - When you want to upload the product diskette images to the Code Server's directory (in this case, select this option).
- **Register** - When you only want to register the product since the product has already been uploaded (which means the CID Tree with the product images must have been created before with the CASSETUP utility).

All entries are retrieved from the (.PRO) profile files and the CASSETUP.STR file you adapted in the steps before. Therefore, you do not need to change the field's values.

Select **OK** to start the operation, and insert diskettes as prompted.

OS/2 Warp Server CD-ROM

You don't have to execute the Load procedure for the products contained in the OS/2 Warp Server CD-ROM. But you need to *register* them in the Code Server Tree.

3. Use the same procedure for all other products that are available in the applications window (suite) created from products contained in the OS/2 Warp Server CD-ROM and additional products installed in the Code Server hard disk.
4. You now may check to see if all applications uploaded in the steps before are available at the Code Server's tree. Expand the tree of Code Server ENRIQUE.

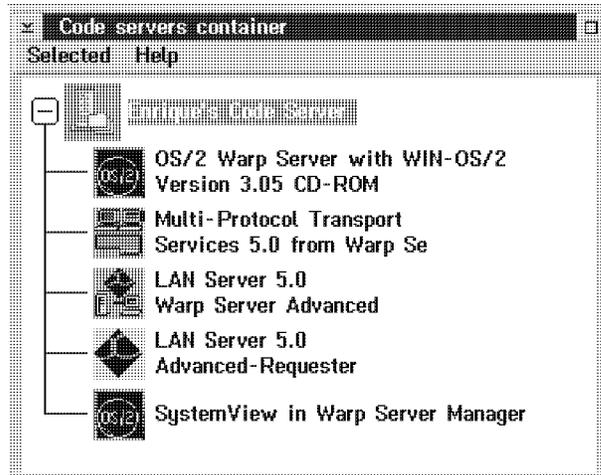


Figure 115. Available Applications at Code Server ENRIQUE

5. To create client boot diskettes for pristine installations, perform the following steps:
 - a. Open the **Code Servers** window (suite).
 - b. Pull down the **Selected** menu (see Figure 105 on page 162).
 - c. Select **Create client (boot) diskettes...**

The Create Client (boot) diskettes window will be opened (which is shown in Figure 116).

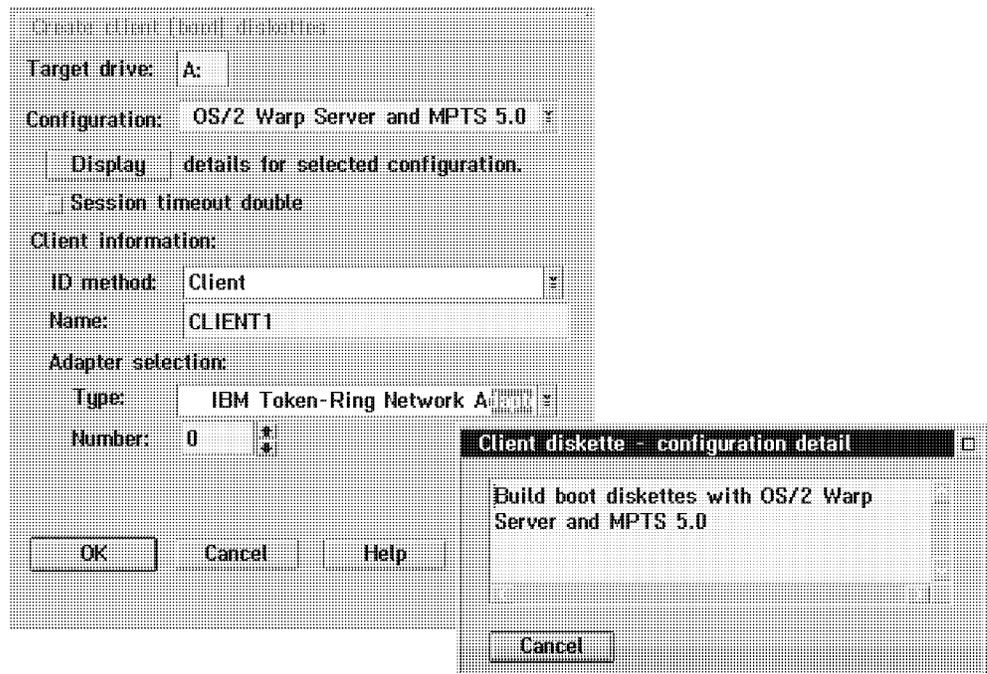


Figure 116. Create Client (Boot) Diskettes Window of CASSETUP

- d. Select the correct configuration, ID method, and adapter type from the pull-down menus. If you select **Prompt** as the ID method, the IPLed client will prompt for the client's name. Otherwise, select **Client**, and enter the client's name. When all selections are made, select the **OK** button. The Boot Diskette Creation utility prompts you for two diskettes. While

creating the boot diskettes, the following steps will be done without user interaction:

- Creation of a pair of OS/2 boot diskettes
- Installation of Multiprotocol Transport Services-LAN Adapter and Protocol Support
- Installation of the Mini-SRVIFS requester
- Installation of LAN CID Utility

After successful completion of the client boot diskette, select **Cancel** to close the window.

After creation of the OS/2 boot diskettes, you need to edit the CONFIG.SYS file of the OS/2 boot diskette, disk 1, and correct the drive assignments.

```
basedev=detne2.sys /p:360
buffers=32
iopl=yes
memman=swap,delayswap
protshell=sysinst1.exe
SET OS2_SHELL=CMD.EXE /K A:\STARTUP.CMD
diskcache=D2,LW
protectonly=yes
libpath=.;\;\os2\install; X :\DLL\OS2F305; X :\IMG\LCU;
ifs=hpfs.ifs /c:64
pauseonerror=no
codepage=850
devinfo=kbd,us,keyboard.dcp
devinfo=scr,ega,vtbl850.dcp
device=\dos.sys
set path=\;\os2;\os2\system;\os2\install;A:\SRVIFSRQ;A:\;
set dpath=A:\;\;\os2;\os2\system;\os2\install;A:\SRVIFSRQ; X :\DLL\OS:
X :\IMG\LCU;
set keys=on
basedev=ibmkbd.sys
basedev=ibm1flpy.add
basedev=ibm1s506.add
basedev=cmd640x.add
basedev=ibm2flpy.add
basedev=ibm2adsk.add
basedev=ibm2scsi.add
basedev=ibmint13.i13
basedev=os2dasd.dmd
device=\testcfg.sys
basedev=xdfloppy.flt
device=\refpart.sys
rem *** Start of ThinLAPS additions ***
device = lanmsgdd.os2
device = protman.os2
device = netbeui.os2
device = netbios.os2
device = IBMTOK.OS2
call = netbind.exe
run = lanmsgex.exe
rem *** End of ThinLAPS additions ***
CALL=A:\SRVIFSRQ\SRVATTCH.EXE X : \ENRIQUE\OTHFILES
DEVICE=A:\SRVIFSRQ\SRVIFS.SYS
IFS=A:\SRVIFSRQ\SRVIFSC.IFS CLIENT1 /S:5 /A:0
```

```
CALL=A:\SRVIFSRQ\SRVATTCH.EXE Z : \\ENRIQUE\LOGFILES
RUN= X : :\IMG\LCU\SRVREXX.EXE
```

These changes are necessary because the drive assignments done by this diskette during OS/2 startup must match the additional drive assignments that the LCU REXX Command File will define during its execution.

You also need to make changes to the STARTUP.COM file.

```
X : \IMG\LCU\CASAGENT.EXE /CMD: X : \CLIENT /L1: Y : \LOG\LCU\SRVIFS_RI
CMD
EXIT
```

6. To create client-specific LAN CID Utility command files for remote installation, open the Code servers container Selected menu (see Figure 105 on page 162) and select **Create Casprep/Command files...** The LAN CID Utility casprep/command files window will be opened (as shown in Figure 117):

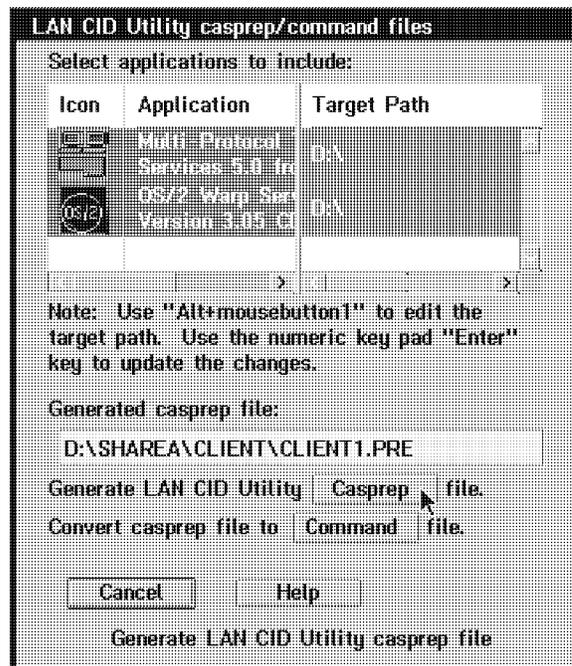


Figure 117. LAN CID Utility Casprep/Command Files Window of CASSETUP

- a. Select the applications you want to install remotely.
- b. Change the target path, if necessary. To edit the target path, use the Alt+left mouse button sequence. The path gets updated when you press the numeric Enter key (which is the Enter key on the numeric keypad).
- c. Select **Generate LAN CID Utility Casprep file.**

This procedure invokes the generation of a LAN CID Utility Casprep file that can be converted to the LAN CID Utility client command file. If OS/2 is selected as an application to be installed remotely, an additional dialog window will be displayed to provide information for the process to create a maintenance system. A maintenance system is needed, for example, for applications that are going to be installed remotely, but do not need, or must not have, Presentation Manager active. If such a dialog window (shown in Figure 118 on page 170) is displayed, select the correct target operating system, and select the **OK** button.

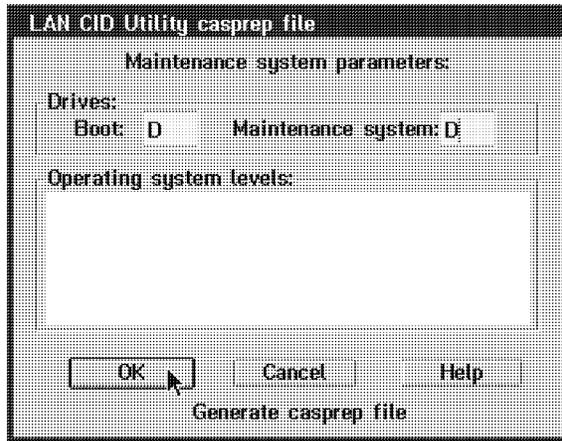


Figure 118. LAN CID Utility Casprep File Dialog Window

After the generation of the casprep file, you should get an information window that displays a successful completion.

Some products like MPTS and LAN Server don't observe the Target Path specification (see Figure 117 on page 169); they only need the Target Drive, because the path is set by the application itself.

SystemView in Warp Server needs to be provided complete information about the Target Path. See Figure 119.

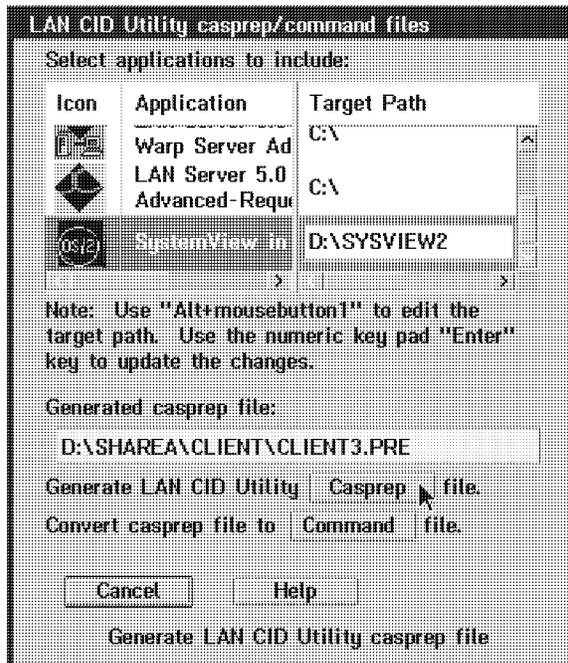


Figure 119. Specifying the Complete Target Path

- d. Now select **Convert casprep file to Command file**. From the Select CASPREP source file window (which is shown in Figure 120 on page 171), select the **CLIENT1.PRE** file you want to convert into a LAN CID Utility client command file.

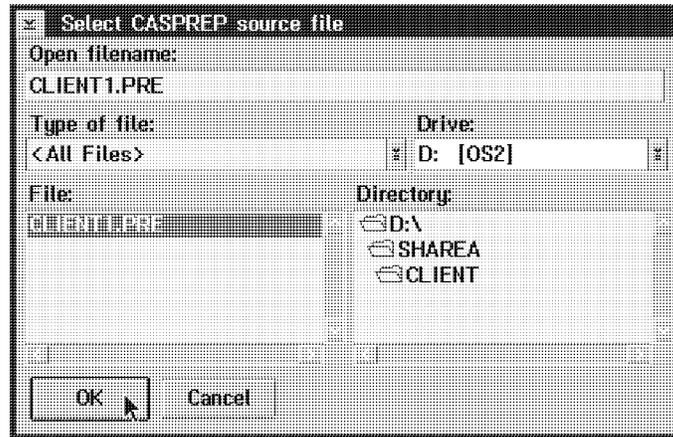


Figure 120. Select CASPREP Source File Window

Select **OK**.

After successful completion, the information window shown in Figure 121 is displayed.

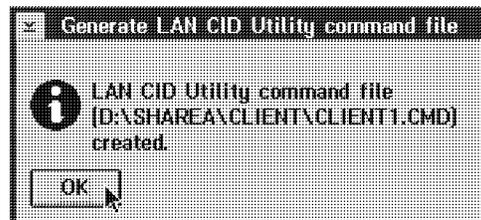


Figure 121. LCU.CMD Information Window

7. Select **Cancel** at the LAN CID Utility casprep/command files window if you are finished with creating client LCU command files.
8. You now may check the newly created client LCU command file for the workstation called CLIENT1. Change to the Code Server's directory to show d: SHAREA CLIENT, and edit the CLIENT1.CMD file.
9. Before you start your remote workstation, you must create product-specific Response Files adapted to the client's needs. See 2.4, "Creating Product-Specific Response Files" on page 172 for more detailed information.

On the OS/2 Warp Server CD-ROM, you can find the following sample response files:

- ASKPSP. \BPIU\ASKPSP\CPINST
- DOS LAN Services 5.0. \CID\CLIENT\DLS
- SystemView Manager \CID\SERVER\SYSVIEW2\SERVER_2
- SystemView Client for OS/2. \CID\CLIENT\SYSVIEW2\CLIENT_2
- SystemView Client for Windows. \CID\CLIENT\SYSVIEW2\CLIENT_W
- LAN Support Program. \CID\SERVER\IBMLS\IBM500L1\SAMPLES
- LAN Distance Connection Server. \CID\SERVER\LDCS\LO296A1
- LAN Distance Remote Server. \CID\SERVER\LDCS\LO296A1
- PSF and PSF Server. \CID\SERVER\PSF2
- Personally Safe'n'Sound. \CID\SERVER\PSNS
- IBM TCP/IP for OS/2 3.0. \CID\SERVER\TCPAPPS
- OS/2 Warp 3.0 \OS2IMAGE

and there are many Response Files for different CID-enabled products in the following directories:

- \CID\SERVER\SYSVIEW2\SERVER_2
- \CID\CLIENT\SYSVIEW2\CLIENT_2
- \CID\SERVER\SYSVIEW2\SERVER_2\NVDI_CLI
- \WARPSRV\OS2CLNT\TABLES
- \WARPSRV\TABLES

10. You may now start your remote workstation with the client boot diskettes. Enter the workstation name CLIENT1 when prompted.

Before installing OS/2 Warp V3.0, be sure that you have previously installed Boot Manager (if you plan to install it), defined partitions, and set the partition where you are going to install the operating system, to *Installable*.

This can be done easily by renaming the file STARTUP.COM of the OS/2 Boot Disk 1. Then boot with the two OS/2 Boot diskettes, and when you get the prompt, type:

```
X:  
CD \EXE\OS2F305  
FDISK
```

2.4 Creating Product-Specific Response Files

This section will describe how to create product specific Response Files. Each product from IBM comes with utilities that create Response Files for you.

Note: In this section, the OS/2 Client's name is always CLIENT1. The DOS Client's name is CLIDOS1.

2.4.1 Definition of a Response File

- A Response File is an ASCII file that supplies the client-specific configuration information required during redirected installation of a product on the client. The Response File contains predefined answers to the configuration questions that users are normally asked during a product installation.
- A Response File contains pairs of keywords and values that are interpreted during a product installation. Usually, these *keyword=value* pairs are unique to a particular product.
- Not all products support the use of a Response File. If the product you are installing does, the Response File makes it unnecessary for you to sit at each client and manually enter an answer to each question that is displayed during installation.
- A Response File is not invoked directly. Instead, a Response File is specified as a parameter value for an installation program. The installation command can be defined in the LAN CID Utility REXX command file or in the change profile for NetView DM/2 2.1. The Response File directs the processing of the installation for a particular product.
- Comments are indicated with an asterisk. Any line beginning with this character will be ignored, blank lines as well.
- Statements do not have to start in the first column.
- Response File statements are not case sensitive.

- Naming conventions:
 - The Response File should always have the same name as the client's workstation name. For example:
 - The workstation's name is: CLIENT1
 - The Response File should be named CLIENT1.RSP
- Note:** If you want to use default Response Files that do not differ from other clients, an OS/2 Response File for instance, then the Response File can be unique to all clients.
- Follow this rule through every product-specific Response File. Response files are stored in their product-specific subdirectories on the Code Server. See the directory discussion in Figure 93 on page 146.

2.4.2 OS/2 Warp 3.0 Response File

In order to get the sample Response File for OS/2 Warp 3.0 and copy it in the CID Tree as a default Response File, you need to perform the following command:

```
COPY F:\OS2IMAGE\SAMPLE.RSP D:\CID\RSP\OS2F305\DEFAULT.RSP
```

Also, copy the file PRDESC.LST from the F: OS2IMAGE PMDD_1 subdirectory to the OS/2 Response File subdirectory, and name the file PRINTER.LST.

```
COPY F:\OS2IMAGE\PMDD_1\PRDESC.LST D:\SHAREA\RSP\OS2F305\PRINTER.LST
```

Also, COPY the file SAMPLE.RSP to, for example, CLIENT1.RSP, and adapt the *keyword=value* pairs to your needs. For example, Table 15 shows *ExitOnError* has been changed from the default. Table 15 discusses *keyword=value* considerations:

Table 15 (Page 1 of 2). OS/2 Keyword=Value Considerations			
Keyword	Default Value	Suggested Value	Comment
BaseFileSystem	1	1	Set this value to 2 if you want to use FAT.
DefaultPrinter	-	-	Edit file PRINTER.LST and notice the line number of the desired printer. The line number is equal to the DefaultPrinter number.
DiagnosticAids	1	1	Leave this value as it is since FFST/2 needs diagnostic aids, and therefore, all other products like LAN Server, DB2/2, CM/2, and so forth, do also.
ExitOnError	0	1	This setting is required so that the SDM can get control after the installation is completed.
Fonts	1	1	Leave this setting as it is, especially if you plan to use CM/2 on the workstation.
FormatPartition	0	1	Set this value to 0 only if you want to migrate the operating system.
RebootRequired	0	0	This setting is required so that the SDM reboots the workstation instead of the SEINST program.

<i>Table 15 (Page 2 of 2). OS/2 Keyword=Value Considerations</i>			
Keyword	Default Value	Suggested Value	Comment
REXX	1	1	LAN CID Utility requires this setting. REXX is required whenever you want to execute REXX commands, whether remotely or locally.

The OS/2 Warp 3.0 Response File we used in our scenarios is shown in Figure 122.

```

AlternateAdapter=0
APM=0
BaseFileSystem=1
CDROM=
SCSI=1
ConfigSysLine=SET RestartObjects=StartupFoldersOnly
ConfigSysLine=PauseOnError=NO
CountryCode=001
CountryKeyboard=US
DefaultPrinter=115
DiagnosticAids=1
DisplayAdapter=0
Documentation=1
DOSSupport=1
WIN-OS/2Support=1
DPMI=1
ExitOnError=1
Fonts=1
FormatPartition=1
MigrateApplications=C:\OS2\INSTALL\DATABASE.DAT
MigrateConfigFiles=0
MoreBitmaps=1
Mouse=1
MousePort=0
OptionalFileSystem=1
OptionalSystemUtilities=1
PCMCIA=1
PrimaryCodePage=1
PrinterPort=1
ProcessEnvironment=1
ProgressIndication=1
RebootRequired=0
REXX=1
SerialDeviceSupport=1
ToolsAndGames=1

```

Figure 122. Response File for the OS/2 2.11 Base System Installation

Note: There are two new lines we have chosen to add to the CONFIG.SYS file of OS/2 Warp 3.0 once installed. These lines are:

- ConfigSysLine=SET RestartObjects=StartupFoldersOnly, and
- ConfigSysLine=PauseOnError=NO

The first one makes only the applications included in the Startup Folder or in the file STARTUP.CMD start when OS/2 starts. The second one allows the starting process of OS/2 to continue despite errors within the CONFIG.SYS file. If this line is not included, the CONFIG.SYS process waits for the user to press a key before continuing to the next line in the CONFIG.SYS file. You may wish to add other lines in CONFIG.SYS in addition to these.

2.4.3 Multiprotocol Transport Services Response File

In order to get a complete Multiprotocol Transport Services Response File, you may use the LAPSRSP utility, which extracts the settings of a current installation.

Note: The LAPSRSP utility does not extract TCP/IP configuration settings.

```
--F:\CID\SERVER\MPTS\LAPSRSP\IBMCOM\PROTOCOL.INI-----  
--d:\SHAREA\RSP\MPTS50\CLIENT\TRSP-I:PRODUCT/U:NEW-----
```

Or, you may use and adapt sample Response Files that are delivered in the SAMPLES directory on the third MPTS diskette. Insert the diskette in drive A:, and issue the following command from an OS/2 command line:

```
--PKUNZIP2-A:\SAMPLES\SAMPLES-DIR\SHAREA\RSP\MPTS\SAMPLES-----
```

The following sample Response File configures an IBM Token-Ring Network adapter driver that binds to the IEEE802.2 and NetBIOS protocol drivers.

```
INST_SECTION = (  
  TARGET = D:  
  INSTALL = PRODUCT  
  UPGRADE_LEVEL = NEW  
)  
PROTOCOL = (  
  [PROT_MAN]  
    DRIVERNAME = PROTMAN$  
  [IBMLXCFG]  
    LANDD_nif = LANDD.nif  
    NETBEUI_nif = NETBEUI.nif  
    IBMTOK_nif = IBMTOK.nif  
  [NETBIOS]  
    DriverName = netbios$  
    ADAPTER0 = netbeui$,0  
  [LANDD_nif]  
    DriverName = LANDD$  
    Bindings = IBMTOK_nif  
    ETHERAND_TYPE = "I"  
    SYSTEM_KEY = 0x0  
    OPEN_OPTIONS = 0x2000  
    TRACE = 0x0  
    LINKS = 8  
    MAX_SAPS = 6  
    MAX_G_SAPS = 0  
    USERS = 6  
    T1_TICK_G1 = 255  
    T1_TICK_G1 = 15  
    T2_TICK_G1 = 3  
    T1_TICK_G2 = 255  
    T1_TICK_G2 = 25  
    T2_TICK_G2 = 10  
    IPACKETS = 250  
    UIPACKETS = 100  
    MAXTRANSMITS = 6  
    MINTRANSMITS = 2  
    TCBS = 64  
    GDTS = 30  
    ELEMENTS = 1200
```

Figure 123 (Part 1 of 2). MPTS Response File IEEE 802.2 and NetBIOS Protocol Drivers

```

[NETBEUI_nif]
  DriverName = netbeui$
  Bindings = IBMTOK_nif
  ETHERAND_TYPE = "I"
  USEADDRREV = "YES"
  OS2TRACEMASK = 0x0
  SESSIONS = 130
  NCBS = 225
  NAMES = 21
  SELECTORS = 15
  USEMAXDATAGRAM = "NO"
  ADAPTRATE = 1000
  WINDOWERRORS = 0
  MAXDATARCVCV = 4168
  TI = 30000
  T1 = 1000
  T2 = 200
  MAXIN = 1
  MAXOUT = 1
  NETBIOS_TIMEOUT = 500
  NETBIOS_RETRIES = 2
  NAMECACHE = 1000
  RNDOPTION = 0
  PIGGYBACKACKS = 1
  DATAGRAMPACKETS = 10
  PACKETS = 350
  LOOPPACKETS = 8
  PIPELINE = 5
  MAXTRANSMITS = 6
  MINTRANSMITS = 2
  DLCRETRIES = 10
  FCPRIORITY = 5
  NETFLAGS = 0x0
[IBMTOK_nif]
  DriverName = IBMTOK$
  ADAPTER = "PRIMARY"
  NETADDRESS = "4000638700AB"
  MAXTRANSMITS = 6
  RECVBUFS = 2
  RECVBUFSIZE = 256
  XMITBUFS = 1
)

```

Figure 123 (Part 2 of 2). MPTS Response File IEEE 802.2 and NetBIOS Protocol Drivers

Note: If you are using a locally administered address, adapt the NETADDRESS statement. Otherwise, delete the line.

The following sample Response File configures an IBM Token-Ring Network adapter driver bound to the TCP/IP, TCPBEUI and NetBIOS protocol drivers. NETBEUI is configured for logical adapter 0, and TCPBEUI is configured for logical adapter 1.

```

INST_SECTION = (
  UPGRADE_LEVEL = NEW
  TARGET = D:
  INSTALL = PRODUCT
)

```

Figure 124 (Part 1 of 3). MPTS Response File TCP/IP, TCPBEUI and Native NetBIOS

```

PROTOCOL = (
[PROT_MAN]
  DRIVERNAME = PROTMAN$
[IBMLXCFG]
  NETBEUI_nif = NETBEUI.nif
  TCPBEUI_nif = TCPBEUI.nif
  TCPIP_nif = TCPIP.nif
  IBMTOK_nif = IBMTOK.nif
[NETBIOS]
  DriverName = netbios$
  ADAPTER0 = netbeui$,0
  ADAPTER1 = tcpbeui$,1
[NETBEUI_nif]
  DriverName = netbeui$
  Bindings = IBMTOK_nif
  ETHERAND_TYPE = "I"
  USEADDRREV = "YES"
  OS2TRACEMASK = 0x0
  SESSIONS = 130
  NCBS = 225
  NAMES = 21
  SELECTORS = 15
  USEMAXDATAGRAM = "NO"
  ADAPTRATE = 1000
  WINDOWERRORS = 0
  MAXDATARCV = 4168
  T1 = 30000
  T1 = 1000
  T2 = 200
  MAXIN = 1
  MAXOUT = 1
  NETBIOS_TIMEOUT = 500
  NETBIOSRETRIES = 2
  NAMECACHE = 1000
  RNDOPTION = 0
  PIGGYBACKACKS = 1
  DATAGRAMPACKETS = 10
  PACKETS = 350
  LOOPPACKETS = 8
  PIPELINE = 5
  MAXTRANSMITS = 6
  MINTRANSMITS = 2
  DLCRETRIES = 10
  FCPPRIORITY = 5
  NETFLAGS = 0x0
[TCPBEUI_nif]
  DriverName = tcpbeui$
  Bindings = ,IBMTOK_nif
  OS2TRACEMASK = 0x0
  SESSIONS = 40
  NCBS = 95
  NAMES = 21
  SELECTORS = 5
  USEMAXDATAGRAM = "NO"
  NETBIOS_TIMEOUT = 500
  NETBIOSRETRIES = 2
  NAMECACHE = 0
  PRELOADCACHE = "NO"
  NAMESFILE = 0
  DATAGRAMPACKETS = 20
  PACKETS = 50

```

Figure 124 (Part 2 of 3). MPTS Response File TCP/IP, TCPBEUI and Native NetBIOS

```

[TCPIP_nif]
  DriverName = TCPIP$
  Bindings = IBMTOK_nif
[IBMTOK_nif]
  DriverName = IBMTOK$
  ADAPTER = "PRIMARY"
  MAXTRANSMITS = 6
  RECVBUFS = 2
  RECVBUFSIZE = 256
  XMITBUFS = 1
)
MPTS = (
[CONTROL]
  Local_IPC      = YES
  INET_Access    = YES
  NETBIOS_Access = NO
[IFCONFIG]
  Interface      = 0
  Address        = 2.2.2.2
  Brdcast        =
  Dest           =
  Enable         = UP
  Netmask        = 3.3.3.3
  Metric         = 0
  Mtu            = 1500
  Trailers       = YES
  Arp            = YES
  Bridge         = YES
  Snap           = YES
  Allrs          = YES
  802.3          = YES
  Icmpred        = YES
  Canonical      = YES
[ROUTE]
  Type           = default
  Action         = add
  Dest           =
  Router         = 4.4.4.4
  Metric         = 1
)

```

Figure 124 (Part 3 of 3). MPTS Response File TCP/IP, TCPBEUI and Native NetBIOS

2.4.4 NetView DM/2 Change Control OS/2 Client Response File

There are sample Response Files for NetView DM/2 CC OS/2 Client installation on the last diskette of NetView DM/2 2.1, labeled Documentation Samples. Only two keywords are necessary to mention. In our test environment, we used the NetView DM/2 CC OS/2 Client Response File shown in Figure 125.

```

ServerName=FLORIDA
ClientName=CLIENT1

```

Figure 125. Response File for the NetView DM/2 CC OS/2 Client Installation

2.4.5 OS/2 LAN Server 5.0 Response File

Use the LANINSTR command to create an OS/2 LAN Server 5.0 Response File for a requester or a server. Change to the Code Server's subdirectory d: CID SERVER IBMLS and invoke:

```
--LANINSTR-/SRV-----
```

Go the tailored installation/configuration path. Depending on the type of client, select **Create Requester Response File for remote installation** or **Create Server Response File for remote installation**. Go through all panels as you would when installing the workstation itself.

Note: If you want the target workstation to be migrated from a previous release, you need to select: **Use target settings**.

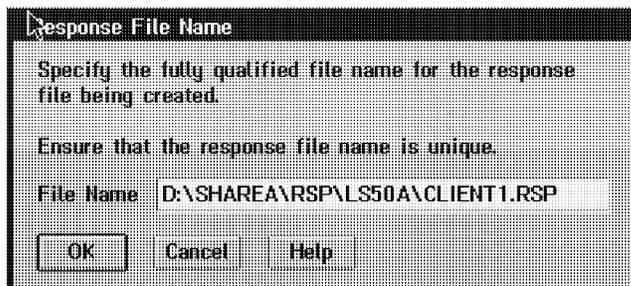


Figure 126. Generating an IBM LAN Server 5.0 Response File

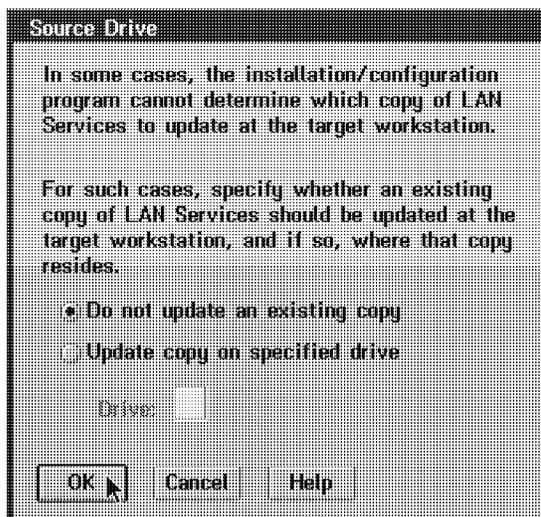


Figure 127. IBM LAN Server 5.0 Response File Source Drive

The Response File shown in Figure 128 on page 180 is intended for a remote installation of an OS/2 LAN Server 5.0 Requester.

```

DELETEIBMLAN = Networks<
  net2 =
  net3 =
  net4 =
  netlb =
>
UPDATEIBMLAN = Networks<
  net1 = NETBEUI$,*,LM10,*,*,*
>
DELETEIBMLAN = Requester<
  wrknets = NETLB,NET2,NET3,NET4
>
UPDATEIBMLAN = Requester<
  Computername = PIPPOSRV
  Domain = PIPPODOM
  useallmem = No
>
ADDIBMLAN = Requester<
  wrkservices = MESSENGER
  wrknets = NET1
>
DELETEIBMLAN = Server<
  srvservices = REMOTEBOOT
  srvnets = NETLB,NET2,NET3,NET4
>
UPDATEIBMLAN = Server<
  autopath = D:\IBMLAN\PROFILES\SRVAUTO.PRO
>
ADDIBMLAN = Server<
  srvservices = ALERTER,DCDBREPL,GENALERT,LSSERVER,NETLOGON,NETRUN,REPLICATOR,TIMESOURCE
  srvnets = NET1
>
Config386Cache = Migrate
ConfigApplDumpPath = D:\OS2\SYSTEM
ConfigApplMaxDumps = 32
ConfigAutoStartFFST = Yes
ConfigAutoStartLS = Yes
ConfigCopyDLR = CopyIfRequired
ConfigCopyLSP = CopyIfRequired
ConfigDisplayMSG = OFF
ConfigDosNumber = 0
ConfigHeap = Migrate
ConfigInitializeDCDB = YES
ConfigLazyWrite = Migrate
ConfigMsgLogName = D:\OS2\SYSTEM\OS2MLOG.DAT
ConfigRouteAlertsTo = NETVIEW
ConfigServerType = DomainController
ConfigSourceDrive = None
ConfigSystemDumpPath = D:\OS2\SYSTEM
ConfigSystemMaxDumps = 32
ConfigTargetDrive = D
ConfigUpsPort = COM2
ConfigUseAllMem = No
ConfigWsId = 00000000
ConfigWsSerial1 = 00
ConfigWsSerial2 = 0000000
ConfigWsType1 = 0000
ConfigWStype2 = 000
Install386HPFS = INSTALL
InstallAPI = INSTALL
InstallDosLanApi = INSTALL
InstallDosRemoteIPL = REMOVE
InstallFaultTolerance = INSTALL
InstallFFST = INSTALL
InstallGenericAlerter = INSTALL
InstallInstallProgram = INSTALL
InstallLocalSecurity = INSTALL
InstallLoopBackDriver = INSTALL
InstallMigrationImportUtil = REMOVE
InstallOS2RemoteIPL = REMOVE
InstallServer = INSTALL

```

Figure 128. Response File for the OS/2 LAN Server 5.0 Server Installation

```
InstallUPM = INSTALL
InstallUps = INSTALL
InstallMSGPopup = INSTALL
InstallGUI = INSTALL
InstallClipboard = INSTALL
InstallDesktopIcons = YES
```

Figure 129. Response File for the OS/2 LAN Server 5.0 Requester Installation

2.4.6 NetView DM/2 CC DOS Client Response File

There are sample Response Files for NetView DM/2 CC DOS Client installation on the last diskette of NetView DM/2 2.1 labeled "Documentation Samples". Only two keywords (listed in the figure below) are necessary to mention. In our test environment, we used the DOS LAN Support Program 1.36 Response File shown in Figure 130.

```
ServerName=FLORIDA
ClientName=CLIDOS1
```

Figure 130. Response File for the NetView DM/2 CC DOS Client Installation

The DOS CC Client only works properly with the DOS LAN Support Program loaded. Therefore, you need to include the `install_802` keyword and set its value to `yes`. Otherwise, the DOS workstation will not be able to load the CC Client.

2.4.7 SystemView in Warp Server Manager Response File

Figure 131 on page 182 shows an example of a SystemView in Warp Server Manager Response File. The template comes with variables identified by `$(description)`.

When you find these variables, it is mandatory to enter information.

```

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;;
;;          SystemView Response File          ;;
;;
;;          It is automatically generated by the CIDPrep Configuration Process
;;
;;          WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING
;; -----
;; Workstation specific variables are enclosed between $( and ); for
;; each of these variables you are required to specify a value before
;; using the Response File.
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

;;
;; DESCRIPTION: SystemView Server sample configuration
;;
;;

; Target path
; It is the path where the product will be installed on the
; target machine.
FILE = D:\SYSVIEW2

; Work area
; It is the path for the data directory
WORK = D:\SYSVIEW2\WORK

; SystemView components to install
COMP = License Use Runtime Server
COMP = Software Distribution Object Preparation
COMP = SystemView Administrator Console
COMP = SystemView Documentation IPF format (.INF)
COMP = SystemView Documentation Bookmanager format
COMP = Software Distribution Server

DELETEBACKUP = No
SAVEBACKUP = Yes
CFGUPDATE = Auto
OVERWRITE = No

; SystemView System Name. This identify the system in the network
; mandatory
SystemName = ENRIQUEVIEW

; Network drivers and Network addresses
; You may specify five types of Driver keywords. The value used is 1 or 0.
; Parm1 keyword is required for NetBIOS, NBALT and SERIPC Driver.
; mandatory
: Driver.TCPIP = 1
Driver.NETBIOS = 1
Parm1.NETBIOS = TEST
; Driver.NBALT = 0
; Parm1.NBALT = $(Parm1_NetBios_Alternate)
; Driver.IPX = 1
; Driver.SERIPC = 1
; Parm1.SERIPC = $(Parm1_SERIPC)

; Force remote logons. The value used is 1 to disable PUBLIC access or 0
; The default is 0
; ForceRemoteLogons = 0

; Service alerts. The value used is 1 to generate the alert or 0.
; The default is 0
; ServiceAlerts = 0

```

Figure 131 (Part 1 of 4). Response File for the SystemView Manager Remote Installation

```

; Network predefined filters. You can specify up to eight keywords, entering
; them as Keyword.1, Keyword.2... Keyword.8
Keyword.1 = ITSO

; Network timeout. Defines the time-out period, in seconds, a SystemView
; managing application waits for client response. Default value is 15
; NetTimeout = 15

; Distribution directories
; Substitute the $(File1) with the target path.
; You can specify other paths if you want.
Repository = D:\SYSVIEW2\REPOS
WorkArea = D:\SYSVIEW2\WORK
BackupArea = D:\SYSVIEW2\BACKUP
ServiceArea = D:\SYSVIEW2\SERVICE

; NetBIOS adapter. The value used is 1 (Alternate NB Adapter) or 0 (Primary
; NB Adapter)
NBAdapter = 0

; Remote Workstation Control Configuration

; Specifies whether the client workstation can end a session with a Remote
; Control Manager or not (1, 0)
; RWC.CanTerminate = 1

; Specifies whether the Remote Control Manager controls the keyboard and mouse
; input and monitors the display output of the client or views the client
; display but does not control the client input (1, 0)
; RWC.StartMonitor = 1

; Is the interval between updates of your screen are sent to the Remote Control
; Manager display. The range, in multiples of one hundred, is expressed in
; milliseconds (100, 200, ...3000)
; RWC.TimeRefresh = 300

; Application Sharing Configuration

; Enables the workstation to access shared applications from a remote file
; server (1, 0)
; SHA.Enabled = 1

; Specifies the type of redirector use to communicate with the remote file
; server (IBM for IBM LAN Requester, NW for Netware Requester, NFS for NFS
; Client)
; mandatory if SHA.Enabled=1
; SHA.NOS = NFS

; Specifies the logon ID with which access the remote file server application
; mandatory if SHA.Enabled=1 and SHA.NOS=NW
; SHA.Userid = UserID

; Specifies the remote file server and path where the application is installed
; mandatory if SHA.Enabled=1
; SHA.RemoteName = RemoteName

; mandatory if SHA.Enabled=1
; SHA.RemoteDrive = Z:

; Values to configure License Use Runtime Client and Server
; General keywords

; Specifies the Client or Server configuration (client, server)
; mandatory to perform License Use Runtime configuration with
; the following LIC.Keywords
; LIC.ConfigureAs=server

```

Figure 131 (Part 2 of 4). Response File for the SystemView Manager Remote Installation

```

; Default to SystemName keyword
; LIC.Username=$(SystemName)

; Any number of words
; Default to systemviewgroup value
; LIC.Usergroup=systemviewgroup

; Network drivers used (tcpip, NetBIOS, both). Default to tcpip.
; It is recommended the value both or tcpip if TCP/IP is running.
; LIC.Transport=tcpip

; NetBIOS machine name.
; Can be set if LIC.Transport is NetBIOS or both.
; LIC.Machname=$(Parm1_NetBIOS)

; Concurrent Nodelock log file name
; LIC.LogFile=C:\ifor\ls\conf\logfile

; Concurrent Nodelock logging level.
; 0 means: no logging
; 1 means: log all delete/add/update licenses
; 2 means: log only not granted licenses
; 3 means: 1 + 2
; 4 means: log all events
; LIC.LogLevel=3

; Concurrent Nodelock max number of messages in log
; LIC.LogMsgsMaxNum=10000

; Concurrent Nodelock licenses installed flag (yes, no)
; LIC.ConcurrentNodelock=yes

; LAN Adapter (0, 1)
; LIC.LanAdaptor=0

; Number of NetBIOS NCBs, the recommended value is 40
; LIC.NCBS=40

; Server-only keywords

; Configure the server as a new Global Location
; Broker in a new cell or as a replicate of another
; Global Location Broker in the same cell (replicate, new)
; LIC.Create=new

; Transport used by Global Location Broker (ip, NetBIOS)
; mandatory if LIC.Create=new
; LIC.Family=ip

; Run Global Location Broker flag (yes, no).
; Mandatory yes if LIC.Create=new
; LIC.RunGLBD=yes

; Run Ally flag (yes, no)
; LIC.RunAlly=no

; Disable remote administration flag (yes, no)
; LIC.DisableRemoteAdmin=no

; LIC.ServLogFile=C:\ifor\ls\conf\log_file

; LIC.LogAllEvents=yes

; Log the license granting (yes, no)
; LIC.LogGrant=yes

```

Figure 131 (Part 3 of 4). Response File for the SystemView Manager Remote Installation

```

; Log license checkin (yes, no)
; LIC.LogCheckin=no

; Log the license wait (yes, no)
; LIC.LogWait=no

; Log Vendor added/deleted (yes, no)
; LIC.LogVendor=no

; Log Product added/deleted (yes, no)
; LIC.LogProduct=no

; Log license timeout (yes, no)
; LIC.LogTimeout=no

; LIC.LogErrors=no

; Log Vendor messages (yes, no)
; LIC.LogVendorMsg=no

; Log Server start/stop (yes, no)
; LIC.LogSvrStartStop=no

```

Figure 131 (Part 4 of 4). Response File for the SystemView Manager Remote Installation

2.5 SystemView Software Distribution

In this section, we describe the Software Distribution component of SystemView. Software Distribution supports the installation of applications that are CID-enabled and non-CID-enabled. While the process of Software Distribution is somewhat similar to that of CASSETUP, SystemView Software Distribution has many additional functions that are not available with CASSETUP. Some of the main functions of SystemView Software Distribution are listed below:

- Easy to use graphical interface
- Software preparation processes for CID- and non-CID-enabled applications
- Support to remove or deinstall applications is included
- Support for installation with deferred activation
- Support for installation with corequisites
- Variable translation on the target workstation at installation time
- User at workstation can initiate software installation via GUI
- Catalog of installed software is maintained on each machine

2.5.1 Software Distribution Components

Software Distribution consists of a number of logical components. These components are embedded within the SystemView options that are available on installation. Below is a list of Server- and Client-related components that can be installed:

- **SystemView Manager**
 1. Software Distribution Server

The Software Distribution Server maintains a catalog of all software objects and sharable applications. This catalog is used to process all the Software Distribution requests. Both the Software Distribution graphical

and command line interfaces are available on the Software Distribution Server. From this server, software can be installed on all managed OS/2 and Windows systems. This component is installed when you select the **Software Distribution Server** when installing SystemView.

2. Software Distribution User Interface (Manager)

This user interface has both the graphical and command line interfaces available. Using this interface, this machine can distribute software to all managed OS/2 and Windows systems. This interface is installed when you select the **SystemView Administrator Console**.

3. Software Distribution Object Preparation

This component provides an easy way to prepare CID- and non-CID-enabled software packages. It is a selectable feature on both Software Distribution Server and client machines. To install this component select **Software Distribution Object Preparation**.

4. Software Distribution Agent

This component actually processes the install requests and is installed by default on all SystemView machines. It reports the result to the Software Distribution Server and starts at machine startup.

• **SystemView Client**

1. Software Distribution User Interface (Client)

This user interface has both the graphical and command line interfaces available. However, this machine can only install software objects from the catalog if it is authorized for that object. This interface is installed when you select the **SystemView Client Graphical Interface**.

2. Software Distribution Base Client

This base client does not have the Software Distribution graphical user interface present. It can only be managed by an administrator and cannot issue install requests. This component is installed when you select the **SystemView Client**.

3. Software Distribution Object Preparation

As described previously, this component provides an easy way to prepare CID- and non-CID-enabled software packages. It is a selectable feature on both Software Distribution Server and Client machines. Software can be prepared for distribution on the client machines and then cataloged on the server for distribution. To install this component, select **Software Distribution Object Preparation**.

4. Software Distribution Agent

As described in the SystemView Manager above.

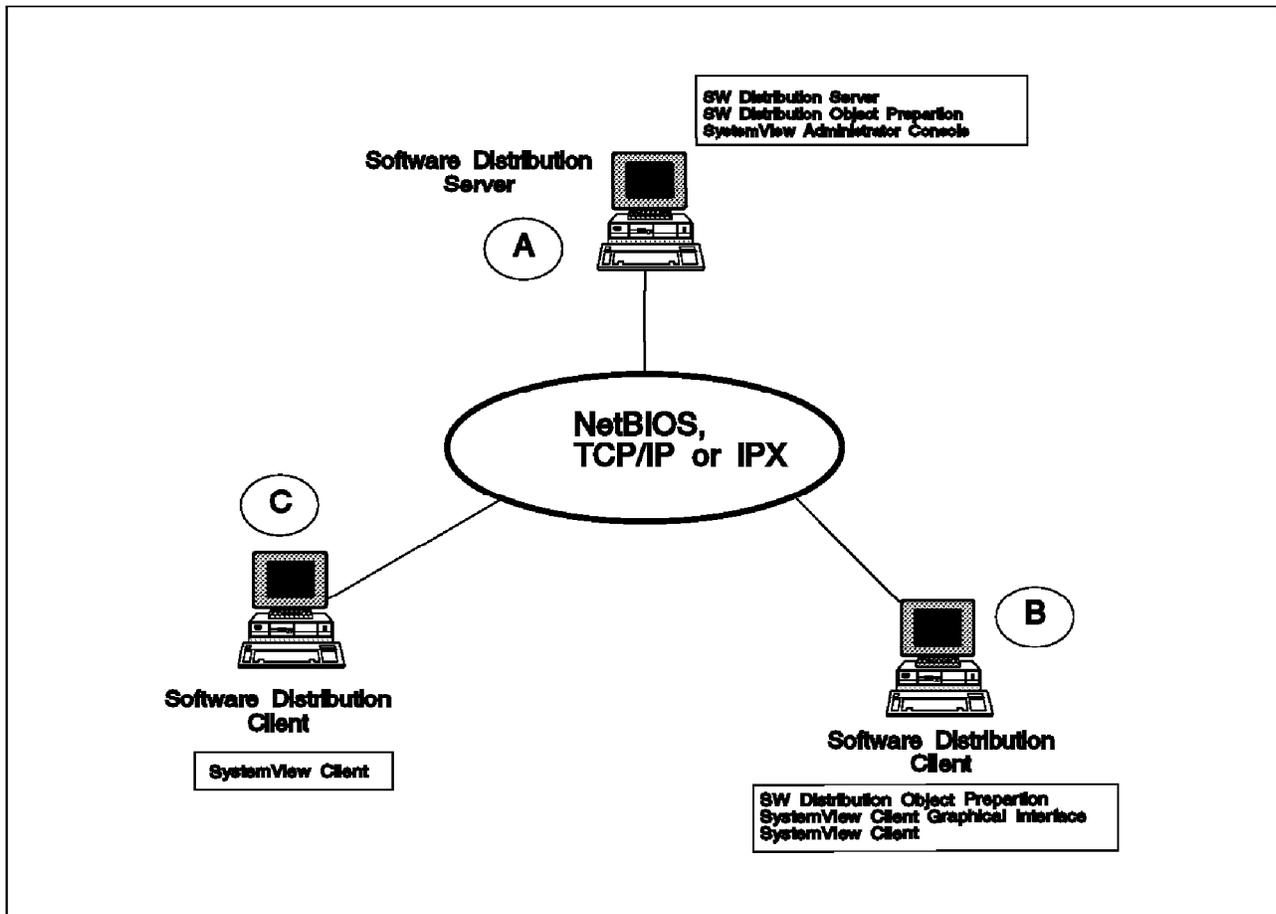


Figure 132. Software Distribution Topology

Figure 132 shows a simple scenario with a single Distribution Server **A** and two Distribution Clients **B** and **C**.

The administrator is able to install, configure, and distribute software from the Distribution Server **A**. All the components required to do this are listed in the figure.

From the first Distribution Client **B**, the administrator can prepare software for distribution. Once the software is prepared, it is cataloged on the Distribution Server **A**. The user at client **B** can also request to install software from the distribution server **A** that they have been authorized for.

From the second distribution client **C** the user cannot do anything other than wait for the administrator to initiate installation of software on the workstation.

2.5.2 System Requirements

Communication with the Software Distribution Server and the Software Distribution Client requires one of the following protocols:

- IPX/SPX

This requires the NetWare OS/2 Requester 2.11 or later to be installed on the Software Distribution Server and on OS/2 Software Distribution Clients.

- NetBIOS

You should have at least IBM LAN Adapter and Protocol Support (LAPS) - CSD WR07060

- TCP/IP
 - IBM TCP/IP for DOS Version 2.1
 - IBM TCP/IP for OS/2 Version 2.x with CSD UN64092 or Version 3.0

The following operating systems support the listed components:

- OS/2 Warp
 - Software Distribution Server
 - Software Distribution Base Client
 - Software Distribution Graphical User Interface
 - Software Distribution Command Line
 - Software Distribution Agent
 - Software Preparation Site (CID and non-CID)
- OS/2 2.11 and Windows 3.1 (with IBM DOS 6.3, 7.0 or MS-DOS 6.2)
 - Software Distribution Base Client
 - Software Distribution Graphical User Interface
 - Software Distribution Command Line
 - Software Distribution Agent
 - Software Preparation Site (CID and non-CID)

2.5.3 Prerequisite Tasks

This section describes the prerequisite tasks that need to be performed before software can be prepared. Since there can be many permutations of where the Software Distribution components are installed, we will describe the scenario as depicted in Figure 133 on page 189.

Note: If you are distributing only non-CID-enabled applications, you do not have to complete steps 6 through 9. These steps are required only for the preparation and installation of CID-enabled applications.

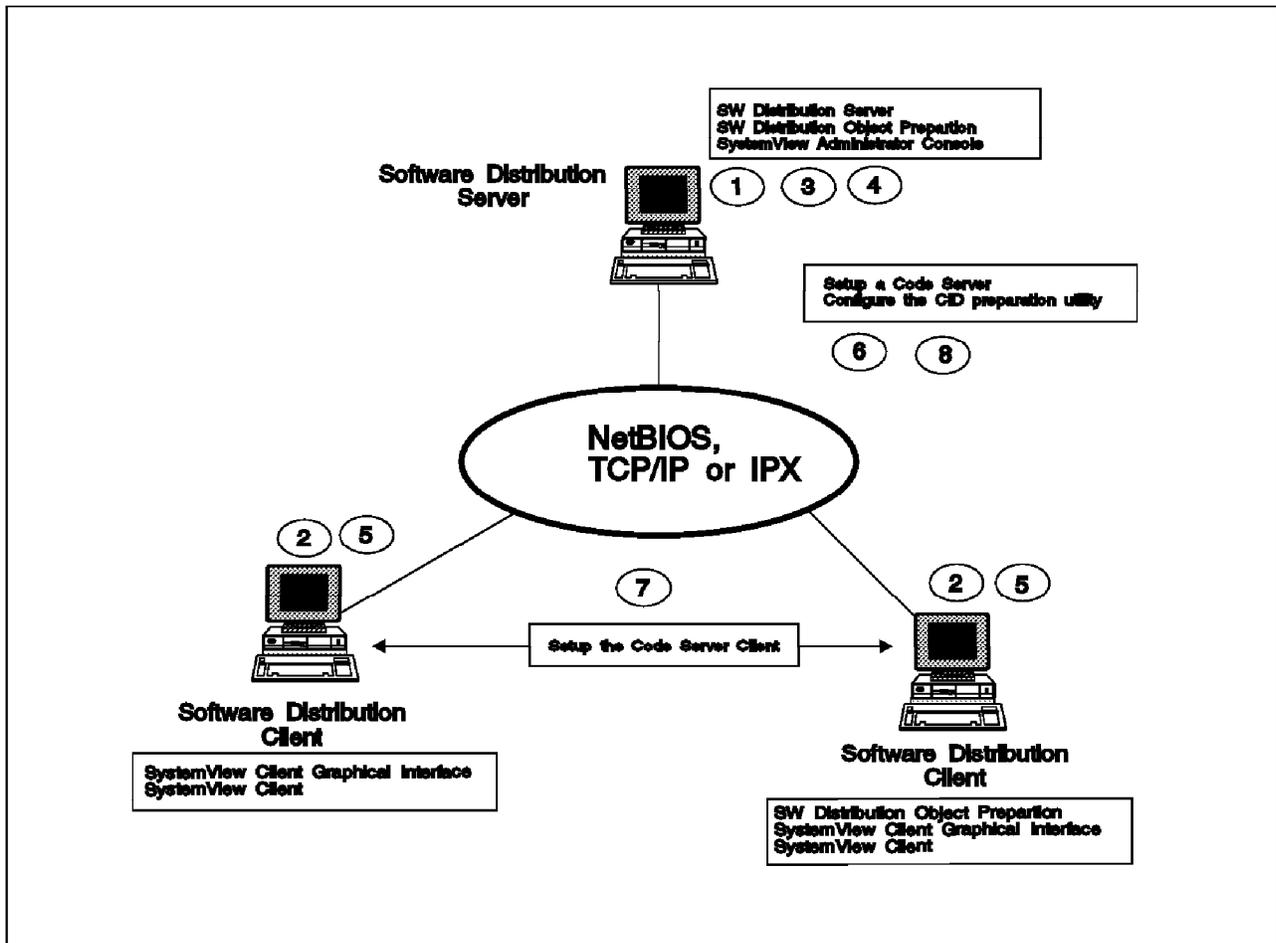


Figure 133. Prerequisite Tasks for Software Preparation

The tasks below describe the order of the configuration in Figure 133.

1. Install and Configure the Software Distribution Server

For the scenario as depicted in Figure 133, the following components need to be selected when installing the Software Distribution Server.

- Software Distribution Server
- Software Distribution Object Preparation
- SystemView Administrator Console

Figure 134 on page 190 shows the available options when installing a SystemView Manager.

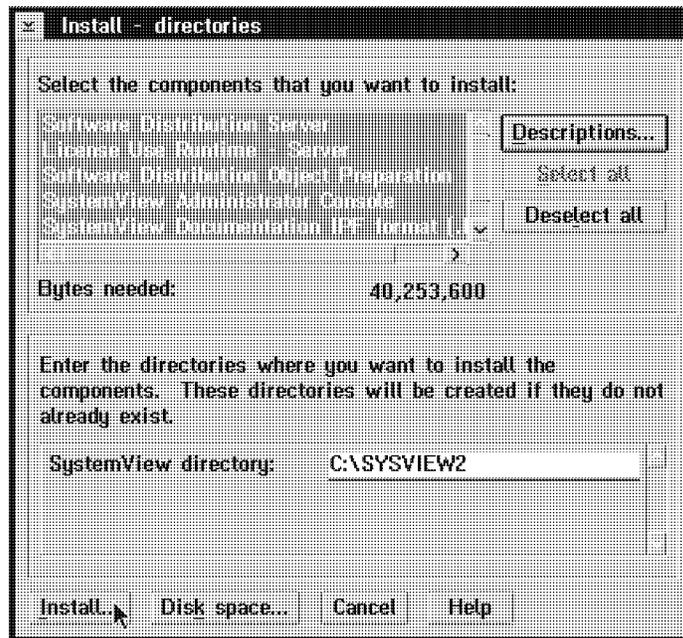


Figure 134. SystemView Manager Configuration Page

The SystemView installation program creates the following directories within the SYSVIEW2 directory:

- **BACKUP**
Contains backup copies of software objects.
- **BIN**
All the executable code and the software object's INI files are stored here.
- **REPOS**
Software objects that are created are stored here.
- **SERVICE**
Software objects that are installed with the activation option are stored here. The software object will remain here until the object is activated.
- **UICFG**
A file containing information about the last Software Distribution Server connection.
- **WORK**
The working area for the Software Preparation Utilities.
- **DB**
The Software Distribution database data is contained in this directory.
- **QUEUE**
Secure queues to hold the input data.
- **CFGS**
Application Definition Files and Configurations.
- **SWLIB**

The software library container.

Configuration for the Software Distribution Server is done through the SystemView Configuration Notebook. The protocols that you wish to choose for Software Distribution are selected on the first page of the SystemView Configuration Notebook. A Software Distribution Server can support more than one protocol, but a Software Distribution Client can only support a single protocol. Ensure the protocols you choose allow distribution to all clients. In our case, we are only using NetBIOS.

The second page contains the configuration for the Software Distribution Server. See Table 16 for a list and description of the parameters.

This configuration will be presented during installation, but can be accessed after installation by double-clicking on the SystemView Configuration icon within the SystemView folder. The Software Distribution Server is shown in Figure 133 on page 189. The configuration page is shown in Figure 135.

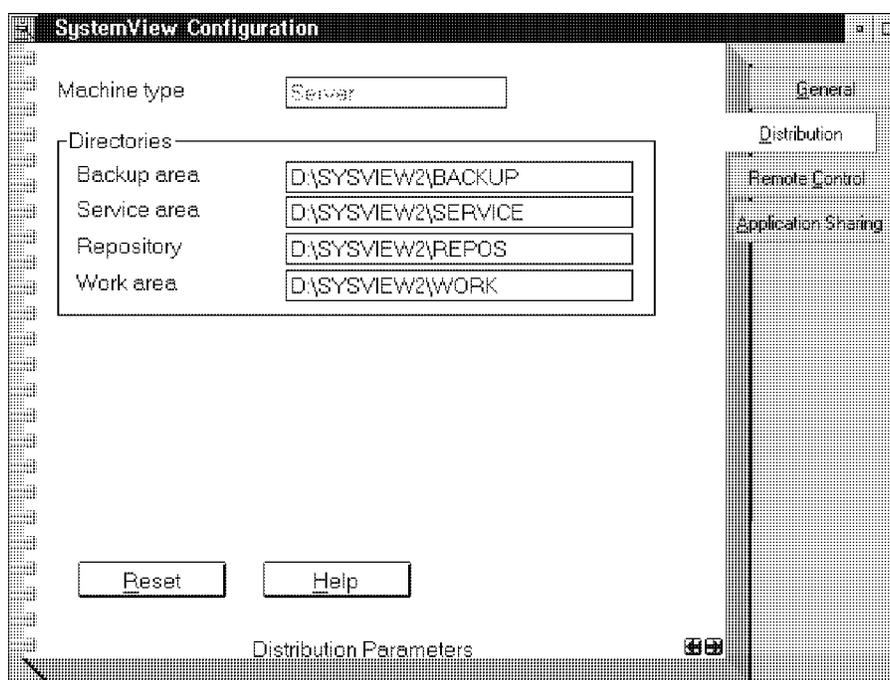


Figure 135. Configuration Page for Software Distribution

This configuration information is stored in the NVDM.CFG file in the SYSVIEW2 directory.

<i>Table 16 (Page 1 of 2). Software Distribution Configuration File</i>	
Configuration Keyword	Description
Workstation Name	The workstation identifier in the form of System_name.Protocol_Type.Network_Address.
Server	The Name, the Protocol Type, and the Network Address (NetBIOS Alias, TCP/IP Hostname, IPX Internetwork Address) of the server to be connected to. On a server machine, this field contains the System Name only.

<i>Table 16 (Page 2 of 2). Software Distribution Configuration File</i>	
Configuration Keyword	Description
Protocol	The protocol used to connect to the server can be IPX, TCP/IP or NetBIOS. Only one protocol at a time is supported on the client, while the server provides multiprotocol support.
Repository	The directory where the software object is stored.
Work Area	The work directory of the product.
Backup Area	The directory where the backup copies of the software object is used when uninstalling.
Service Area	The directory where the software objects installed that require activation are stored.
Configuration	The possible values here are Server, Client or Client_Manager (Administrator Console).
Message Log Level	The actual logging level set for this machine (minimal, normal, diagnostic).
Log File Size	The maximum size of the file FNDLOG. Default value is 64000 bytes.
API Trace File Size	The maximum size of the file FNRBAPI, where the RB API traces are stored. The default value is 64000.
Trace File Size	The maximum size of the file FNDTRCx, where the product traces are stored. The default value is 64000.
Max User Interfaces	This is the maximum number of UI concurrently supported by the server.
Target Mode	This is the target level of authorization. It is set for PULL for the client and PUSH for the manager.
Target Address	This contains the target address of the machine. This value is specified during configuration.
Machine Type	This is a description of the machine operating system (OS/2 or Windows).
Max Attempts	This is the maximum number of attempted logons before the user ID needs to be reset. This parameter is not used.
Manager-Only Keywords	
Authorize_Mode	The default is NONE for every pull target, meaning the clients are not authorized to the software object they have not prepared. The value ALL allows the client to access new software objects.
LAN Authorization	Values are 0 or 1. The default is 0. If it is set to 1, there is a security check done using the address of the adapter. The server then needs to have a list of all adapters allowed.
DACA Retry Time	This sets the interval time when the server tries to contact the client. The value is in seconds, and the default is 300 seconds. The maximum value is 32767 seconds.
Automatic Target Registration	The possible values are YES and NO. If set to YES (default), the target registration is automatically performed the first time a client connects to the server.
Max Targets	This is the maximum number of targets that can be configured. The default is 5.

2. Installing the Distribution Clients

The following components are automatically installed when installing from the OS/2 Warp Server CD.

- SystemView Client
- Software Distribution Object Preparation

Figure 136 shows the OS/2 Client installation options. The Windows client options are the same.

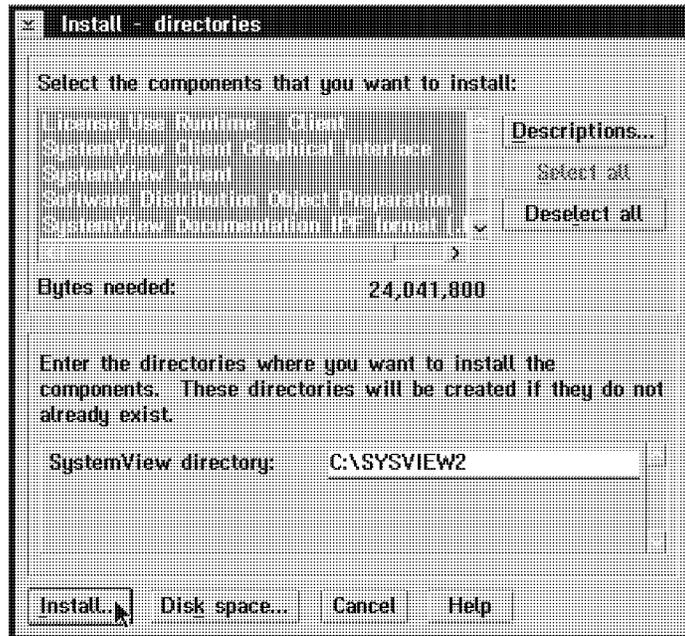


Figure 136. SystemView Client Configuration Page

Configuration for the Software Distribution Client is done through the SystemView Configuration Notebook. The second page contains the configuration for the Software Distribution Client. This configuration will be presented during installation, but can be accessed after installation by double-clicking on the **SystemView Configuration** icon within the SystemView folder. The Software Distribution Client is shown in Figure 133 on page 189. The configuration page is shown in Figure 137 on page 194.

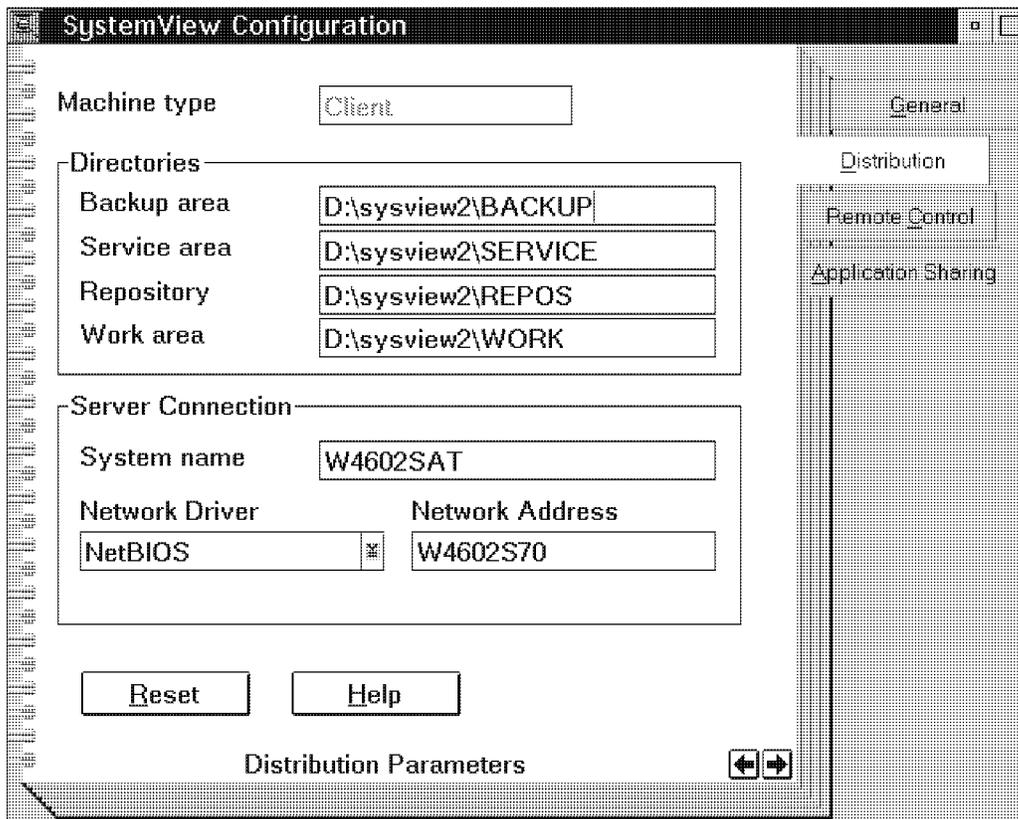


Figure 137. Configuration Page for the Software Distribution Clients

At this point, you are required to choose a network driver (protocol) for Software Distribution. Ensure the protocol chosen is supported on the Software Distribution Server. The protocols supported on the Software Distribution Server are specified on the first page of the SystemView Server Configuration Notebook. Note, the System Name, Network Address and Network Driver must correspond to the first page configuration of the Software Distribution Server. See "First page - General: Network Configuration Parameters" on page 19.

The configuration values specified here are saved in the NVDM.CFG file in the SYSVIEW2 directory. Table 16 on page 191 describes the keywords in the NVDM.CFG file.

3. Starting the Software Distribution Server

The Software Distribution Server is automatically started during startup. If for any reason it has been stopped, it can be restarted by double-clicking on the **Start Distribution Server** icon within the Distribution OS/2 Server folder, which is contained in the SystemView systems management folder.

You can do this remotely by using the Remote Workstation Control Function or the Remote Session and issuing the command:

```
NVDM START
```

The Software Distribution Server starts up a number of processes. The SystemView Software Distribution Agent window is shown in Figure 138 on page 195. This indicates the Software Distribution Server has started up, and the local agent has connected successfully. See Figure 138 on page 195.

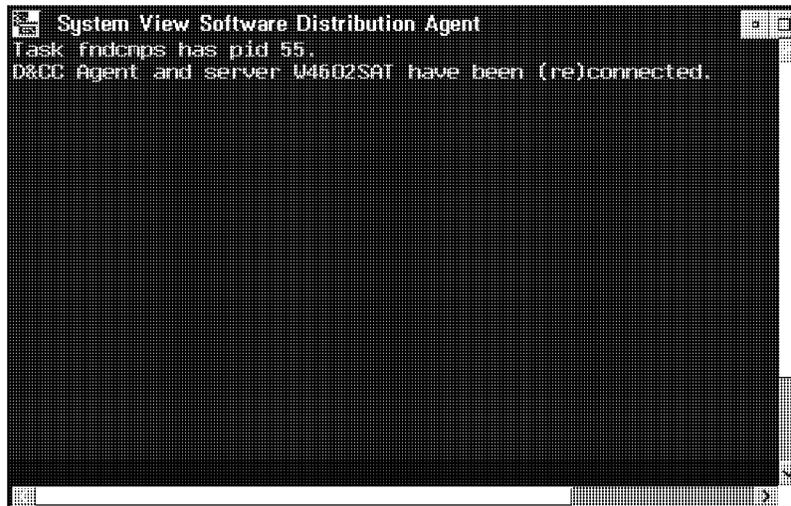


Figure 138. Software Distribution Agent Window

If the server does not start up successfully, the errors are logged in the FNDLOG file. This file is an ASCII file and it is located in the SYSVIEW2 directory. This file is locked if any Software Distribution service is ready. You can rename or delete the file by stopping all Software Distribution services. On startup of a Software Distribution service, a new one will be created. The messages stored in the FNDLOG file are identified by a unique code in the form FNDXXAAAB where:

- XX is the internal component that logs the error
- AAA is the message number
- B is the error severity: I (Informational), W (Warning), E (Error)

You can also view the log file using the NVDM command line. The log command has the following options:

- -w target (for the source of the messages)
- -co for correlators
- -I X (where X can be W, I or E for Warning, Informational or Error messages, respectively)

Explanations to the messages are listed in the online *Messages* documentation in the SystemView Information folder.

4. Defining the Distribution Clients

In your organization, you should have a number of workstations that usually require similar software and hardware configurations. As a result, when software changes need to be made, you would most likely be distributing the same changes to all of the workstations within this department.

For this reason, it is best to use the Remote Systems Manager to create groups of these similar machines. See 1.6.1, "Creating a Group" on page 31 for information on how to create these groups. Once these groups are defined, you can select to distribute software to the entire group. However, you will still be able to select distribution by individual client.

5. Starting the Software Distribution Clients

The Software Distribution Server is automatically started during startup. If for any reason it has been stopped, it can be restarted by double clicking on the

Start Distribution Client icon within the Distribution OS/2 Client folder which is contained in the SystemView folder.

You can also use the `NVDM start` command to start the client. This starts the client process in the window below. See Figure 139.



Figure 139. Software Distribution Client Agent Window

When the client starts up for the first time, it connects to the Software Distribution Server to perform an automatic registration procedure. This is done without user intervention. Once the client is defined at the server, you can check the status of the target by issuing the `NVDM stattg *` command. This will list the status of all the defined targets.

If the client fails to make a connection to a Software Distribution Server, a message will be logged on the agent window displayed in Figure 139. The client also makes use of the `FNDLOG` file for logging error messages.

Non-CID Applications

Note that the following steps are required only for the distribution on CID-enabled applications. If all you wish to distribute is non-CID-enabled applications, you do not have to complete steps 6 through 9.

6. Setting Up the Code Server

Before CID-enabled applications can be prepared, you have to set up a Code Server. The Code Server is a repository for the images of the CID software, the relevant Response Files, and the log files which are created when a CID application is installed.

The Code Server is a concept and not an additional product. In Figure 133 on page 189, the Code Server is installed on the same machine as the Software

Distribution Server. It is possible to have another machine configured as the Code Server; however, to keep the configuration simple, the Code Server and the Software Distribution Server are the same machine. The following tasks need to be completed to set up the Code Server:

- Set up the drive redirection mechanism
- Create the CID directory structure
- Copy the Disk Images into the CID directory structure
- Customize the drive redirection mechanism

a. Setting up the drive redirection mechanism

For the distribution of CID-enabled applications, the Software Distribution Server requires that the Code Server utilize a drive redirection mechanism. The drive redirection mechanism can be provided by LAN Server, NetWare, SRVIFS, or TCP/IP (NFS).

The Software Distribution Server will initiate the software installation routine at the client. During this routine, the client will attach to the shared drive provided by one of the Code Servers. The software installation will begin on the client, using the parameters supplied by the Software Distribution Server.

In our example, we are using LAN Server to provide the drive redirection. The Software Distribution Server in Figure 133 on page 189 has LAN Server installed and set up. If you choose to use TCP/IP, you would have to install the NFS kit on the Software Distribution Server, and if you choose to use NetWare, you would have to have to set up the Code Server functions on a NetWare file server.

For the purposes of our exercise, the Code Server has LAN Server installed and configured.

b. Create the CID directory structure

The Code Server directory structure consists of a CID directory with IMG and RSP subdirectories and a LOG directory. IMG, RSP, and LOG contain, respectively, the product code images, the Response Files, and the message log files. Under each of these directories, you need to create a separate subdirectory for each software product in which to store the data for that product.

If you use LAN Server as the redirection mechanism, you can have the CID Preparation utility automatically generate and run a command file that performs the following setup activities on the Code Server workstation:

- Create the base CID directory structure.
- Create the aliases for the directories CID and LOGINST.
- Create access profiles for the directories.
- Authorize the IBM LAN Server user group USERS to read the files in the directory CID.
- Authorize the IBM LAN Server user group USERS to write in the directory LOGINST.

For the purposes of this exercise, we will create the CID directory structure manually. The directories may be located on separate drives, however; for maintenance purposes, you may choose to keep them on

the same drive. In the example, the images are stored on drive D, and Figure 140 on page 198 lists the commands used to create the CID directory structure.

```
MD CID
MD CID\IMG
MD CID\IMG\DB2210
MD CID\IMG\TCPIP30
MD CID\IMG\MPTS
MD CID\IMG\LS40SRV
MD CID\IMG\LS40REQ
MD CID\IMG\SYSVIEW\SERVER_2
MD CID\IMG\SYSVIEW\CLIENT_2

MD CID\RSP
MD CID\RSP\DB2210
MD CID\RSP\TCPIP30
MD CID\RSP\MPTS
MD CID\RSP\LS40SRV
MD CID\RSP\LS40REQ
MD CID\RSP\SYSVIEW\SERVER_2
MD CID\RSP\SYSVIEW\CLIENT_2

MD LOG
MD LOG\DB2210
MD LOG\TCPIP30
MD LOG\MPTS
MD LOG\LS40SRV
MD LOG\LS40REQ
MD LOG\SYSVIEW\SERVER_2
MD LOG\SYSVIEW\CLIENT_2
```

Figure 140. Creating the Directory Structure for the Code Server

Figure 141 on page 199 shows a sample directory structure created on the Code Server. This directory structure has been set up for DB2/2 Version 2.10, TCP/IP Version 3.0, MPTS, LAN Server and Requester Version 4.0, and the SystemView Server and Client software. Had you used the Code Server setup utility to automatically create the directory structure, it would have created all the directories to the left of the dotted line. All the product directories on the right of the dotted line have to be created by the administrator. A directory is required for each CID product to be prepared.

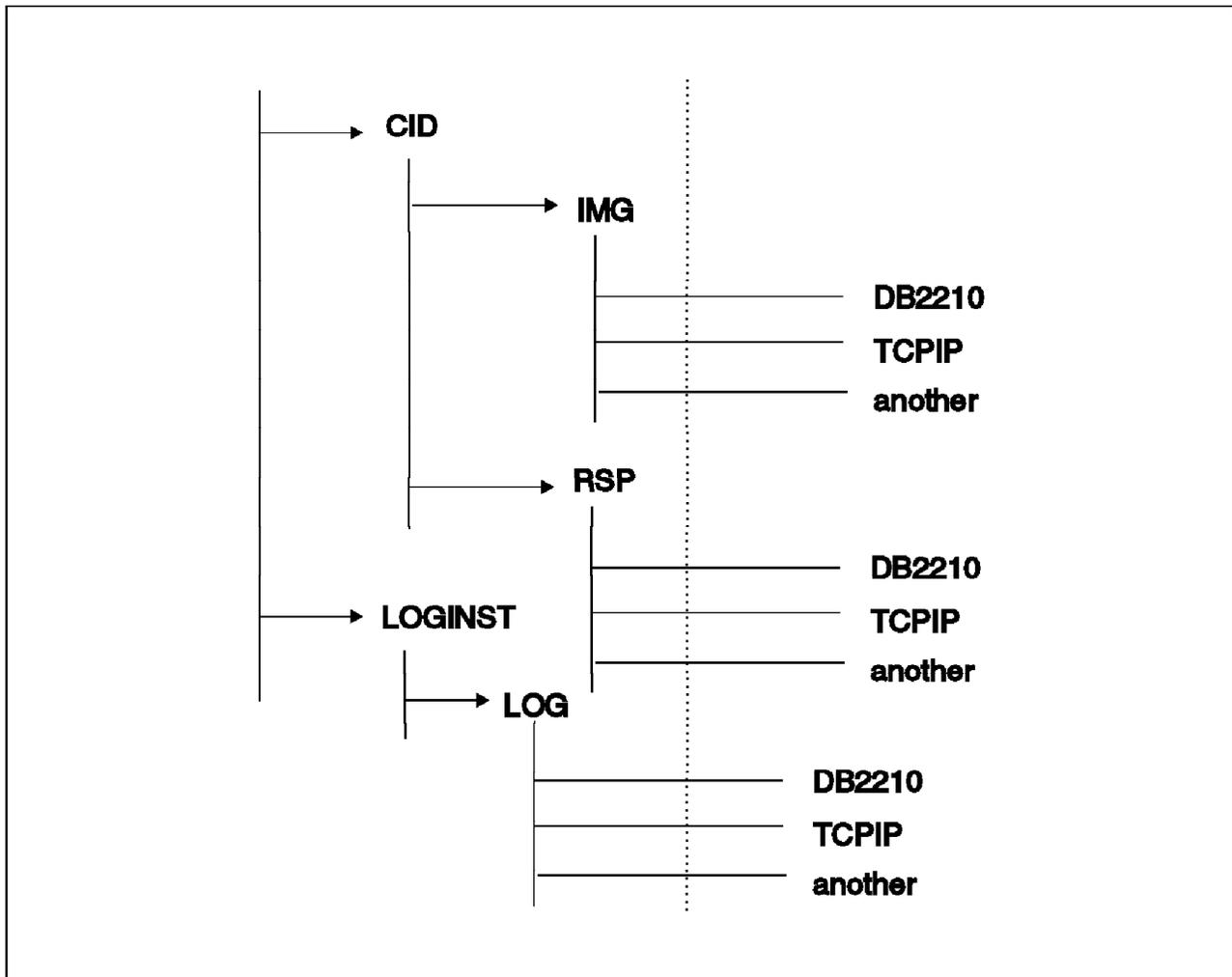


Figure 141. CID Directory Structure

It is possible to define a structure that is different than the one described in Figure 141. To do this, you will need to modify the `INTONVDM.CMD`, `FROMIMGD.CMD` and `SDMRSPNM.CMD` files. These files are located in the `SYSDVIEW2 SWLIB` directory. These files generate the CID installation program and parameters, substituting the actual values of Code Server information.

c. Copying the Disk Images

The next step in preparing a Code Server is to copy the product images and Response Files to the Code Server.

Before any software can be installed on the clients, the product code images must be copied to the Code Server's hard disk in order to be made available to the clients through a redirection mechanism. The product images need to be copied into their respective directories within the `IMG` subdirectory.

Many products provide a utility for copying the images to a server. Others provide a documented procedure, often using the `XCOPY` command, to copy the images. Refer to the specific products' documentation for a detailed explanation of how to copy the product images.

In the example, we will be distributing Database Manager Version 2.1. To copy the images, the following command is issued for each of the DB2/2 diskettes:

```
xcopy A: *.* /s D: CID IMG DB2210 /S
```

d. **Customize the drive redirection mechanism**

The final step in preparing the Code Server is to customize the redirection mechanism. If you are using LAN Server, this would mean creating aliases for the CID and LOG directories. You would also need to create access profiles for the aliases.

Figure 142 describes the aliases that are created.

```
Alias = CIDALIAS
Description = Images for CID Preparation
Server Name = W4602SAT
Server path to directory = D:\CID
Access control = XR (group users)

Alias = LOG
Description = Logging directory
Server Name = W4602SAT
Server path to directory = D:\LOGALIAS
Access control = XRW (group users)
```

Figure 142. *Creating Aliases for the CID Directories*

After you have set up your Code Server environment, you will need to configure the Distribution Server with the information on how and where the Code Server is set up. This enables the software preparation utilities to point to the correct drives when preparing the CID software.

7. **Setup the Code Server Client**

The Code Server Client requires access to the Code Server's shared drives. For this reason, you need to install the necessary redirection software on the clients. In the example, LAN Requester is installed to gain access to the LAN Server aliases. It is important that you test this functionality before you proceed.

8. **Configuring the CID Preparation utility**

After setting up the Code Server, we need to define, at the SystemView Software Preparation Site, the CID Preparation utility. This utility stores information about:

- Type of redirection mechanism to be used by the Software Distribution Agent to connect to the Code Server
- Code Server name
- Aliases that have been defined by the redirection mechanism

This step must be performed before any CID-enabled software is prepared. This information will be used during the generation of the change file profile.

To configure the CID Software Preparation utility, you will need to Double-click on the **CID Software Preparation** icon. This is contained within the SystemView Service Manager in the SystemView folder. Figure 143 on page 201 shows the second page of the Code Server Setup utility.

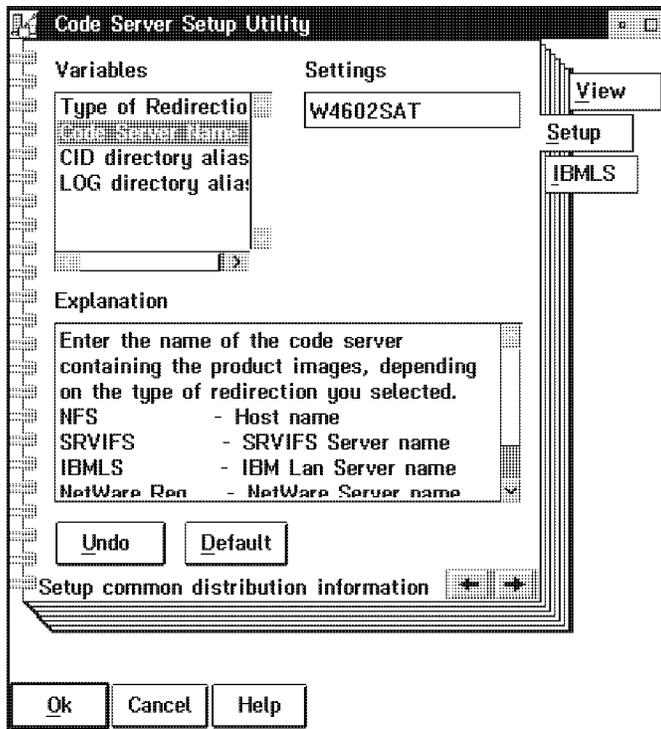


Figure 143. Code Server Setup Utility Page 2

Table 17 outlines the configuration data required depending on the type of redirection that you are using.

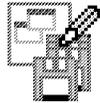
Table 17 (Page 1 of 2). Configuring the CID Software Preparation Utility

Type of Redirection	Configuration Data
IBMLS	
Code Server	Enter the server name of the Code Server containing the application diskette images. In our example, the server name is W4602SAT. This is the server name and not the domain name.
CID Directory Alias	Specify the alias of the IMG and RSP directory as defined on your Code Server. In our example, the alias is called CICALIAS.
LOG Directory Alias	Specify the alias of the LOG directory as defined on your Code Server. In our example, the alias is called LOGALIAS.
NFS	
Code Server Alias	Enter the Host name.
CID Directory Aliases	Enter the fully qualified name of the exported directory containing the IMG and RSP directories.
LOG Directory Alias	Enter the fully qualified name of the exported directory containing the LOG directory.
SRVIFS	
Code Server Alias	Enter the SRVIFS server name.
CID Directory Alias	Specify the alias of the IMG and RSP directory.

<i>Table 17 (Page 2 of 2). Configuring the CID Software Preparation Utility</i>	
Type of Redirection	Configuration Data
LOG Directory Alias	Specify the alias of the LOG directory.
NetWare Requester	
Code Server Alias	Enter the NetWare Server Name.
CID Directory Alias	Specify the alias of the IMG and RSP directory.
LOG Directory Alias	Specify the alias of the LOG directory.
No Redirection	
Code Server Alias	Not Applicable.
CID Directory Alias	The full path name of the directory containing the IMG and RSP directories.
LOG Directory Alias	The full path name of the directory containing the LOG directories.

Note: The option to specify *No Redirection* may be misleading. What this implies is all applications are going to be installed locally, that is, on the Software Distribution Server. This entry would probably only be chosen for testing and not for production purposes.

2.5.4 Preparing Non-CID-Enabled Applications for Distribution



Software Preparation

The Software Preparation application is used to prepare and add non-CID-enabled applications to the software library. This application is contained within the SystemView LAN Service Manager folder and is accessed by double-clicking on the **Software Preparation** icon.

Applications can be prepared on the Software Distribution Server or on a client that has Software Object Preparation installed. Double-click on this icon to begin preparing non-CID-enabled objects. You will be presented with the window in Figure 144 on page 203.

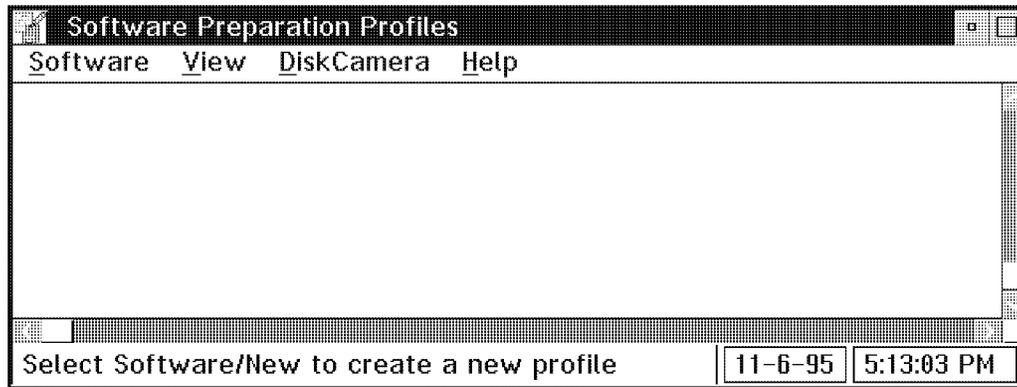


Figure 144. Software Preparation Profiles for Non-CID-Enabled Applications

There are two ways to prepare non-CID-enabled applications for distribution. You can manually prepare the definition for non-CID-enabled applications, or you can use the DiskCamera Utility. Both methods are accessible from the Software Preparation Profiles window shown in Figure 144.

2.5.4.1 Creating a New Software Object - Manual Definition

Before you begin creating a new software object, you need to install the software on the machine where the software is going to be prepared. For this reason, it is best to prepare software on a machine other than the Software Distribution Server. In our example, we distribute Arcadia Workplace Companion, Version 2.00.

The first step is to install the software on machine **B** in Figure 132 on page 187. You will need to take note of all the changes the software makes to define the software later. The product documentation may also include this type of information.

In our example, we have chosen to install Arcadia Workplace Companion on drive C. The software creates a directory, WPC200, and installs all the relevant files in this directory. The only other change it makes is to create an object on the Workplace Shell. Now that we have noted all the changes it makes, we can begin creating the software object.

To create a new software object, you need to select **New** from the Software Action bar in Figure 144.

You will be prompted for an Object Name and Type. The name you enter here will identify both the software profile you are defining for a specific object and the software object itself once it is built in the Software Distribution Server. In our example, we will use the acronym WPC as the software profile name as shown in Figure 145 on page 204. The Software Distribution service will use this name to define the Software Object Name (Global Name).

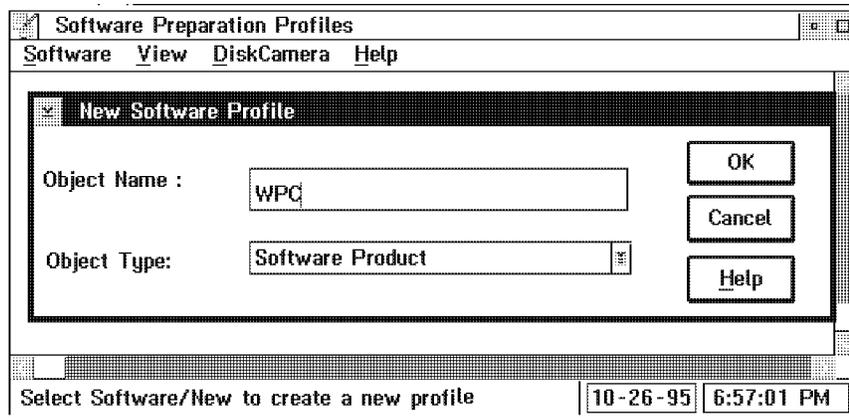


Figure 145. Software Preparation - New Profile

Once you have entered the name, the Object Details window is displayed as in Figure 146.

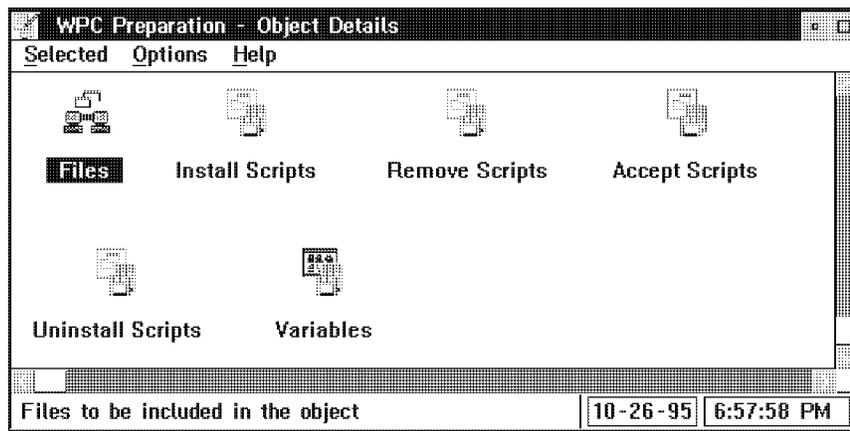


Figure 146. Software Preparation - Objects Components Window

This is the window that you use to edit the information on the elements that make up the software object. One of the first things you may want to change is the Global Name. Select the **Characteristics** menu option that is listed under the Options action item. Figure 147 on page 205 shows you the parameters that can be specified.

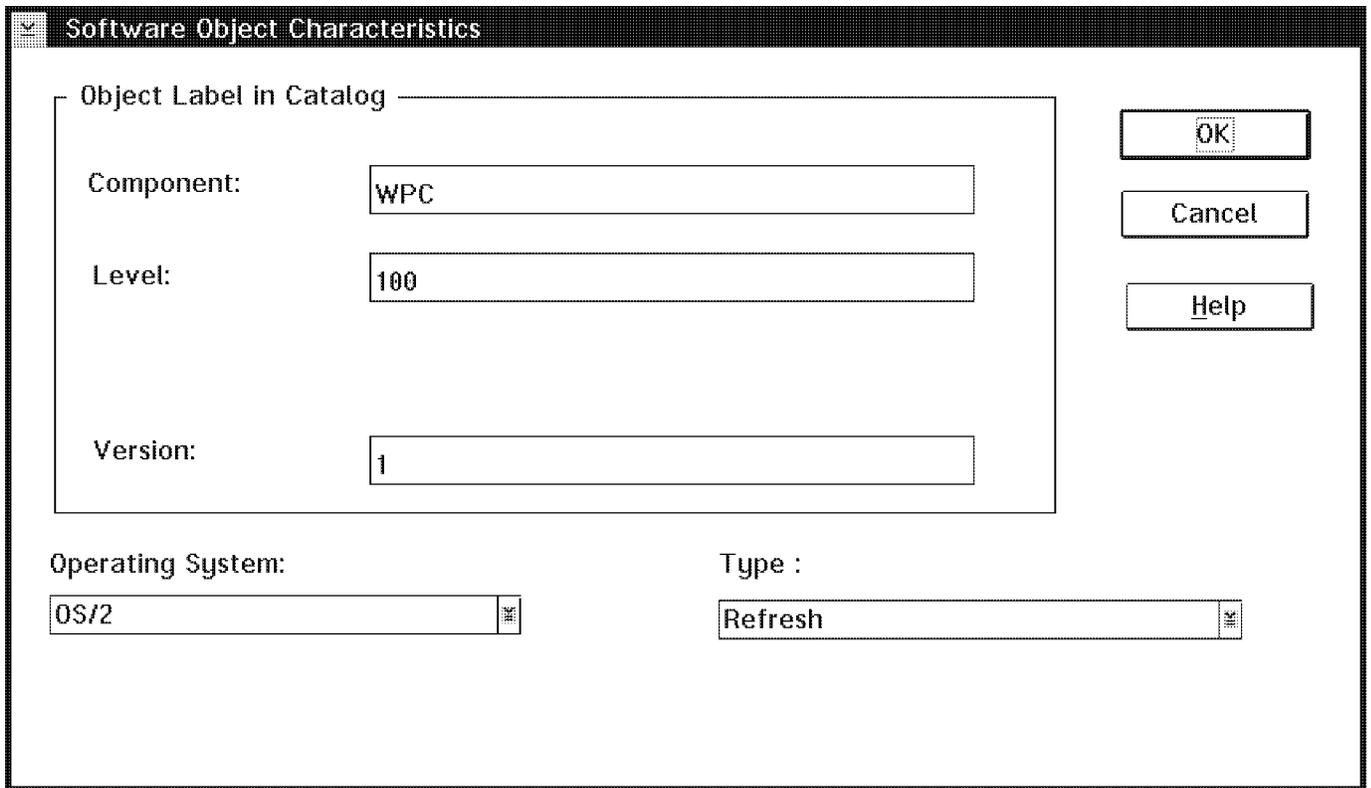


Figure 147. Software Preparation - Object Characteristics

The Global Name is of the form:

Token1.Token2.Token3Token10

Global Names for software objects will have one of the following formats:

- componentID.REF.level.version (New software)
- componentID.UPD.newlevel.oldlevel.version (Updated Software)
- componentID.FIX.level.fix.version (Fix)

In our example, the WPC software will have a Global Name of *WPC.REF.100.1*. Once the name is defined, you can go on and define the application installation.

In Figure 146 on page 204, there are a number of icons, each corresponding to an element that you may need to package in the software object. Click on the icon of an element to add information about it.

The three components that are represented in the window are:

- **Files**

You would use the Software Object Details - Files window to select the files that you want to include in the software object you create. You can directly enter a source file name specification in the FileName field, or choose the needed files with the Find window.

You also select all the files of a directory by double-clicking the chosen directory from Directory List; in this case, the FileName field will be filled with a file specification including the wildcard characters *.* Figure 148 on page 206 shows the list of files chosen for the WPC application.

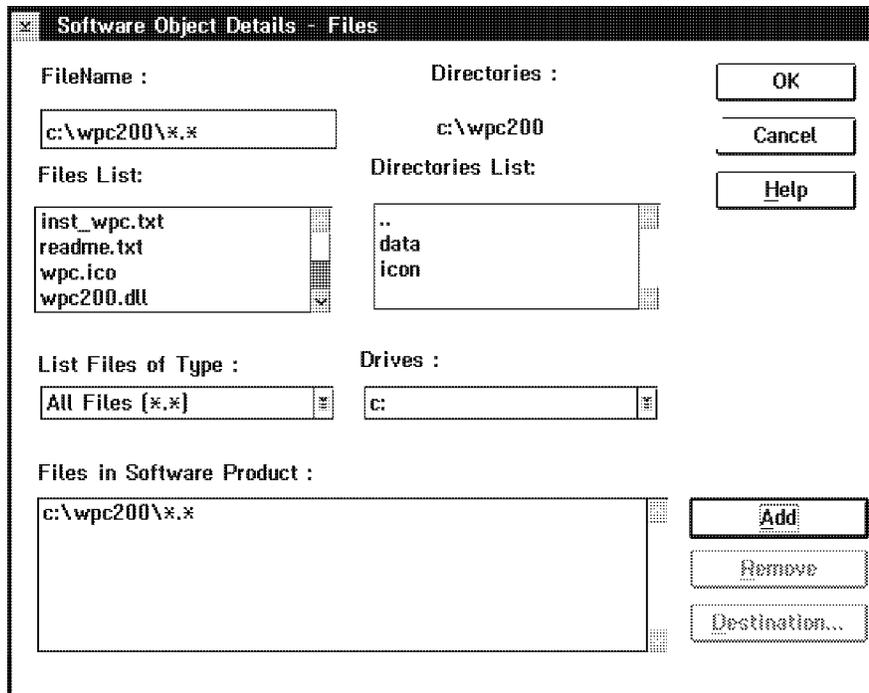


Figure 148. Software Preparation - Object Details

Select the files you have chosen in the Files in Software Product list and select **Destination**. In the Destination Options window shown in Figure 149 on page 207, you may need to specify the following:

- Action - Select the action to be performed on the target machine, such as copy or delete files. We chose to copy a file.
- Destination - The destination on the target machine. In the destination path, you can specify an already defined variable by entering \$(variable_name). In this way, when Software Distribution encounters the string \$(variable_name), it substitutes \$(variable_name) with its value. In the example, we use the \$(drive) to specify a variable for the installation drive letter.
- Directory Level - This parameter can be set to primary or nested. We will choose nested so that subdirectories are included in the software profile.
- Translate variables at install time - This option allows you to specify that the variables be replaced at install time.

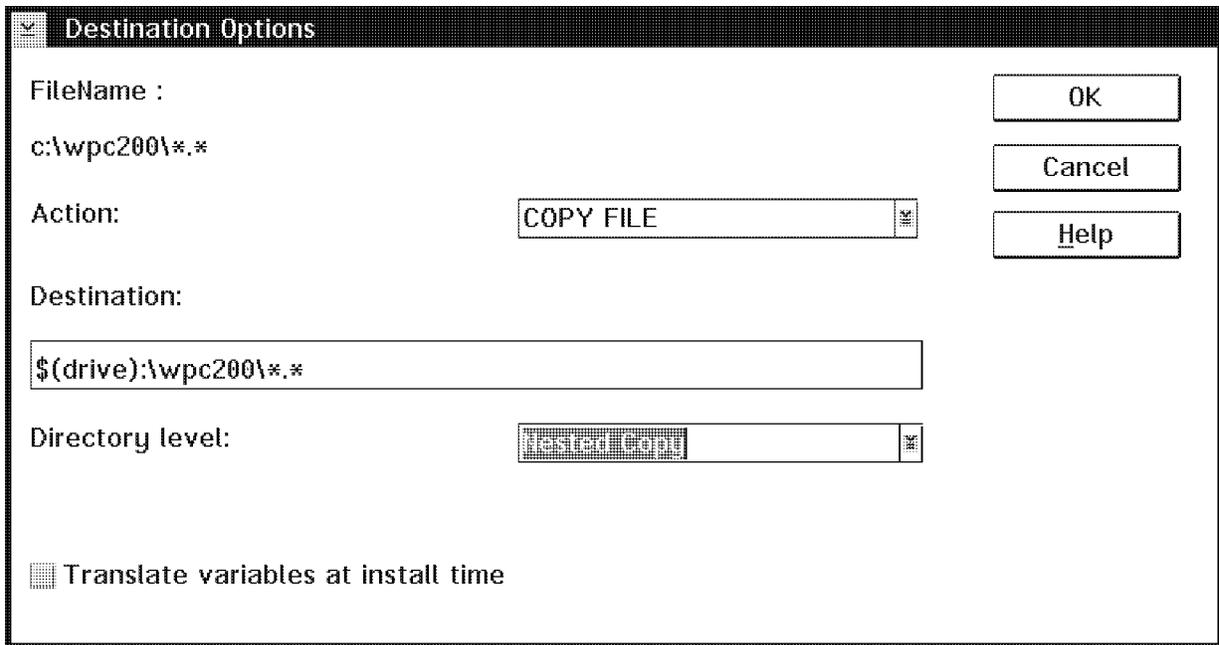


Figure 149. Destination Options Window

Once you have entered the FileName specifications, select **OK** to validate your selection and to update the list of files to include in the Software package. You can remove a file specification from the Files in Software Product list by selecting it and by pressing the **Remove** push button.

You can use wildcard characters in both source and destination file names. Do not use wildcard characters in path specifications. Also include any scripts that you need for this software product as files to be installed unless they already exist on the target. The specification must contain the complete path where the script will be installed at the target.

- **Scripts**

You can perform change control scripts before (pre-script) and after (post-script) most installation or change change control operations. Using pre-scripts and post-scripts, you can, for example:

- Add lines to a configuration file
- Delete files that already exist
- Run a configuration utility
- Check for software or hardware prerequisites

You can specify the names of the scripts within the software object. If no name is specified, no script is run. The specified program or procedure will have to be included in the software object files unless they already exist on the target. The specification must refer to the complete path name where the script will be installed at the target.

A script should produce a return code of 0 if it is successful. Any other value signifies an error has occurred. If an error occurs, the entire change control request that is in progress fails.

When scripts are being run, any output generated to standard output is automatically redirected to a file called `REQUEST.OUT`. This file is stored in the work area and is deleted before each new request.

The type of scripts you can use here are:

- Install
- Remove
- Accept
- Uninstall

Figure 150 shows the Install script window. You can specify a Pre-Install program with related startup parameters and a Post-Install program with related startup parameters. For example, we could run a script that creates an icon on the desktop for the WPC software.

The image shows a dialog box titled "Software Object Details - Scripts". It is divided into two main sections: "Pre-Install Script" and "Post-Install Script". Each section contains a "Program Name:" label followed by a text input field and a "Find ..." button. Below each "Program Name" field is a "Startup Parameters:" label followed by a larger text input field. At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Help".

Figure 150. Install Script Window

- **Variables**

In this element, you set default values for variables you use in the other elements of a software object.

Variables are short keywords, up to 11 characters long, whose default values can be defined at Object Preparation time. Note the keyword is case sensitive. The variable is referenced with the $\$(variable_name)$ notation, where the `variable_name` is the defined keyword.

When a variable is referenced in other software elements (as in included files, files destination, scripts specification, and scripts parameter), the actual variable value is replaced.

You can redefine the variable at every workstation by overwriting the default value via the Software Installation services. Usually, a redefinition is needed only for those workstations which you want to deviate from the given default.

You can also reference some predefined variables without the need to add them in the software variables element. Predefined variables are automatically defined on all targets and have workstation-specific values.

In our example, we defined the variable \$(drive). Figure 151 shows the window where the default value for the variable is set.

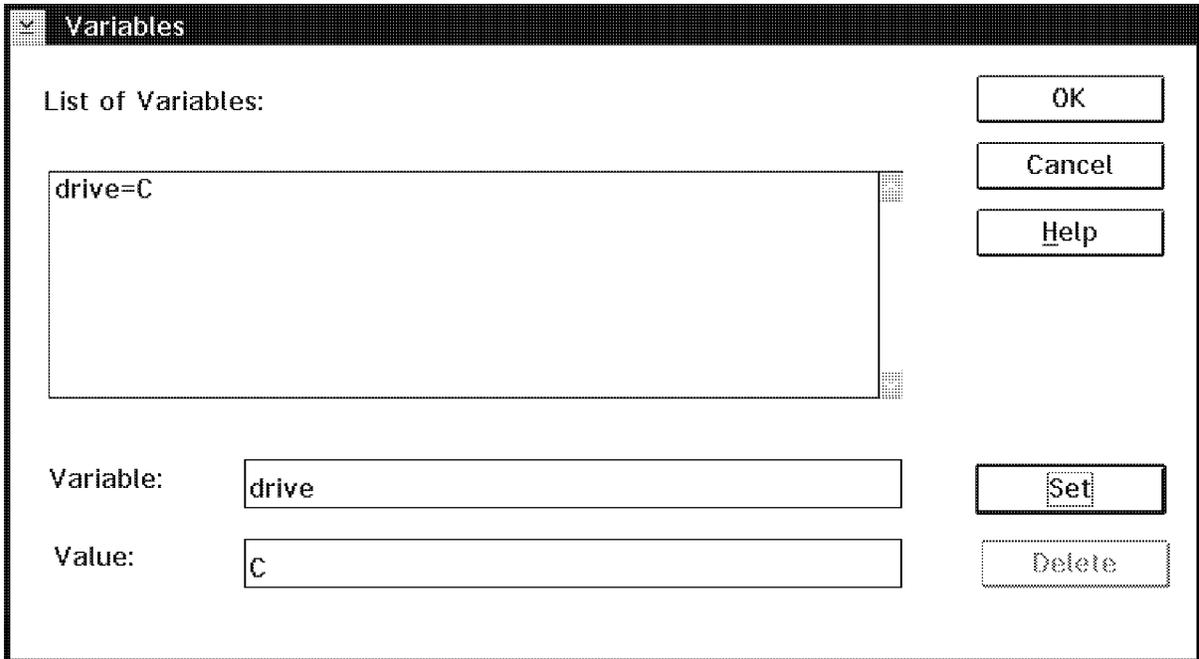


Figure 151. Specifying Values for Variables

Once you have completed adding all the information required, you may exit from this window. You will be prompted as to whether you would like to catalog the product now. If you do not, you will still have the choice later. In our example, we choose to catalog now. Figure 152 shows the message box indicating a successful catalog.

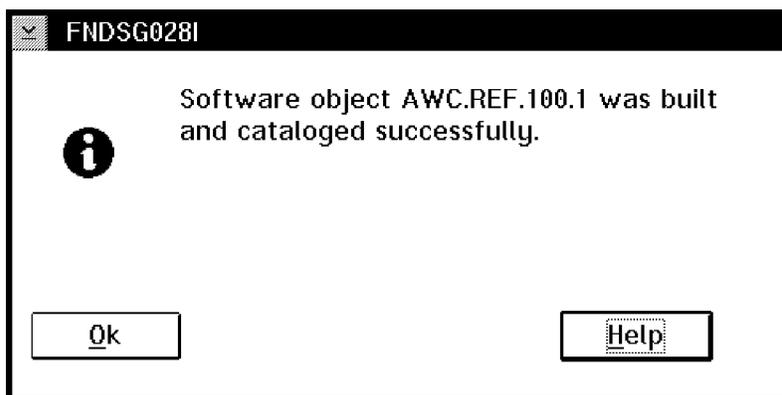


Figure 152. Catalog Message Window

The Arcadia WorkPlace Companion is now cataloged and ready for distribution.

2.5.4.2 Using DiskCamera

DiskCamera is a utility program that provides the means to replicate, at a OS/2 or Windows workstation, an application installation that was performed manually at another workstation.

DiskCamera creates the WRK directory, which it uses as a working directory under the SYSVIEW2 BIN directory. The parameters for the DiskCamera are stored in the DSKCAM.INI file which is located in the SYSVIEW2 BIN directory. The default file is shown in Figure 153.

```
filestoexcludeinOS/2
$(PROD)
filestomonitoriesinOS/2
$(BOOT):\CONFIG.SYS
```

Figure 153. Default DSKCAM.INI File

The `filestoexcludeinOS/2` header lists files that will not be inserted into the Software Object.

The `filestomonitoriesinOS/2` header lists files that will be monitored, and all updates will be inserted into the software object. At this point, only changes to the CONFIG.SYS are supported.

DiskCamera performs the following steps in order to generate a software object:

1. First, DiskCamera takes a snapshot of the drive before installing the application. You can start the snapshot by selecting the **Disk Picture** menu item under the DiskCamera Action Item. This information is stored in the SYSVIEW2 BIN WRK . It stores a copy of the `filestomonitoriesinOS/2` and information on all the other files on the selected disk.

In our example, we are once again going to use the Arcadia Workplace Companion. Before installing the application we will select the **Disk Picture** item. A confirmation box will appear notifying you when it has started and completed.

2. After taking a snapshot of the drive, you begin the Installation of the software on the workstation. The installation procedure of the program has to be invoked by you through the Install menu item under the DiskCamera Action item. This installation process is monitored by the DiskCamera program to identify the list of files being installed and to record the changes applied.

In our example, we choose the INST_WPC.EXE installation program. Figure 154 on page 211 shows the installation program prompt through DiskCamera.

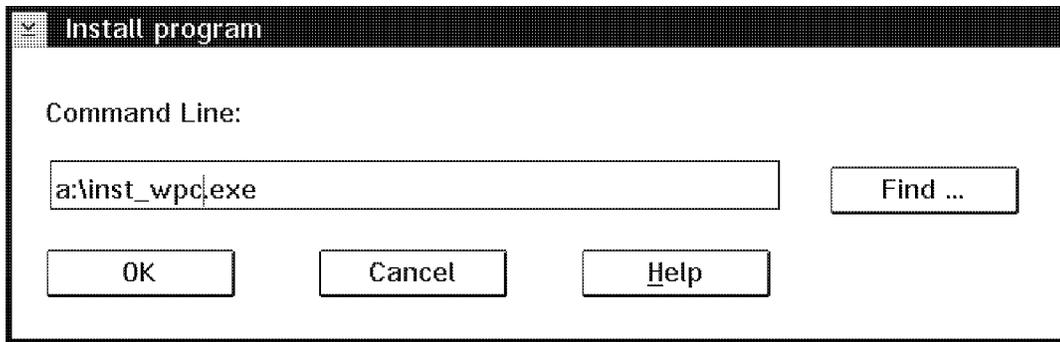


Figure 154. DiskCamera Software Installation Window

3. Once the installation of the application ends, you can generate the software object. To do this, select the **Object Generator**. This creates the software object from the changes recorded in the previous step.

Note that this process can take a long time if you have a large disk. This is because it is comparing all the contents of the disk with the items it recorded during the Disk Picture process. For this reason, it is best to install the application on a disk with the least number of files.

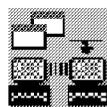
4. Once the object is generated, the various components can be edited. Once all changes are complete, the software profile can be cataloged, and the object is ready for distribution

Limitations

The following limitations of the DiskCamera utility need to be taken into account:

- The utility assumes the whole installation takes place on a single drive.
- The utility detects the changes made to the system files by the installation program, but it cannot interpret the logic behind them. For example, if a program adds a line after the third line in the CONFIG.SYS file, DiskCamera can record the change. However, DiskCamera will attempt to add a line after the third line in CONFIG.SYS of the target system. If the target system's CONFIG.SYS has only one line, the update will fail.
- Since the utility works on comparing the disk before and after installation, it is possible, given the multitasking nature of OS/2, that some other process may effect changes. DiskCamera has no means of distinguishing the origin of all of the changes; so it records all changes and reapplies them.
- DiskCamera cannot monitor a change that replaces a file with another having the same size, full path, date, and time attributes.
- If a file changes its size and time on the target drive during the application installation (for example SWAPPER.DAT), DiskCamera inserts it in the profile.

2.5.5 Preparing a CID Application for Distribution



CID Software Preparation

The task of preparing CID-enabled software for distribution is much simpler than preparing non-CID-enabled software. This is because the software installation programs have been designed to be distributed in such a manner.

CID Software Preparation is used to prepare CID software for distribution. Before you can use the CID Software Preparation application to prepare a software product for distribution, you must have an application definition file (ADF) for the product. SystemView provides sample application definition files for a set of products. You can use those files, copy and change them, or create your own application definition files. Table 18 lists the ADF and Response Files supplied with SystemView. The following files are located in the SYSVIEW2 directory:

<i>Table 18. ADFs and Response Files Supplied with SystemView</i>		
ADF	Response File	Description
CM211.ADF	CM211.RSP	Communications Manager/2 Version 1.11
DB212.ADF	DB212SRV.RSP DB212CLT.RSP	DB2/2 Version 1.2 Client and Server Configuration
DB221.ADF	DB221SRV.RSP DB221CLT.RSP	DB2/2 Version 2.1 Client and Server Configuration
LANDIST.ADF	LANDIST.RSP	LAN Distance Version 1.11
LS30SRV.ADF	LS30SRV.RSP	LAN Server Version 3.0
LS30REQ.ADF	LS30REQ.RSP	LAN Requester Version 3.0
LS40SRV.ADF	LS40SRV.RSP	LAN Server Version 4.0
LS40REQ.ADF	LS40REQ.RSP	LAN Requester Version 4.0
MPTS.ADF	MPTS.RSP	Multiprotocol Transport Services
TCPIP30	TCPIP.30	TCP/IP for OS/2 Version 3.0

If you do not have an ADF file, you will need to create your own. This is described in the online documentation and is discussed later in this section.

In deciding whether to use a provided ADF or create your own, consider that you can choose from two approaches for providing responses during a CID installation:

1. You can code an application definition file to specify that an existing Response File is to be used.
2. Alternatively, you can code an ADF to specify that SystemView is to generate the Response File from information provided during CID Software Preparation.

Once the ADF file is defined, you need to go through a number of steps to define the application before it is cataloged and ready for distribution.

In our example, the DB2/2 V2.1 Server will be distributed to the Software Distribution Clients. Since both the ADF file and the Response Files are available, only the following tasks need to be completed:

- Ensure that the software product images are copied into the respective directories.
- Copy the sample Response File into the Response File directory.

- Start the CID Software Preparation Utility by double-clicking on the **CID Software Preparation** icon contained in the SystemView Manager folder.
- Double-click on the **Software Library** folder.
- Select the **DB2/2 V2.1** icon from the SystemView software library. The software library icon is contained in the CID Software. This is shown in Figure 155.

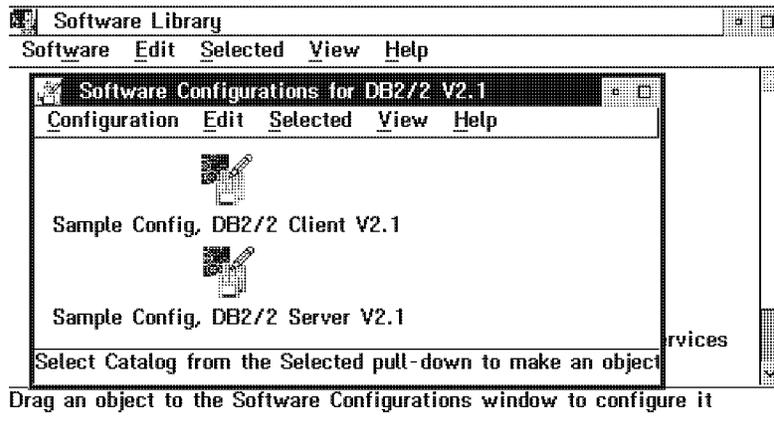


Figure 155. Software Library DB2/2 2.1 Sample Configuration

- Double-click on the **Sample Config, DB2/2 Server V2.1** icon. This is the notebook that will contain all the information the client will use when DB2/2 will be installed. The ADF file determines the contents of this notebook.

Should an ADF file have been designed not to have a Response File, all the installation parameters for DB/2 2.1 would have been listed here, rather than in the Response File.

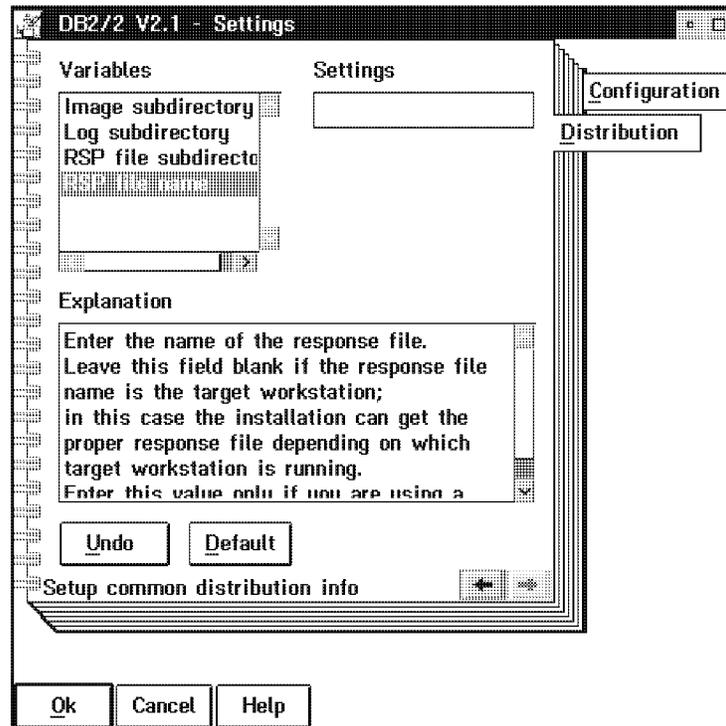


Figure 156. DB2/2 Folder

Parameter	Value
Image subdirectory	This is the name of the directory where the product images are stored. This must be relative to the path <CIDALIAS> IMG.
Log subdirectory	This is the name of the directory where the log files are to be stored. This must be relative to the path <LOGALIAS> .
RSP file subdirectory	This is the name of the directory where the RSP files are stored. This must be relative to the path <CIDALIAS> RSP.
RSP file name	If you leave the Response File name blank, SystemView assumes the variable \$(SystemName).RSP, which is resolved at installation time with the actual system name of the workstation. You can use the provided Response File (in this scenario, DB212CLT.RSP) to create additional Response Files customized for particular workstations. This approach is recommended if you need to install a CID-enabled product on several workstations using the same configuration. This is the name of the Response File to use.

- Click on **OK** to save the configuration.
- By answering Yes in the pop-up window shown in the Catalog the Object Pop-Up Window, the DB2/2 software object is cataloged at the Distribution Server.
- A generation progress indicator window is displayed, and a message window with the confirmation of the catalog is shown.
- The software is now ready for distribution.

2.5.6 ADF File Structure

The ADF file contains all the information needed to define and configure a CID-enabled software product. This file can be provided by the company that developed the application, by IBM technical support centers, or it can be defined by the administrator.

Your application definition file must contain four sections:

1. The DEF section contains some basic parameters that must be supplied for every software product.
2. The MCF section contains information that Software Distribution requires to install software.
3. The MRF section is a list of all the Response File keywords for each software product. For each keyword, you can hard-code a value that will be used in every configuration, tell CID Software Preparation to proceed to the variable section to evaluate the value, or set the value after evaluation of a conditional statement.
4. The VAR section contains all the variables specified in other sections of the application description file and specifies how they are to be assigned values in a particular configuration.

The ADF sections are free-text sections and contain the following special keywords:

Keyword	Description
@INCLUDE filename	Embed a file.
@IF <simple condition>	Parse the next few lines depending on the result of the condition. If the condition is false, ignore the lines until and @ENDIF is found.
@ENDIF	End statement for the @IF conditional statement.
@NOINCLUDEIFNOVALUE	This statement excludes the lines following it if some place-holders have an empty value.
@INCLUDEIFNOVALUE	This statement includes the lines following it even if the place-holders have an empty value. This is the default.

2.5.6.1 General Information (@DEF)

This section contains general software definition information. This information determines the name, version, and so on when the software is cataloged. The following is the DEF section of the DB2/2 2.1 ADF file with a description of the parameters:

```

@DEF
* *****
* Descr   is not specified here; it is the icon title
* Name    is the short name of the product, (max. 16 char, and
*         only alphanumeric)
* BaseProd is the short name of the Package that is the product name without
*         explicit references to the version/release, (max. 16 char, only alphanumeric)
* Release is the version/release of the product, (no dots allowed, only numeric).
* Level   is the maintenance Level of the product, (no dots allowed, only numeric)
* Platform is the required Operating System: OS2 or DOS
* Category is the type of application: OpSys, LANTran, SWDistr, Appl, CSD
* Manufacturer is the company that produced the package, (max. 16 char, only alphanumeric)
* Language is the NLS version of the product, (max. 16 char, only alphanumeric)
* FileList is the list of files composing the ADF.
* *****
      Description      "DB2/2 V2.1"
      Name              DB2210
      BaseProd          DATABASE2
      Release           0200
      Level             10
      Platform          OS2
      Category          Application
      Language          US_EN
      Manufacturer      IBM
      FileList          "db221.adf"

@ENDDF

```

Figure 157. @DEF General Information section of DB2/2 ADF File

2.5.6.2 Model Change File (@MCF)

This section describes how to create the Change File Profile for the application software under definition. A generic CID.MCF file is provided as default. This file is part of the product and must be used as is. It is not recommended that you modify CID.MCF.

This section contains the information the client machine uses to connect to the code server and complete the installation. This occurs after the Distribution Server has passed this information to the the client machine. Figure 158 is the MCF section for the DB2/2 2.1 ADF file.

```
* *****  
*           Change File Profile skeleton section  
*           -----  
* WARNING: do not change the lines between @MCF and @ENDMCF  
* *****  
@MCF  
@INCLUDE CID.MCF  
@ENDMCF
```

Figure 158. @MCF Change File Section of DB2/2 ADF File

The current CID.MCF that is used with the Software Distribution is as follows:

```
GLOBAL NAME: &Manufacturer&.&Baseprod&.&Cfgname__&.REF.&Release&&Level&.&Language&  
DESCRIPTION:  &comment&  
  @if PLATFORM = OS2  
CHANGE FILE TYPE: OS2CID  
  @endif  
  @if PLATFORM = DOS  
CHANGE FILE TYPE: DOSCID  
  @endif  
  @if PLATFORM = WINDOWS  
CHANGE FILE TYPE: WINCID  
  @endif  
  
&locals__&  
  
@if RedirectionType <> "NORED"  
PREREQ COMMAND: cidmount &RedirectionType& $(FREEDRIVE1) $(FREEDRIVE2)  
&ServerAlias& &CidAlias& &LogAlias&  
POSTREQ COMMAND: cidunmnt &RedirectionType& $(FREEDRIVE1) $(FREEDRIVE2)  
@endif  
  
INSTALL PROGRAM:  
  PROGRAM NAME:  &SDM_InstallProgram&  
  PARAMETERS:   &SDM_InstallParms&  
  @if RemoteResponseFile = No  
  RESPONSE FILE: &rff__&  
  @endif  
  
  @if UninstallAllowed = 1  
UNINSTALL PROGRAM:  
  PROGRAM NAME:  &SDM_UninstallProgram&  
  PARAMETERS:   &SDM_UninstallParms&  
  @endif
```

Figure 159. @MCF Change File Section of DB2/2 ADF File

All the variables in this section are replaced with their respective values that are taken from the information provided when the Code Server utility is configured and the Notebook is completed. The resulting information is used to catalog the product.

2.5.6.3 Model Response File (@MRF)

In this section, you need to specify a template file that will be used to build a Response File for the unattended installation of a product. As mentioned previously, if you wish to create the Response File on your own or if you already have a Response File, you can specify a dummy entry here.

The object created will then prompt you for the location of the Response File. If you want the utility to generate the Response File, you will need to specify something other than the dummy entry. The DB2/2 ADF file contains the following dummy entry:

```
* *****  
*                               Response File skeleton section  
*                               -----  
* Specify the name of the model Response File in the include statement;  
* the model R/F is a skeleton of a Response File with place-holders  
* instead of keyword value and conditional statements to include or exclude  
* part of the file, depending on the value of some configuration keywords.  
* *****  
@MRF  
@INCLUDE DUMMY.MRF  
@ENDMRF
```

Figure 160. @MRF Model Response File Section of the DB2 ADF File

The contents of the DUMMY.MRF file are as follows:

```
* *****  
*This is a 'Model Response File' Dummy file.  
*Use this when you have already a Response File ready to use.  
*In this case write the Response File fully qualified path that  
*you want to use.  
*Don't use this dummy file when you want to create a real Model  
*Response File. Refer to Documentation about the way to build  
*a Model Response File.  
* *****
```

Figure 161. Dummy File @MRF Section of the DB2/2 ADF File

For example, if you wish to have the Response File generated for you, you could have the following entries in the @MRF section or in a file that could be added by using the @INCLUDE statement. The statements making up this section can be of two types:

```
Keyword = fixed value  
Keyword = &variable_name&
```

```
* *****  
*                               Response File Template  
* *****  
DELETEBACKUP = &DELETEBACKUP&  
SAVEBACKUP = &SAVEBACKUP&  
CFGUPDATE = &CFGUPDATE&  
OVERWRITE = &OVERWRITE&  
  
;SystemView System Name. This identifies the system in the Network  
SystemName = &SystemName&
```

Figure 162. Generating a Response File in the MRF Section of the DB2/2 ADF File

During the configuration process, the above place-holders will be presented in the Notebook configuration. During the Response File generation, they will be replaced with their current values.

2.5.6.4 Variables (@VAR)

This section contains all the variables referenced as place-holders in the other ADF sections. For each variable, the user can specify some predefined mechanism to get its value. For example, you could use:

- User exit
- External file
- Dialog

The Configuration Notebook is completely driven by the @VAR section in the sense that the number of pages and the content of each page is determined by the ADF writer.

The syntax of each variable is documented in the "Creating an Application Definition File" on-line manual.

IBM provides a .VAR file that must be included in the main ADF. Moreover, some predefined variables must be specified in the ADF file. They are:

- CODESERV.VAR

It contains the variables involved in the distribution action of the software product. You should simply include this file on top of your @VAR section. This file must be used as is. It is recommended not to modify the CODESERV.VAR file.

- Predefined Section Commands

These section commands must be specified in the ADF after the INCLUDE command of CODESERV.VAR. This section must contain the following variables:

- InstallProgram

This is the name of the CID installation program.

- InstallParms

This is the list of the input parameters to the CID installation program.

- UninstallAllowed

This indicates if the software under definition has a program to uninstall itself (1 means YES).

- UninstallProgram

This is the name of the uninstallation program, if any.

- UninstallParms

This is the list of the input parameters to the uninstallation program.

It is recommended that you do not change the definition of the section commands or their variables.

The following is an example of the DB2/2 @VAR section of the ADF file:

```

* *****
*
*           Parameter section
* This section lists all the parameters that are used during the process
* of generating response and change files; the values are collected
* when you configure this software
* *****
@VAR
* *****
* The following included file contains variables about the set-up of
* the code server
* *****
@INCLUDE CSREMOTE.VAR
* *****
* The following section contains the command to install and
* uninstall the product
* Use special symbols
*   $S   to specify the path containing the product images
*   $R   to specify the Response File
*   $B   to specify the boot drive
*   $L1-5 to specify up to 5 log files
*   $L   to specify the first log file
* Each of them as a correspondant SDM_xxxxxx keyword in the
* SDMCMSD.VAR that translates the command in the Software
* distribution format.
* Note:
* It is reccomeded to specify the drive or directory where to install
* the software as a keyword of the Response File rather than a parameter
* of the command line.
* *****
section Commands
{
    InstallProgram
    {
        "INSTALL.EXE"
    }
    InstallParms
    {
        "/S:$S /R:$R /L1:$L1 /L2:$L2 "
    }
}
* *****
* Uninstall command and install commands have to use the same Response File.
* UninstallAllowed = 1 means that the software object created could be
* installed and uninstalled.
* Use UninstallAllowed = 0 when the software product does not support an
* uninstall program.
* *****
UninstallAllowed { 1 }
    UninstallProgram
    {
        "INSTALL.EXE"
    }
    UninstallParms
    {
        "/S:$S /R:$R /L1:$L1 /A:D"
    }
}
* *****
* ** INCLUDE here the configuration keywords that will be used in the
* ** model Response File for the specified product
* *****
*@INCLUDE DB212RSP.VAR
@ENDVAR

```

Figure 163. @VAR Parameters Section of the DB2/2 ADF File

For further details on the User Exit Routines, External files, and so on, refer to the online documentation.

2.5.6.5 Generating a Software Profile

Figure 164 describes how the ADF file is used to generate the various components used by the software title.

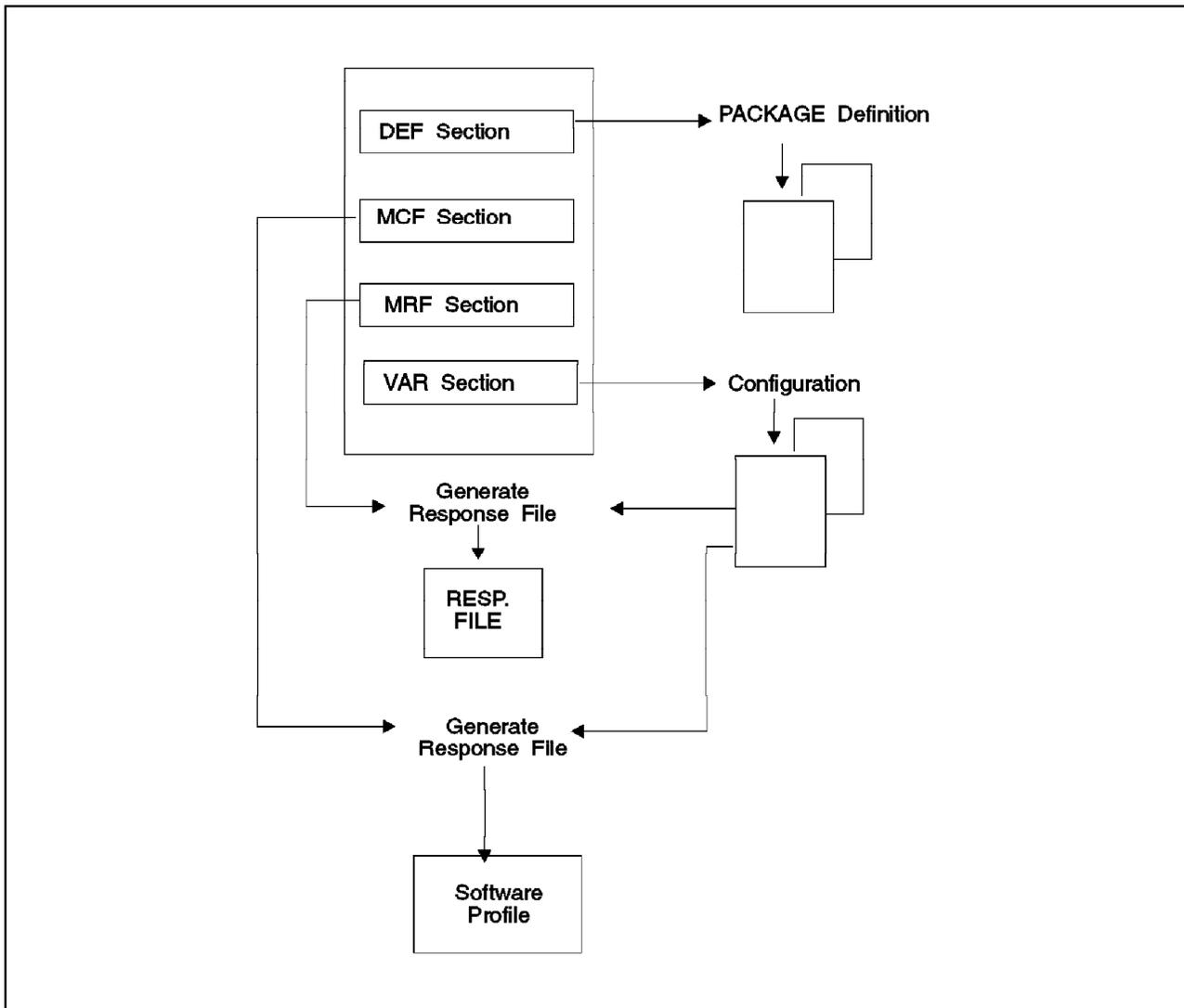


Figure 164. ADF File Schematic

In the above schematic, it is assumed that the Response File is generated by the ADF file through the Notebook configuration. If you code the ADF file and wish to use an externally supplied ADF file, the MRF file and the VAR section do not contain information required for the Response File. Only the software profile is generated.

Once you have created an ADF file, it is necessary to register it so that it is available in the software library to catalog. This can be done easily by selecting **NEW** off the pull down menu in the CID Software Preparation GUI. This allows you to specify the ADF file or to search for it.

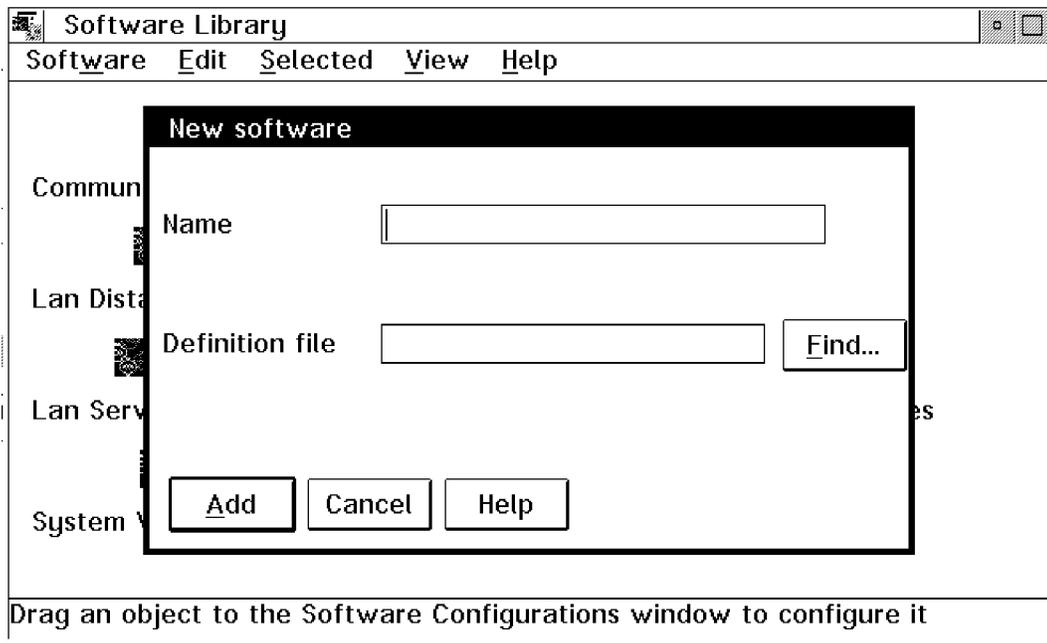


Figure 165. Registering a New ADF File

You will also be prompted for a descriptive name of the file. The new CID product ADF file is added to the Software Library directory.

Note: The directory location can be customized by setting the environment variable SWLIB in the CONFIG.SYS. For example:

```
SET SWLIB=Z:\SYSVIEW2\SWLIB
```

The SWLIB directory contains all the Application Definition File. This directory could be on a shared disk and used among different Software Preparation workstations. SWLIB.INI contains the list of the registered ADF files. This is contained in the CFGS directory.

Once the ADF file is registered, it can be used to define and catalog software for distribution.

2.5.7 How Distribution Works

Software Distribution works differently for CID-enabled and non-CID-enabled software. Although they are initiated in the same way, the processes are different. These are described in the figure below:

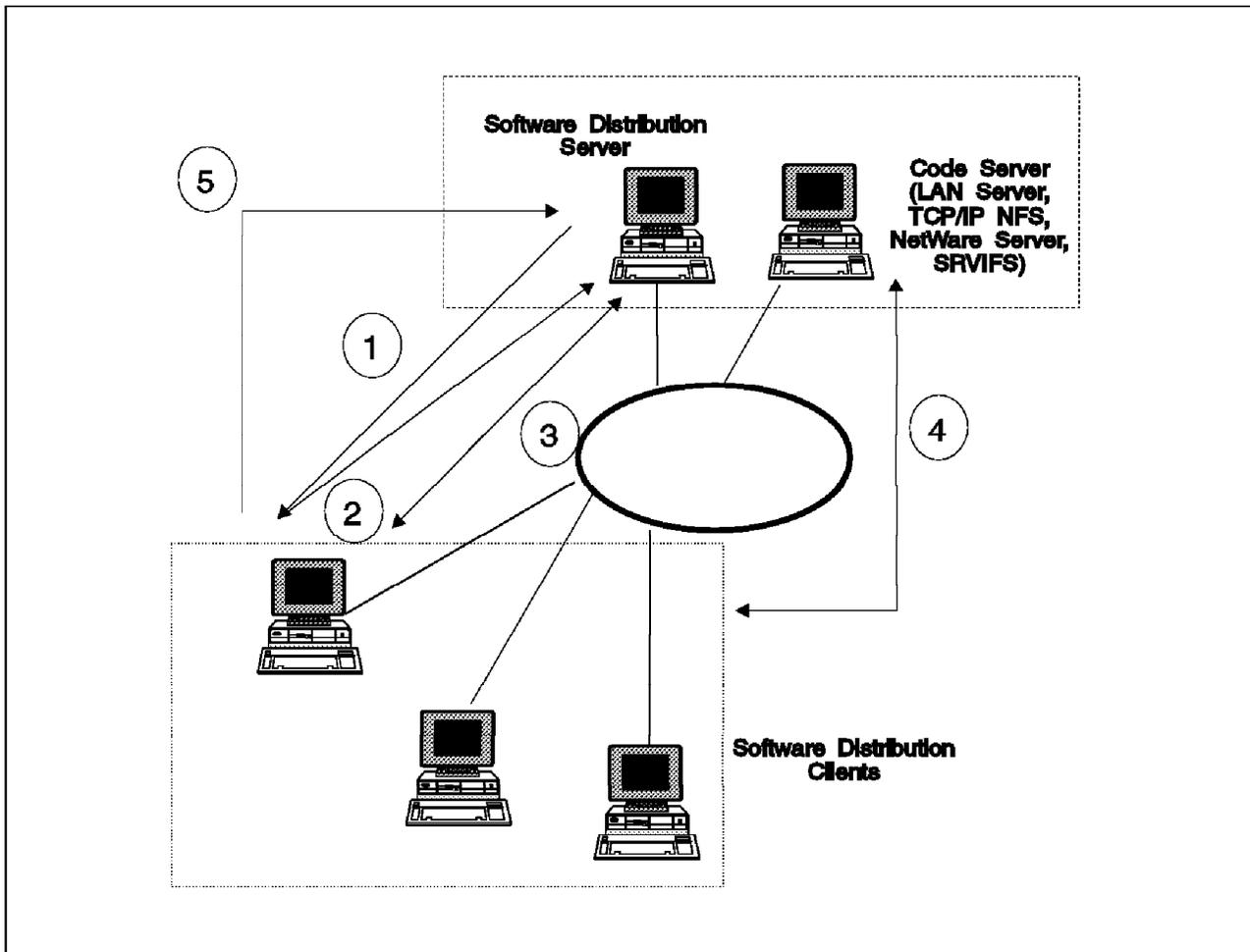
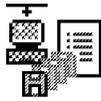


Figure 166. Software Distribution Processes

1. First, the Software Distribution administrator decides on which workstation or groups of workstations to distribute to or authorize for the selected software. They start the distribution or authorization process.
2. If the workstations are authorized to software, they have to use the software installation option to begin installation.
3. With either 1 or 2, if the software is non-CID software, the communication continues until the software is installed. Once the installation completes successfully, or unsuccessfully, the catalog is updated accordingly. The installation ends.
If the software is CID-enabled, only control information is passed and the rest of the installation occurs during step 4.
4. All the information used in step 3 is used to connect to the Code Server, which could physically be a different machine, to the Software Distribution Server. Here, the required connections are made, and the installation is initiated. You may need to log on. For example, if the Code Server is LAN Server-based, you will need to log on to LAN Server before the process can continue.
5. Once the installation completes successfully or unsuccessfully, the connections to the Code Server are deleted, and the client workstations inform the Software Distribution Server as to outcome of the installation. The catalog is updated accordingly.

2.5.8 Distributing Software



Software Installation

Once CID and non-CID software is cataloged, the steps required to distribute the software object are exactly the same. However, the underlying processes that occur are different. There are three methods that can be used to initiate the installation of software objects on remote machines. They are:

1. Using the Remote Systems Manager

This method uses the Remote Systems Manager to pass through to the remote system. You then install the software using the Software Installation icon by selecting the object and choosing **Install** off the menu bar.

You would use this method for only one of the installations because it is time consuming to use the graphical interface to initiate the software installation on a number of machines.

2. Event Scheduler

This method uses the event scheduler within the SystemView Graphical User Interface to initiate the installation of software on the remote machines. By setting up the groups within the Remote Systems Manager, you can use the scheduler to schedule the installation of software on a number of workstations simultaneously.

This method would be preferable if wish to install software objects on a group of machines. Using the scheduler also allows you to schedule the job to start automatically at some other time, for example, after hours.

3. Command Line

Use the:

`INST`

command to request the installation of up to seven software objects. The software objects you specify are treated as corequisites, which means that either all installations succeed or all do not. You can specify:

- The target on which the installation is to be performed.
- Whether the installation will be completed by an activation, in which case the installation is done to the service area. If an activation is not required, the installation should be done direct to the active area.
- Whether the software object installation is:
 - Removable
 - Automatically accepted
- The date and time at which the installation should take place.

2.5.8.1 Using a Remote Systems Manager

This section provides an example on installing the Workplace Companion that was cataloged earlier on a workstation. With this method, all you are really doing is accessing the software installation procedure on the remote machine and installing the software. The following steps need to be completed.

- To install the product, you first need to gain access to the target machine. To do this, you need to double-click on the **Remote System Manager** icon from the SystemView Service Manager window of the SystemView Manager.
- Now choose the group where the machine is defined. Double-click on this group, and then access the workstation by double clicking on its icon.
- The SystemView Service Manager window for the workstation is displayed, as shown in SystemView Service Manager Window for W4602WEO. Select the software installation icon.
- You need to double-click on the **Software Products** icon. The software products Catalog window will appear. This contains all the software objects we have cataloged that are available for distribution.

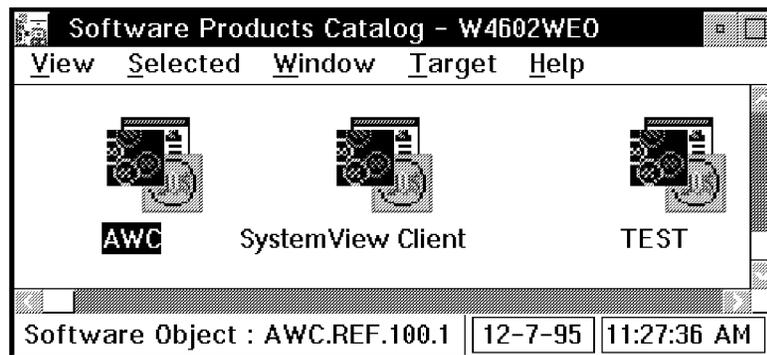


Figure 167. Software Distribution Products Catalog

- Select the product, and choose the install option which appears under the Selected action item. You also have the option here to authorize the user to install the software themselves.

You could also change the variables, such as the drive letter we defined earlier.

- You will be presented with a number of options that relate how the object is installed. The options that you have are explained below:

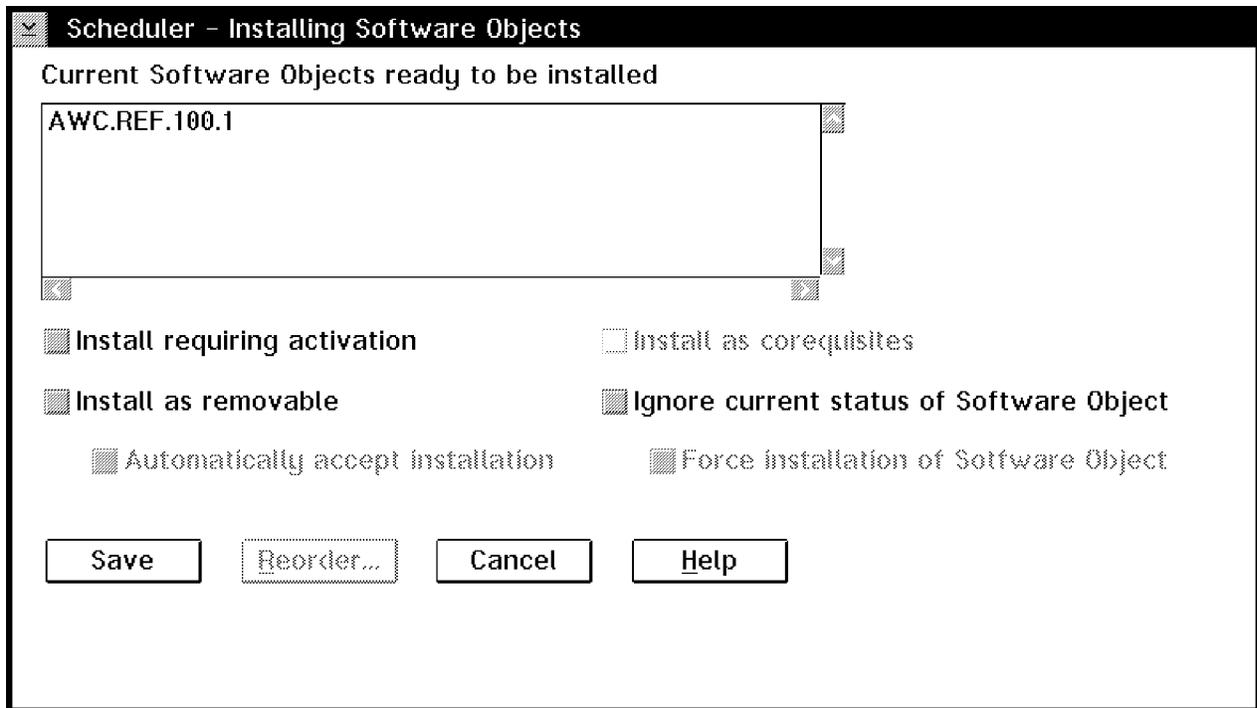


Figure 168. Software Distribution Installation Options

Install requiring activation

Select this option to have the installation completed when targets are activated.

Install as removable/Automatically accept installation

Select this option to install the software object after a backup copy is made of any affected files. The installed software object can be removed at a later date by restoring the backup files. You have three possible combinations:

1. Removable, no auto-accept

Backups are made during the installation. If the installation does not succeed, the backups are used to tidy up; otherwise, they are stored.

2. Removable, auto-accept

Backups are made during the installation. If the installation does not succeed, they are used to tidy up. If the installation completes successfully, the backups are automatically deleted.

3. Not removable

No backups are made. If the installation does not succeed, the internal disk on the target needs to be tidied up by manual intervention. Some original files from the disk may have been lost.

Ignore current status of Software Object

Select this option if software objects are scheduled for installation ignoring their current status to force the installation. That is, the installation takes place even if the file history does not report the software object as being available for installation and even if the maintenance level checks for the component failure.

Ignore current status of Software Object

Select this option if you do not want the status of the software object to be checked at the time you issue the request. That is, the request is queued even if the file history does not report the software object as being available for change control operations when you issue the request.

Install as corequisites

Select this option to install up to seven software objects as corequisites. To set the order of the corequisite software objects, use the **Re-order** push button.

You install the software objects in a single operation. If the installation of one of the corequisites fails, the whole installation fails. For this reason, use this option only if you need to install more software objects at the same time.

2.5.8.2 Using an Event Scheduler

To install a product using the event scheduler, you need to follow these steps:

1. Double-click on the **Event Scheduler** icon from the SystemView Service Manager window and select **New**.

In the Schedule New Event window, enter a name in the New Event Name field, and select **Software Distribution** from the tasks list. This is shown in Figure 169.

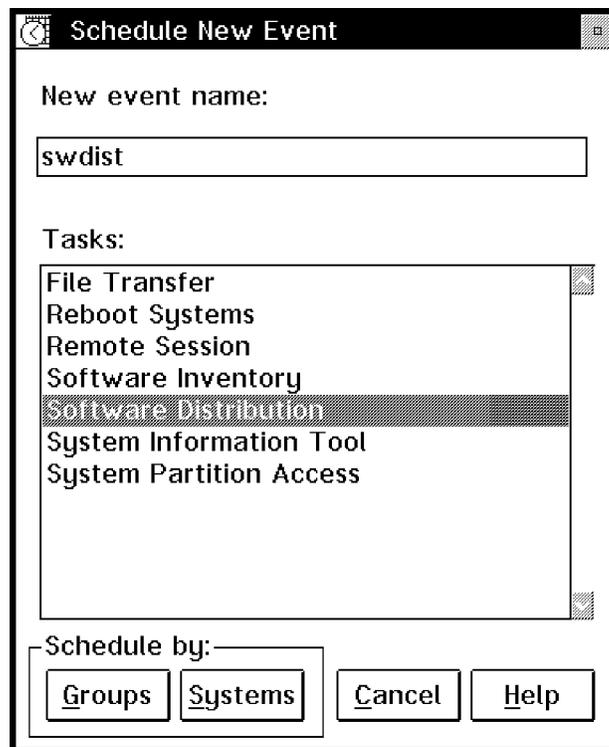


Figure 169. Scheduling a Software Distribution Event

Select **Systems**. You could select groups for distribution to a group, but for this example, we are just going to distribute to a single system. On the Schedule Groups or Systems window, select the target workstation and click on the **Schedule** button. You will be presented with the Schedule - Software Distribution Groups. At this point you will proceed as on page 224. Once you have defined the software, you select to save the event, and the scheduled installation event is created.

2.5.9 Using the Command Line

Many tasks can be performed from the command line, including the installation of software. Using the command line allows you to build batch files that could be processed in whatever sequence you wish.

For further details on the command line options, refer to the online documentation.

2.6 Summary

There are many options that can be used to achieve the purpose of easing the installation of workstation software. In this chapter, we discussed two of them, CASSETUP and Systems Management Services Software Distribution. You may however, currently be using CASSETUP or NVDM/2. It is important for you to choose the product that best suits your needs.

In the next few paragraphs, we outline some of the points you should keep in mind when deciding to change or adopt a new software distribution strategy.

2.6.1 CASSETUP

This Presentation Manager-based program is provided as a utility with MPTS/2. It assists the administrator in preparing a Code Server and in distributing code. The advantages of using CASSETUP are:

- Available at no extra charge with OS/2 Warp Server
- Easy to use and set up
- Supports pristine OS/2 Clients
- Ideal for small workgroup LANs

The disadvantages of using CASSETUP are:

- Not a strategic software distribution product for IBM, as a result, updates or added features may not appear as regularly
- Does not support any WAN protocols
- Does not support DOS or DOS/Windows environments
- Not recommended for use in an Enterprise Environment
- Does not maintain a catalog of installed products
- Error reporting is minimal
- Not automatically installed with OS/2 Warp Server

Despite these shortcomings, CASSETUP is an effective way of distributing software, especially in a workgroup environment that is purely OS/2. It is quick and easy to set up and allows you great flexibility.

If you have more DOS/Windows Clients, it may not suit your needs. Also, if you have a large number of clients using a protocol other than NetBIOS, you may have to use some other software distribution product.

2.6.2 Systems Management Services Software Distribution

This distribution product is based on NVDM/6000 R 3.1.0 and has been adapted and integrated into the Systems Management Services in OS/2 Warp Server.

The advantages of using this mechanism are:

- Available at no extra charge with OS/2 Warp Server
- Fairly easy to use and setup
- Ideal for small workgroup LANs
- Maintains a catalog of installed software
- Can be used with a software discovery tool
- Can be configured to rollback to a previous version
- Supports TCP/IP, NetBIOS and IPX
- Has an easy-to-use graphical utility to prepare both CID- and non-CID-enabled applications for distribution
- Supports Windows Clients
- Clients can initiate software installation after authorization occurs
- Error reporting is good with trace mechanisms available
- Does not require DB2/2
- Is a strategic software distribution product for IBM and will therefore be enhanced more often as new requirements emerge

The disadvantages of using this mechanism are:

- Does not support APPC
- Does not support the installation of pristine clients
- No support for DOS
- Not recommended for use in an Enterprise Environment
- Error reporting minimal
- Some skill required when setting up
- Requires additional redirection software when distributing CID-enabled applications
- No interoperability with NVDM/2
- Requires agent be installed using some other method

Systems Management Services Software Distribution is the first release of the NVDM/6000 product on the Intel platform. It is proven technology and offers numerous features. If you are currently using some other software distribution product, one of the main shortcomings of this product is the support for Pristine Clients. However, if this is not an issue, the product is ideal for software distribution with its easy integrated interface.

For users of NVDM/2, other than the support for pristine clients, another concern may be the support for APPC, which is currently not available. Should APPC be a requirement, you will have to stay with NVDM/2 until this product is capable.

Some of the advantages that it offers over NVDM/2 are:

- Client can initiate installation
- Easy-to-use integrated graphical interface
- No need for DB2/2, therefore, requires less system resources
- Integrated installation procedure

In summary, this product is ideal for small to large workgroups and autonomous enterprise departments. Its support for TCP/IP makes it available for medium-sized enterprises that use TCP/IP as a primary protocol.

2.6.3 Summary Table

The table below lists the features that are available within each of the products. It is not comprehensive, but lists many of the features. It is also not advisable to select the one with the most features but rather to select the one that matches your requirements as closely as possible.

NVDM/2 and LAN CID Utility are also included for comparison.

<i>Table 19 (Page 1 of 2). IBM's Software Distribution Managers and Their Features</i>				
Features	Software Distribution Manager			
	LAN CID Utility	CASSETUP	NetView DM/2 2.1 Extended	SystemView in Warp Server Software Distribution
Integrated Installation	-	-	-	Yes
PM Application	-	Yes	Yes	Yes
Object Oriented (Drag and Drop)	-	Yes	-	-
Command Line Interface (CLI)	Yes	-	Yes	Yes
Response File Generator	-	-	-	-
OS/2 CID Software Distribution	Yes	Yes	Yes	Yes
DOS CID Software Distribution	-	-	Yes	Yes
DOS/Windows Software Distribution	-	-	Yes	Yes
Non-CID Software Distribution	-	-	Yes	Yes
LAN Support (Q2)	Yes	Yes	Yes	Yes
WAN Support (Q4)	-	-	Yes	-
Additional products needed	-	-	DB2/2	-
Support for Pristine installations	Yes	Yes	Yes	-
Supports APPC	-	-	Yes	-
Supports NetBIOS	Yes	Yes	Yes	Yes
Supports TCP/IP	-	-	Yes	Yes
Supports IPX	-	-	?	Yes
Suitable for multi-segment LAN	-	-	Yes	-
Suitable for single-segment LAN	Yes	Yes	Yes	Yes

<i>Table 19 (Page 2 of 2). IBM's Software Distribution Managers and Their Features</i>				
	Software Distribution Manager			
Clients can initiate the Software Distribution	Yes	Yes	-	Yes
Server can initiate the Software Distribution	-	-	Yes	Yes
Need an external product to obtain redirected drives	-	-	Yes	

2.7 Related Publications

The following publications are suitable for further reading on the topics discussed in this chapter.

- *SystemView Up and Running! V1.1*, SH19-4184
- *OS/2 Installation Techniques: The CID Guide*, SG24-4295
- *Inside OS/2 LAN Server 4.0*, SG24-4428
- *Software Distribution Using SystemView for OS/2 Version 1.1*, SG24-4609

Chapter 3. Print Services in OS/2 Warp Server

The print functions and features of both the OS/2 Warp operating system and OS/2 LAN Server 4.0 are included in OS/2 Warp Server. In addition to these, OS/2 Warp Server offers a set of Advanced Print Services that makes life easier for users who need to print different types of documents on LAN-attached printers. It also provides support for managing advanced printers that are capable of two-way communication, known as bidirectional (or *bid*) printers, including AFP-capable IPDS printers, when using Print Services Facility/2 (PSF/2), a component of Advanced Print Services.

This chapter describes all of the Advanced Print Services provided with OS/2 Warp Server. It also describes the print services provided with OS/2 Warp and OS/2 LAN Server 4.0.

3.1 Printing with OS/2 Warp

This section briefly describes how to set up and use OS/2 Warp's printing facilities. For detailed information, please refer to the online documentation in OS/2 Warp (see *Printing in OS/2* in the *Information* folder).

In OS/2 Warp, you use printers by first creating *Printer Objects* associated with them. Each printer you want to use must have a printer object associated with it. You can also have more than one print object for a single physical printer, with each object having different printer job properties. For example, a printer can have one printer object set to print on letter-size paper and another to print envelopes.

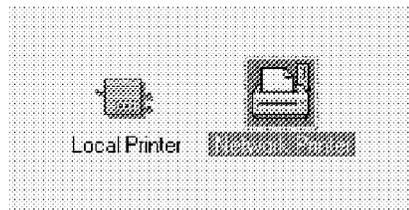


Figure 170. OS/2 Warp Printer Objects

Each printer connected to the system requires at least one *printer driver*. Printer drivers provide information that enable the operating system to format a data file for the particular printer model you selected.

When you connect new printers, you must install the appropriate drivers. Each driver may support several printers, and in this case, you can select the specific model(s) you need. For example, if you have an HP LaserJet printer, you can select LaserJet IID, LaserJet Series II, or the model name that describes your printer.

Some printers can emulate other printers. In this case, each type of emulation requires a different printer driver.

Printer drivers have *printer properties* to describe the physical setup of your printer. A printer driver also has *job properties* to describe the default setup for a print job.

Each printer object has a *printer port* it is associated with. Printer ports are usually the physical connections to the printer, such as the parallel and serial ports, but they can also be logical ports. This is the case when the printers are remotely attached and there is software (a *printer port driver*) emulating a physical port, and when using PSF/2. One example of such a connection is the IBM LAN Connection for Printers and Plotters - IBM 4033, using a MarkNet printer port driver (see 3.6, "MarkVision for OS/2" on page 255).

There are many ways to print data in OS/2 Warp. Printing can be initiated from an application program; you can drag a file icon with the mouse and drop it on a printer object icon; you can select *Print* from a pull-down menu; you can use the *Print Screen* key on the keyboard; or you can use a command such as `PRINT` or `TYPE` from the OS/2 command line or from a DOS session. In any case, the data will be placed in the queue that corresponds to the selected printer object. The queue driver will get the data from the queue and pass it to the printer driver. The printer driver will format the data for the printer and send it to the printer port, from which the data will travel to the printer.

In the case of a network printer, the data is sent to the server, and the process described above occurs there.

3.1.1 Creating a Printer Object on OS/2 Warp

To create a printer object in OS/2 Warp:

1. Open the **Templates** folder.
2. Click and hold the right mouse button over the **Printer** icon, drag it to the **OS/2 Desktop** and release the button. The Create a Printer window shown in Figure 171 will open.

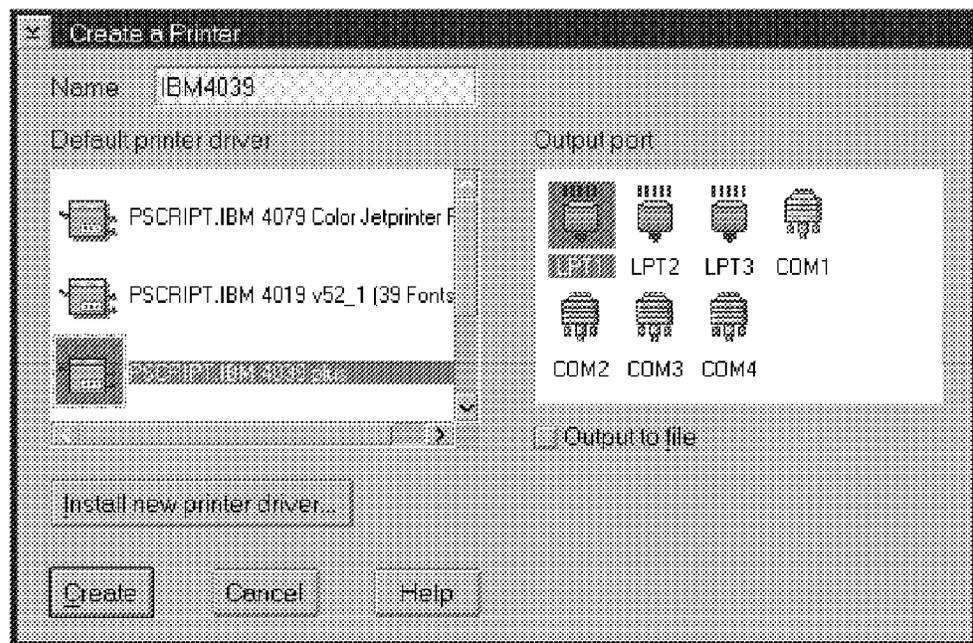


Figure 171. Creating a Print Object

3. Type in the printer name in the **Name** field. This can be any convenient name you choose for this printer.

4. Select the correct printer driver (on the left side) and output port (on the right side).

You can install a new printer driver if required, by clicking on the **Install new printer driver...** button. This will open the Install New Printer Driver window shown in Figure 172 and display a list of all printer drivers shipped with OS/2. Select the appropriate driver from the list, or if you need to install a new driver, select **Other OS/2 printer driver** and type in the directory from where the new printer driver will be loaded; then click on **Install**.

5. After making all the selections, click on the **Create** button. If you have Windows support installed, you will be asked if you want to install an equivalent WIN-OS/2 printer configuration. If you reply Yes, you will be prompted for the correct disk.

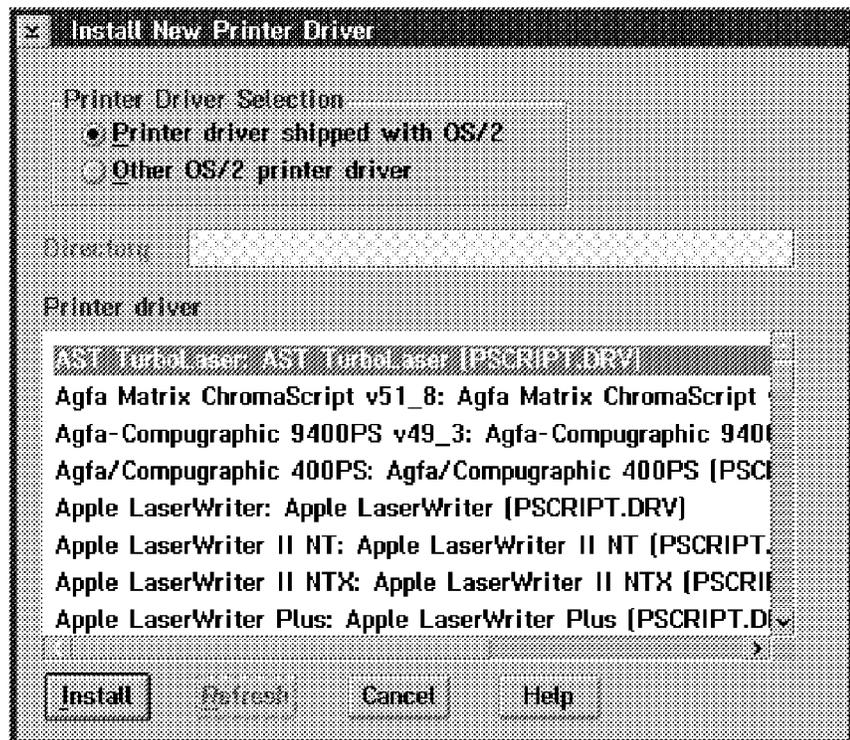


Figure 172. Installing a New Printer Driver

Once the printer object is created, an icon for it appears on the OS/2 desktop. By clicking the right mouse button on it and then selecting **Settings**, you can alter the printer object's characteristics, such as:

- Printer driver
- Output port to which the printer is connected
- Queue driver to be used
- Print options such as separator pages and printing hours

Printer objects can represent locally attached printers or network printers. A network printer is one that is accessible through a server such as OS/2 LAN Server. Creating a network printer object is even simpler than creating a local one. Just drag the **Network Printer** object from the Templates folder to the OS/2 desktop. The Access another network printer window shown in Figure 173 on page 234 will open.

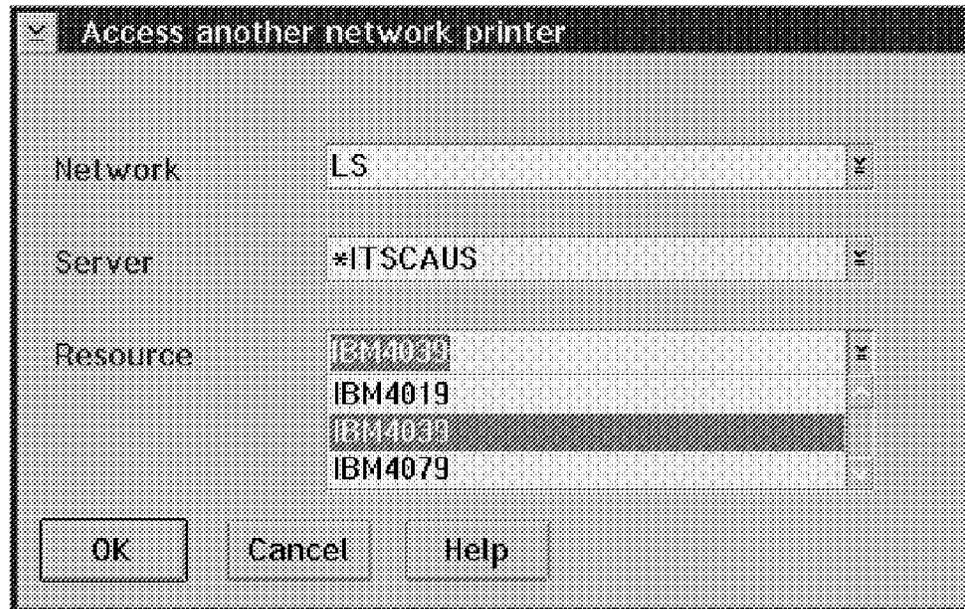


Figure 173. Access Another Network Printer Window

In this window, select the Network, the Server within that network, and the Resource within that server. A network printer object will be created on the OS/2 desktop.

A network printer object, as you see, points to a printer object that is defined on the server as a shared resource. Using the network printer requires that you have access to this shared resource.

3.2 Sharing Print Resources with OS/2 LAN Server

Print resources can be shared among the users of an OS/2 LAN Server network. To share a printer resource, the LAN administrator creates a Printer Alias by dragging the Printer Template in the Resource Definitions folder and filling the fields in the Printer Alias Identity page. *In reality, what is shared is a print queue.* The procedure for this is described in page 23, "Sharing Printers with the Administration GUI", in the redbook titled *Inside OS/2 Warp Server, Volume 1*, SG24-4602.

Once a printer is defined on the server as a shared resource, users can define network printer objects for it on their workstations.

3.3 Advanced Print Services in OS/2 Warp Server

In addition to the LAN Server print services seen above, OS/2 Warp Server offers Advanced Print Services that provide printing of the most popular print data formats on different kinds of printers, removing from the user the task of determining whether the document to be printed is in the right format for the available printer. Other services provide for remote administration and control of printers capable of two-way communications, commonly referred to as *bidirectional*, or *bidi*, printers. The following sections discuss these advanced printing functions.

3.4 Print Services Facility (PSF/2) for OS/2 Warp Server

All network operating systems provide print sharing functions. Users connected to a LAN can send documents to be printed on a network printer. The problem is, there are many different formats of documents, and there are many different kinds of printers. In general, it is up to the user to determine if the document being printed is in the right format for the printer.

Print Services Facility for OS/2 Warp Server (PSF/2), which is the program behind the Advanced Print Services component, extends the normal print services to provide support for printing documents formatted in a variety of the most popular data streams on a variety of printers connected to the server.

When a user sends a print file to an OS/2 Warp Server print object managed by PSF/2, PSF/2 will convert the data to the format supported by that printer. When a printer is replaced, the users don't have to modify anything on their LAN stations. All the LAN administrator has to do is to alter the PSF/2 configuration to reflect the change.

Table 20 shows the types of print data streams that PSF/2 can handle as input print files and the types of printers to which it can print:

Print File Input Data Streams	Printer Data Streams			
	IPDS	PPDS	HP-PCL	PostScript
ASCII	Yes	Yes	Yes	
JISCII (DBCS ASCII)	Yes	Yes	Yes	
PAGES (Japanese only)	Yes	Yes	Yes	
OS/2 Metafile	Yes	Yes	Yes	
AFPDS	Yes	Yes	Yes	
PostScript	Transform	Transform	Transform	Passthru
WordPerfect	Transform	Transform	Transform	
HP-PCL	Transform	Transform	Passthru	

Yes means that PSF/2 will recognize the data stream and convert it to the output data stream format.
Transform means that there is a transform provided with PSF/2 that supports this conversion. You must define a transform exit for the conversion to take place.
Passthru means that you can set up a transform exit so that files will be sent directly to a printer that supports this data stream.

PSF/2 integrates with the OS/2 Warp Server print components. It adds a new layer to the OS/2 print model, the *PSF/2 Device*. A printer object is typically associated with a printer port. For a printer object that uses PSF/2, the printer port function is provided by the PSF/2 Device. The definition of the PSF/2 device points to an OS/2 printer port, which can be a physical parallel or serial port, a logical port such as software controlling a LAN connected printer, or a TCP/IP connection.

When a file is sent to be printed on a PSF/2 device, PSF/2 will process it in the following sequence:

- If there is a transform sequence defined for this PSF/2 device:
 - First, PSF/2 will apply each step of the sequence to the file, with the output of each step being the input to the next step. For example, to convert HP-PCL files to PostScript format, you can define a transform exit sequence on which the first step is to convert Postscript files to AFP, and the second is to convert AFP files to HP-PCL.
- If a step in the transform exit sequence is marked as a *terminal transform*, this is the last step executed by PSF/2, and no further processing of the input file occurs. This is useful for functions such as uploading to a host platform for printing. See 3.4.6, "Setting Up Transforms" on page 243 for more information on transforms.
- When the transform exit sequence is complete (provided there's no terminal transforms in the sequence), then the resulting file is converted to an AFP data stream.
- The resulting AFP file is converted to the data stream suitable for the printer on this PSF/2 port. This can be either PPDS, one of the variations of PCL, or the file may be sent directly as an AFP file in the case of IPDS printers.

If no transform exit sequence exists for this PSF/2 device, PSF/2 will convert the input file to an AFP data stream and then to the data stream suitable for the printer.

3.4.1 Installing PSF/2

You can install PSF/2 during the initial installation of OS/2 Warp Server, or you may install it later by running WSCONFIG.EXE from the \WARPSRV directory.

Either way, to install PSF/2, you will follow one of two paths.

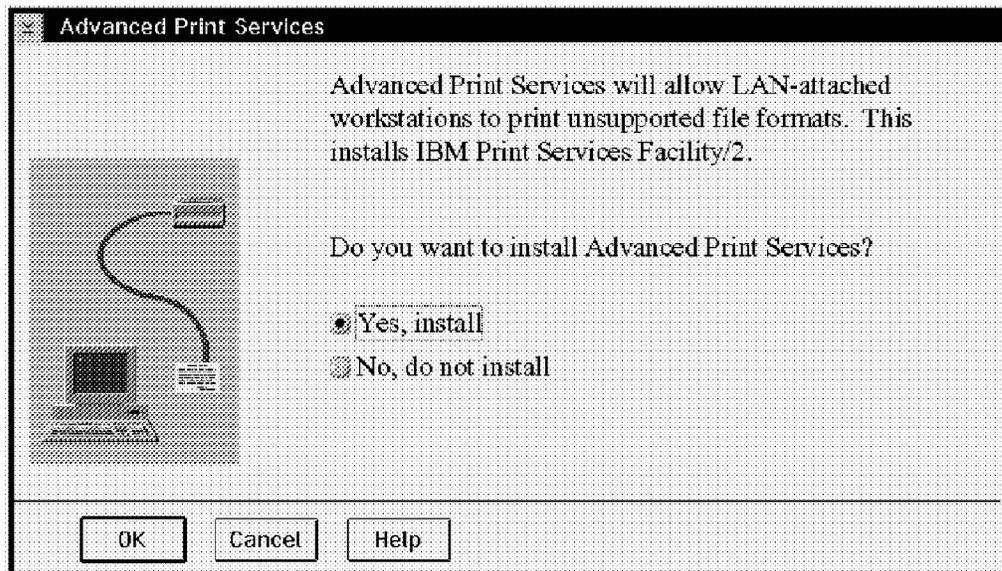


Figure 174. Advanced Print Services Easy Installation Path

If you select the **Easy Installation** path, PSF/2 will be installed if you select **Yes** on the Advanced Print Services screen shown in Figure 174.

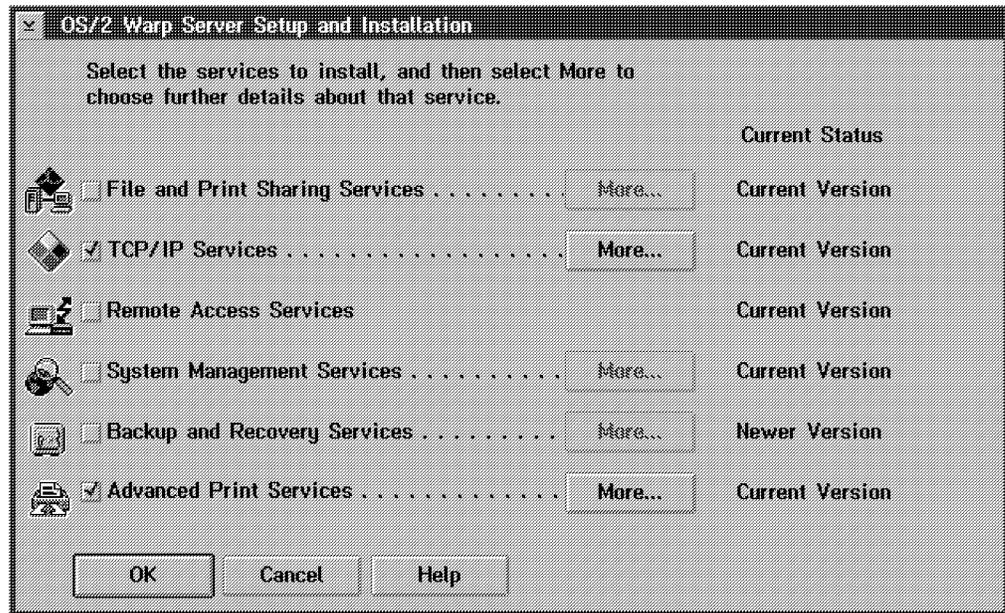


Figure 175. Warp Server Setup and Installation Menu

If you select the **Advanced Installation** path, then to install PSF/2, you must select **Advanced Print Services** on the OS/2 Warp Server Setup and Installation menu shown in Figure 175. If you click on the **More** button next to Advanced Print Services, this will open the Advanced Print Services menu shown in Figure 176. In this menu, you can select which types of printer attachments you want to install. See 3.4.3, “Printer Attachments” on page 239 for a detailed description of the types of printer attachments.

You can also select which types of print format conversions you want to install. Select **PostScript job conversion** if LAN users will be printing PostScript jobs on non-PostScript printers. Select **AFP job conversion** if users will be printing AFP jobs on non-AFP printers. You may select both types of printer attachments and both types of format conversions.

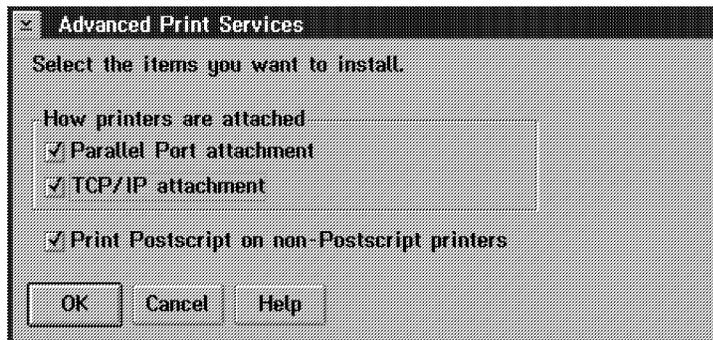


Figure 176. Advanced Print Services Options

After selecting the items you want to install, click on **OK** on the Advanced Print Services menu, then again on the Warp Server Setup and Installation menu. The installation process will continue.

Tip

We recommend you install the optional Postscript and TCP/IP support to enable usage of a wider variety of printers and for future flexibility.

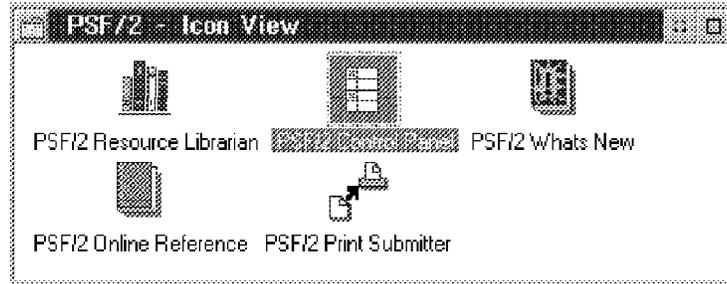


Figure 177. PSF/2 Folder

When the installation is complete, there will be a PSF/2 Advanced Print folder on the OS/2 Warp Server desktop. The contents of the PSF/2 folder are shown in Figure 177. We recommend that you shadow the PSF/2 Control Panel icon to the LaunchPad for convenience.

3.4.2 Creating a Print Device for PSF/2

By selecting the **Control Panel** icon in the PSF/2 folder, the Control Panel window will open. Initially, the window will display the default printer. Before using PSF/2 with new printers, you must define a print device and its settings.

To define a print device for use with PSF/2, do the following:

1. Select the **Profile** menu item, then select **New...** The New device window shown in Figure 178 on page 239 will open.
2. Enter the name of the device in the Device name field.
3. If desired, change the default path provided. The settings and other files associated with the device will be saved on this path.
4. Enter a description for the device in the Description field.
5. Select an attachment type from the Attachment Type list. Printer attachments are described in 3.4.3, "Printer Attachments" on page 239.
6. After selecting an attachment type, select **Settings...** This will bring up the Settings window for the attachment type you selected.
7. Select the appropriate settings for the attachment type, then select **OK**. The settings for each printer attachment type are described in 3.4.4, "Printer Attachment Settings" on page 240.
8. Select a resolution from the Device Resolution list. The device resolution indicates the printer resolution, in dots per inch (dpi), to use when printing an OS/2 metafile. Select the appropriate resolution based on the printer you are using.

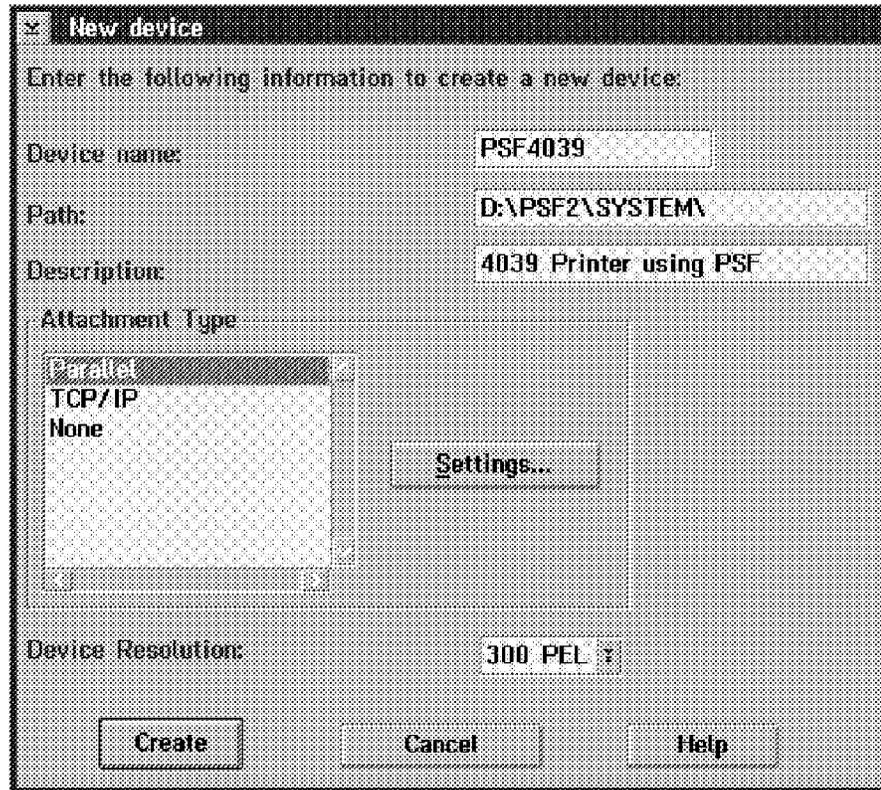


Figure 178. Defining a New Device in PSF/2

9. Select **Create** to create the device. The new PSF/2 device you created will appear in the PSF/2 Control Panel window.

Once you defined a device, you can define new devices of the same type by using the Copy option. On the PSF/2 Control Panel window, select the device you want to copy. Then, from the Profile pull-down menu, select **Copy...** The Copy device window will open, which has the same information as the New device window shown in Figure 178. Follow the same procedure as for creating a new device. When you're done, click on **Copy**.

3.4.3 Printer Attachments

You use a printer attachment to connect a printer to the network. PSF/2 for OS/2 Warp Server supports the following types of printer attachments:

- Parallel** Uses either the parallel port to directly attach the printer to the OS/2 Warp Server workstation, or the printer is remotely attached using a LAN connection such as the IBM LAN Connection for Printers and Plotters - IBM 4033. In either case, data is sent to an OS/2 port.
- TCP/IP** Uses a TCP/IP connection to the printer (for example, for connecting an IBM 3935 printer or for connecting a printer using the i-data 7913 IPDS Printer LAN Attachment), using Token Ring or Ethernet.
- None** Use this option when you do not want to direct the job to a printer attached to the server. You may, for instance, use the PSF/2 transform exits to print to a file or to upload the transformed file and print it elsewhere.

Using Serial Printers

PSF/2 does not provide a *Serial* attachment type. To attach a serial printer, you select **Parallel** for the attachment type. In the Settings window, select a **COMx** printer port.

3.4.4 Printer Attachment Settings

For each type of printer attachment, there are different settings, as follows:

3.4.4.1 Parallel Attachment Settings

The Parallel Attachment settings window is shown in Figure 179 on page 241.

For a parallel printer attachment, you must define the data stream supported by the printer and the printer port to which it is attached. All the other settings are set to their default values and may be changed if desired.

The data stream must be the one the printer supports and can be one of the following:

- PPDS
- HP-PCL4
- HP-PCL5
- HP-PCL5C

PPDS (IBM Personal Printer Data Stream) is the data stream used by LexMark printers such as the IBM 4019 and 4029.

HP-PCL (Printer Control Language) is the data stream used by most Hewlett-Packard (HP) printers. PCL4 is used on LaserJet Series II printers; PCL5 is used on LaserJet Series III printers, and PCL5C is used in PaintJet XL300 printers (for color printing).

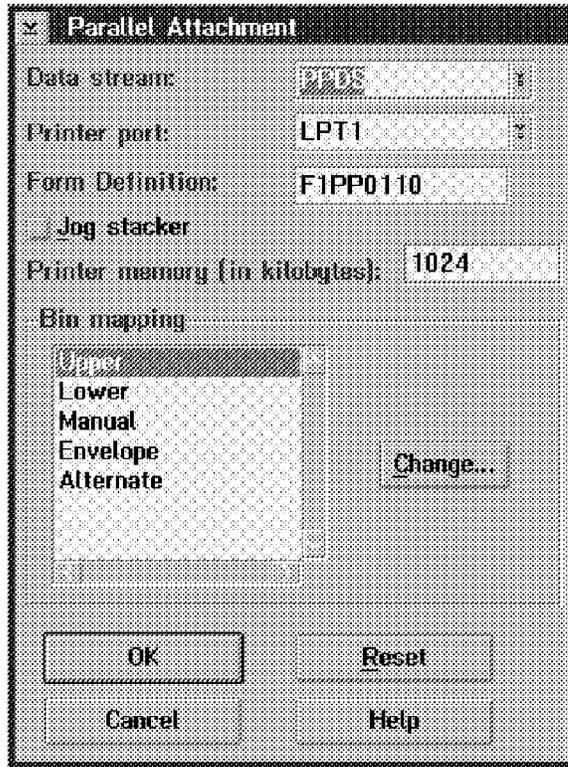


Figure 179. Parallel Settings Window

The Printer port can be a parallel port (LPTx), a serial port (COMx), a file or a redirected port. In the case of a redirected port, you must install the software to support the connection before configuring the printer attachment. The printer port pull-down list will show the available ports depending on the type of connection and its software.

The default Form Definition is set according to the data stream selected. You can change it to any other form definition present on the resource libraries.

You can select Jog stacker to cause the printer to separate jobs in the output bin (tray) using jog (offset) stacking. If the printer does not support jog stacking, this will have no effect in the output.

Printer memory defines the amount of memory that will be used during print processing. This value must be no greater than the amount of memory available in the printer.

You can select which input bin the printer will use. If you click on **Change...**, the Change bin mapping window shown on Figure 180 on page 242 will open.

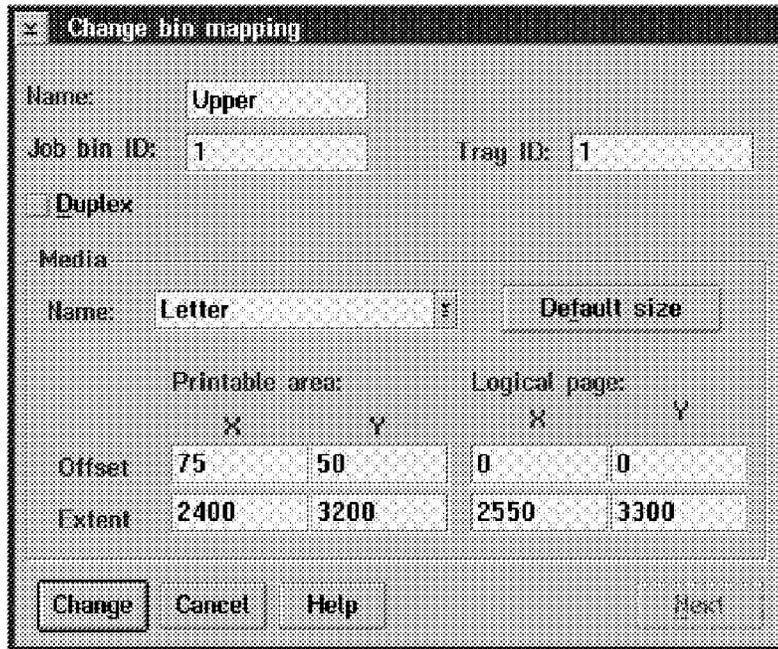


Figure 180. Change Bin Mapping Window

On this window, you can change the parameters for the paper bin selected.

3.4.4.2 TCP/IP Attachment Settings

The TCP/IP Attachment settings window is shown in Figure 181. For a TCP/IP printer attachment, you must provide the IP Address of the printer. You can change the default settings of the TCP/IP Port Number, the Form Definition and the Connect Timeout value.

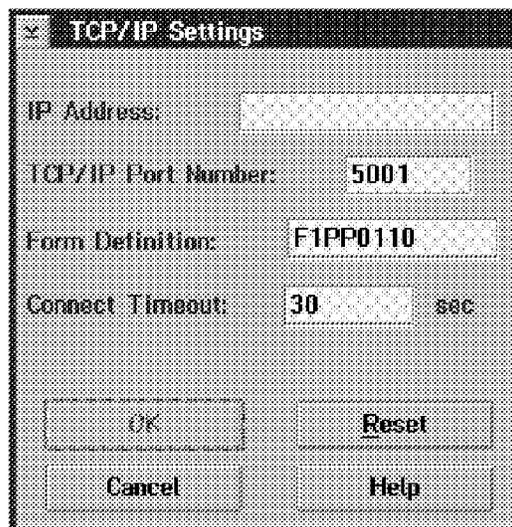


Figure 181. TCP/IP Settings Window

3.4.5 Creating a PSF/2 Queue

Once a print device is created and its settings are defined as seen in the previous sections, you need to create a queue for it. This is actually an OS/2 print object you create by doing the following:

1. On the PSF/2 Control Panel window, select the **Options** menu item.
2. Select **Setup queues**. The Setup queues window shown in Figure 182 will open.
3. Type in the name of the queue to be used with the device.
4. Type the description of the queue. This information is displayed under the item for the queue on the OS/2 desktop.
5. Make sure that the Device name selected in the Device list is the correct PSF/2 Device for this queue.
6. Select **Setup**, and a printer object will appear on the desktop.

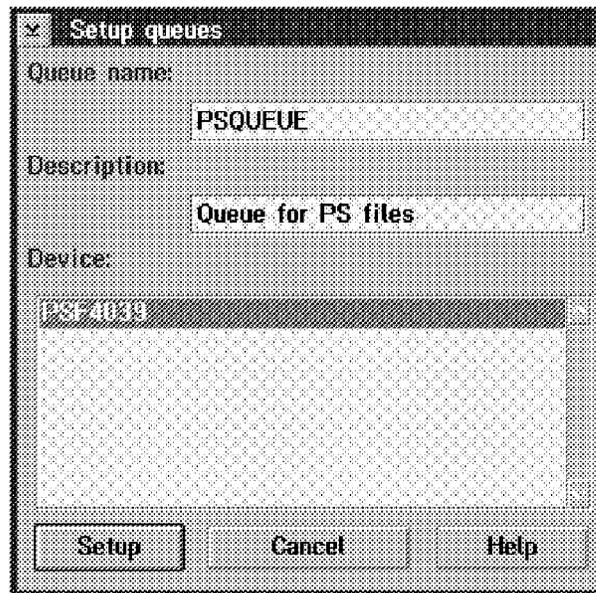


Figure 182. Setup Queues Window

3.4.6 Setting Up Transforms

PSF/2 can change data from one format to another so the data is in the appropriate format for the printer you select. Changing the data format is called a *data stream transform*. A *transform exit* lets you specify how the data is transformed.

You need to set up a transform exit, for example, when you want to print PostScript files. To specify a transform exit for a device from the PSF/2 Control Panel, do the following:

1. Select the device to associate with a transform exit.
2. From the Profile pull-down menu, select **Change...**, and then select **Transform options...**. This will open the window shown in Figure 183 on page 244.

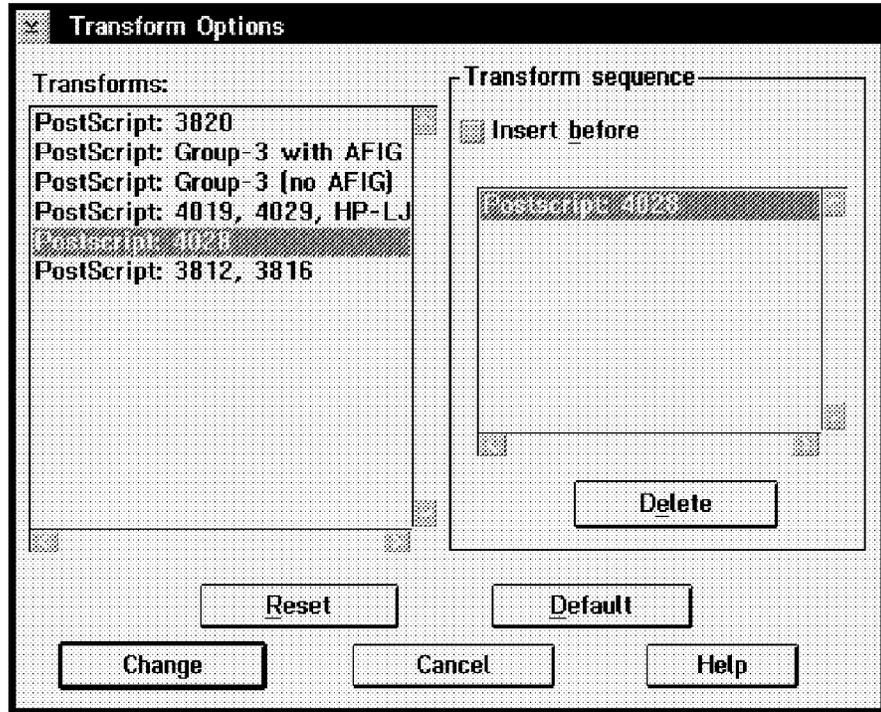


Figure 183. Transform Options Window

3. In the Transform Options window, double-click on the transform you'd like to use in the Transform list. The transform name will then appear in the Transform sequence list. For example, if you want to print PostScript documents on an IBM 4028 printer, double-click on the **PostScript: 4028** transform. Figure 183 shows the Transform Options windows after that selection was made.
4. Click on the **Change** button to save your selection. This will return you to the PSF/2 Control Panel window.

When you install PSF/2, only the PostScript to AFP transforms shown in Figure 183 are shown when you open the Transform Options window. There are, however, other transforms provided with PSF/2, including ones which allow you to define and use your own options. The list of these transforms is shown in Table 21:

DLL	Transform
PS2AFP	PostScript to AFP
WP2AFP	WordPerfect to AFP
AINXA2AF	ASCII to AFP
BPSHOAXO	DBCS ASCII to AFP
XFMNUP	PostScript to multiple-up PostScript
AINHU370	Upload-n-Print
XFMFLTR	Generic transform filter
DELSPFIL	Delete spool file

To use these transforms, they must first be added to PSF/2 by following these steps from the PSF/2 Control Panel window:

1. Select **Options** from the menu bar.
2. Select **Setup transforms** from the Options pull-down menu.
3. Select **Add**. The Setup transform window appears.
4. Select **Add**. The Add transform window appears.
5. Enter the name of the transform you want to add.
6. Enter the DLL name for the transform you're adding. Select from the list in Table 21 on page 244.
7. Select **Options** if you need to change any options for the transform you are adding. This will open the Options window, which is different for each transform. Make changes as needed, then click on **OK**.
8. Click on **Add** on the Add transform window. The transform you added will now be shown on the Setup transforms window.
9. Click on **OK** to return to the PSF/2 Control Panel main window.

You may need to define more than one transform for the same device. For example, you may want to print WordPerfect files in addition to PostScript files. For this, you can define a transform exit sequence. Following the same procedure listed above, you can choose more than one transform to add to the transform exit list. The transforms will then be processed by PSF/2 in the sequence listed, based on the data type of the print job.

3.4.7 Generic Transform Filter

One of the transforms provided with PSF/2 is XFMFLTR.DLL, which is the *Generic Transform Filter*. When XFMFLTR is included in a transform exit sequence, it allows you to include your own programs to process the data.

When you select **Options** for XFMFLTR, a generic window appears. You can then enter a command (such as a REXX program) that will be executed when PSF/2 reaches this transform exit.

Let's suppose, for example, you want to create a transform exit that will take a PostScript file and save it as an AFP file. You can do that by executing the following steps:

1. First, we'll create a transform for saving the AFP file that PSF/2 creates. We'll do this by using XFMFLTR. We start by selecting **Setup transforms...** from the PSF/2 Control Panel *Options* pull-down menu.

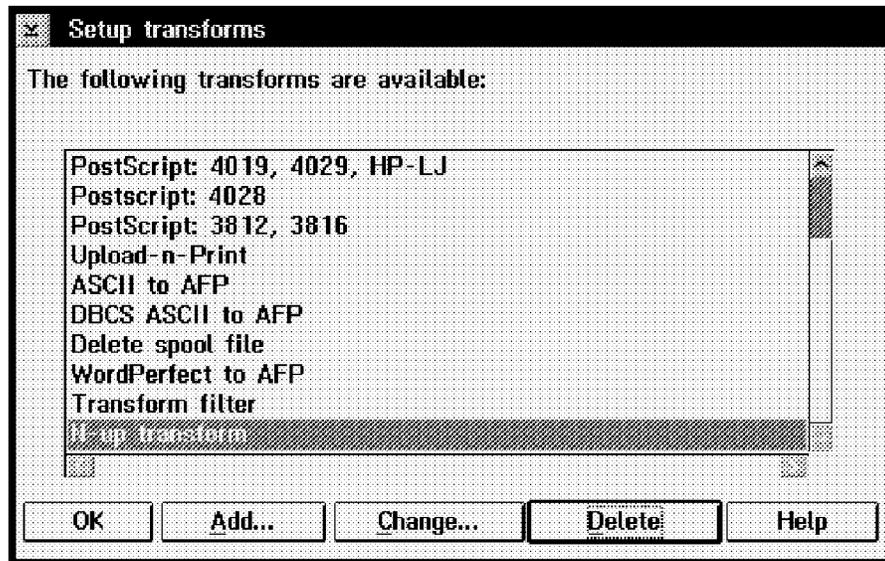


Figure 184. Setup Transforms Window

2. The Setup transforms window shown in Figure 184 will open. Select **Add...**

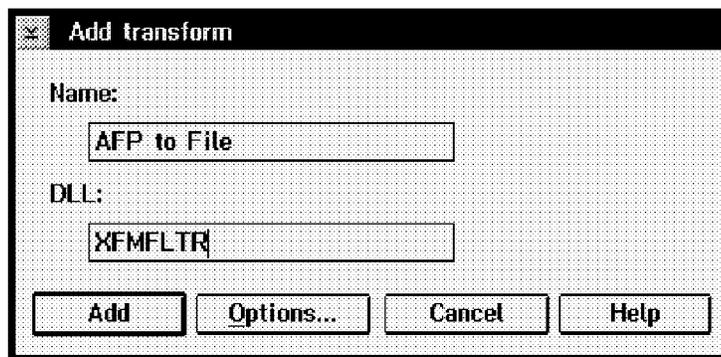


Figure 185. Add Transform Window

3. The Add transform window shown in Figure 185 will open. Fill in the name of this transform and the DLL. In this case, we'll use XFMFLTR. Select **Options....**

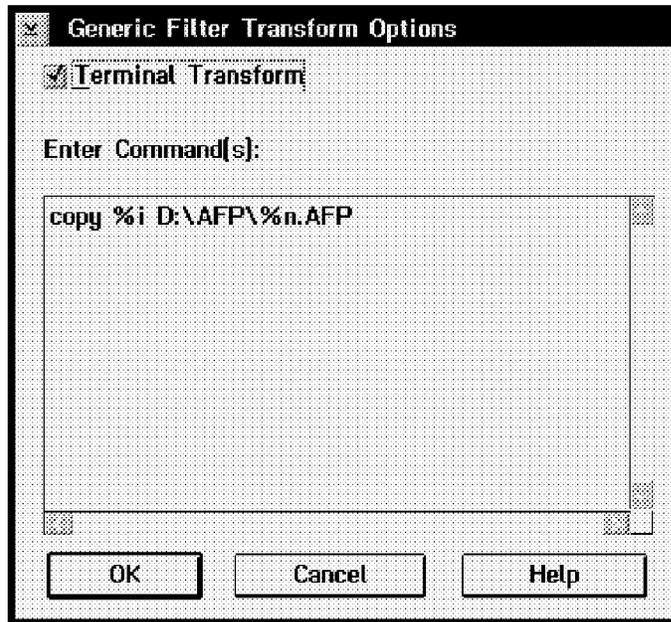


Figure 186. Generic Filter Transform Options Window

4. The options window for the Generic Transform Filter shown in Figure 186 will open. Here is where we'll enter the operations we want to execute. In this example, we're entering the following operation: `copy %i D:\AFP\%n.AFP`. What this operation will do is to copy the input to this transform (the `%i` variable) to a file in the `D:\AFP` directory, with the same file name (the `%n` variable) and with a file extension of `AFP`. Notice the Terminal Transform box on the top of the screen. What this box means is, whenever PSF/2 executes this transform, it will not go any further, even if there are other transforms in the transform sequence after this. In our example, we want to copy the AFP file and stop; so we'll check this box. After entering all operations, select **OK**.
5. On the Add transforms screen, select **Add**.
6. On the Setup transforms screen, select **OK**.

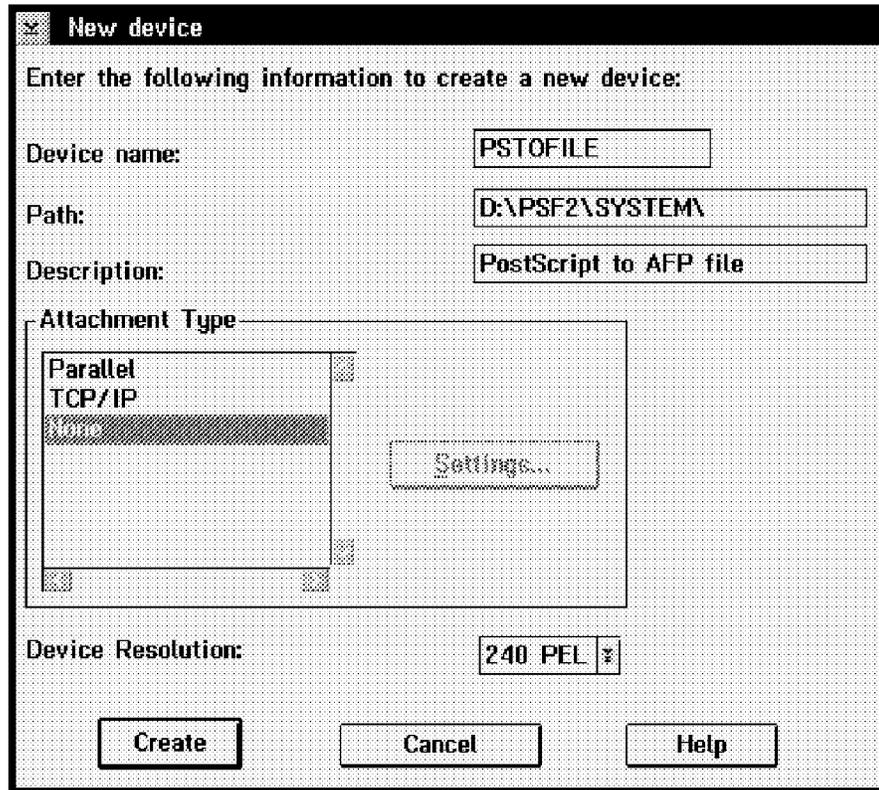


Figure 187. Creating a PSF/2 Device for the Transform Filter Exit

7. Now we need to create a PSF/2 device that will execute the transform without actually printing the data. From the PSF/2 Control Panel Profile menu, select **New...** On the New device window, enter the device name and description, and select **None** as the attachment type, as shown in Figure 187. Then, click on **Create**.
8. We have the device, and we have the transform that will copy the AFP file. Now all we need is to transform our PostScript file into an AFP file. On the PSF/2 Control Panel Profile menu, select **Change**; then select **Transform options...**

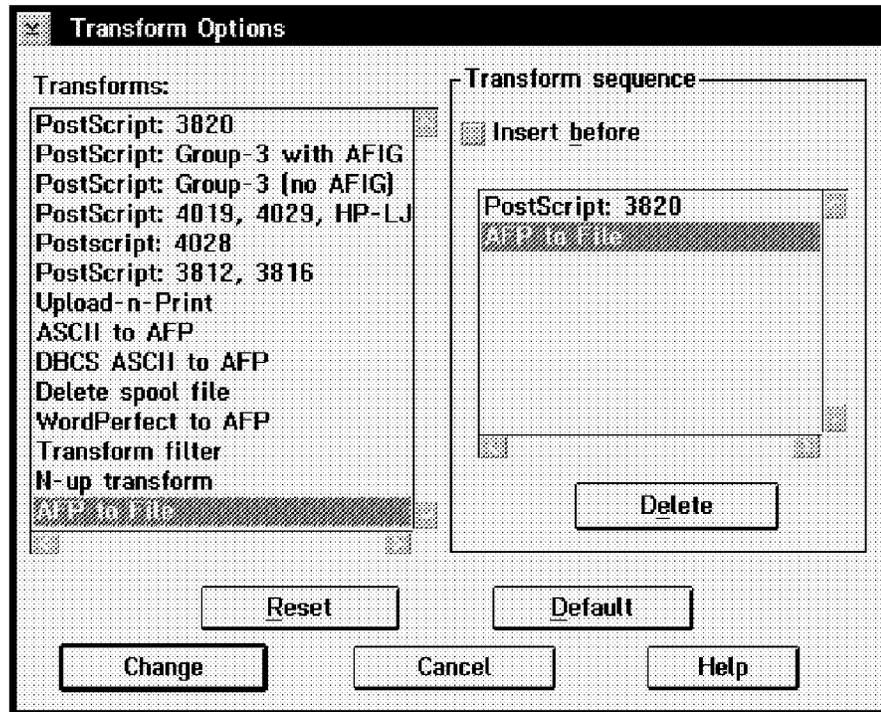


Figure 188. Creating a Transform Sequence

9. This will open the Transform Options window. Click on **PostScript: 3820** from the Transforms list, then on **AFP to File**. The two transforms will be added to the Transform sequence on the right. Now, click on **Change**.

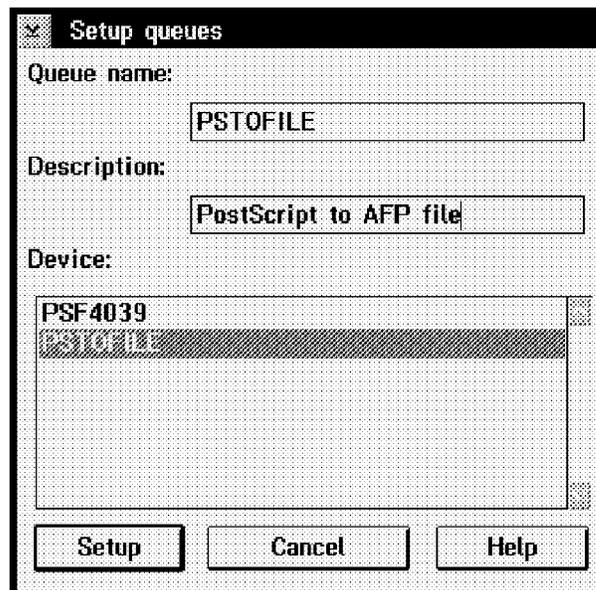


Figure 189. Creating a Queue

10. Back to the PSF/2 Control Panel, we only need to do one more thing. If you said "create a queue", you're right! On the Options menu, select **Setup queues....** Then, on the Setup queues screen, enter the queue name and description. Be sure you have the right device selected; then click on **Setup**.

Now, every time you send a PostScript file to the PSTOFILE queue, the PostScript file will be converted to an AFP file, this file will then be copied to the D:\AFP directory with an extension of .AFP.

Note

You cannot select the **Output to file** option in the OS/2 printer object output port when you're using a PSF/2 printer port. If you need to send print data to a file, set up a transform exit for that.

In the example, we used the variables %i and %n. XFMFLTR provides these and other substitution variables. They are:

- %i** Name of the input file in the spool
- %o** Name of the output file which PSF/2 will be looking for, if processing is to continue after the transformation
- %j** Name of the job being printed, this is the name of the original file, unless the APRINT JOBNAME parameter has changed it
- %n** Name of the job being printed but without its extension part
- %d** Name of the type of data in the input file
- %q** Name of the print queue
- %#** Spool ID of the input file
- %a** APRINT command line parameters, if any

3.4.8 PostScript, HP-PCL and HP-PGL Passthru

If you have native PostScript or HP-PCL printers on your server, you can set up a transform exit so that any PostScript or PCL files will go directly to the respective printers. This is possible by using XFMFLTR.DLL because the transform filter allows us to specify that an operation be executed only for a particular type of data.

For example, the following line:

```
PS;COPY /b %i LPT1
```

tells XFMFLTR to copy the input file directly to the LPT1 port only if it is a PostScript file. If the input file is not in PostScript format, this transform exit will be bypassed.

If we use PCL instead of PS in the example above, the same is true for HP-PCL or HP-PGL files.

3.4.9 Upload-n-Print Transform

Another transform exit provided with PSF/2 is the Upload-n-Print transform, AINHU370.DLL. This transform provides a way of sending LAN print jobs directly to an AFP printer on an MVS or VM host system.

The Upload-n-Print transform accepts file in AFP data stream format. It sends the file to the host system through a 3270 emulation session using OS/2 Communications Manager/2. A program in the host (provided with PSF/2) receives the file, reblocks it, and sends it to the host PSF program to be printed on the selected printer.

The details on how to set up PSF/2 and the host system to use the Upload-n-Print transform are in the *What's New* manual in the PSF/2 online documentation. It is also possible to write a generic uploader using TCP/IP LPR.

3.4.10 Using the **APRINT** Command

Another way of sending files to be printed by PSF/2 is by using the `APRINT` command from the OS/2 command line. The `APRINT` command has a variety of parameters that allow you to select the same kind of options as when using the PSF/2 Print Submitter. When would you use the `APRINT` command instead of the Print Submitter? When you know exactly what file you want to print and the parameters associated with it. Or you can write a procedure (an OS/2 `.CMD` file) and use the `APRINT` command from inside it. The `APRINT` command syntax can be listed by typing `APRINT ?` at the command line. It is also covered in both the *PSF/2 Online Reference* and in the PSF/2 documentation listed at the end of this chapter.

Tip

If you are unsure of the destination when using the `APRINT` command to print a file, type `APRINT <filename> dest=?`. The error message will list the possible destinations.

3.4.11 Using the **PSF/2 Print Submitter**

The Print Submitter is one of the ways in which you can send files to be printed by PSF/2. With the Print Submitter, you can print files that contain the following types of application data:

- ASCII from any OS/2 application
- Metafile from OS/2 graphical applications
- AFPDS from AFP applications, from the LAN or downloaded manually from a host
- PostScript (using a PostScript transform)
- WordPerfect (using a WordPerfect transform)

To use the Print Submitter, follow these steps:

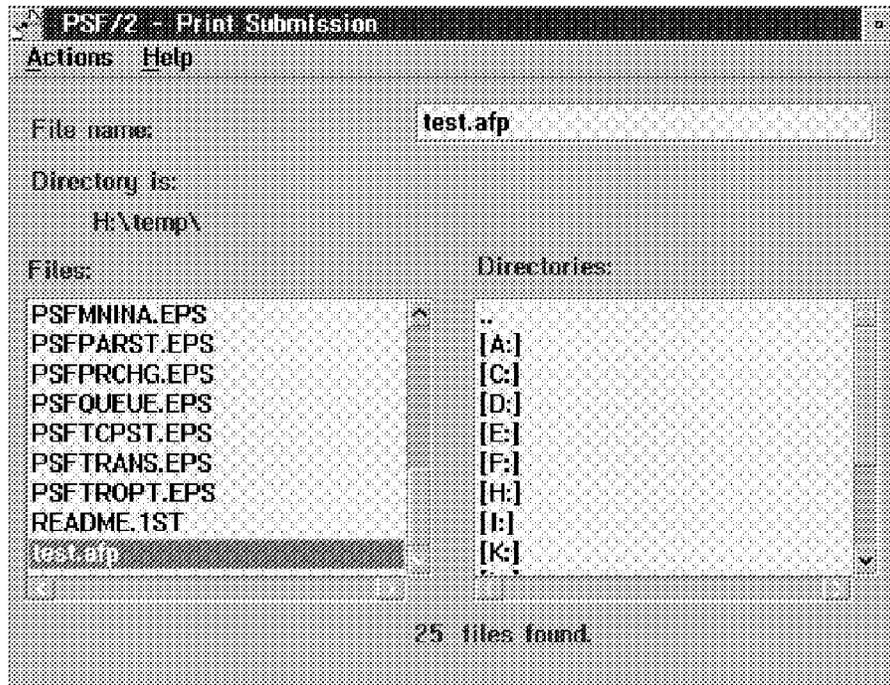


Figure 190. Print Submission Window

1. On the PSF/2 folder, click on the **Print Submitter** icon. The Print Submission window shown in Figure 190 will open. It shows a list of the files in the current directory on the left side and a list of directories and drives on the right side.
2. Select a directory from the Directory list
3. Select one or more files from the Files list. In the example, file *test.afp* on the *d:\temp* directory was selected.
4. From the Actions pull-down, select **Print**; then select either **Use current print options** or **Change print options**. For this example, let's assume you chose to change the print options. The Print window shown in Figure 191 on page 253 will open.

From this window, you can change many different print options. You can save your settings for later use by clicking on the **Save...** button. You can choose one of the existing profiles, or you can save the settings to a new profile by typing in a new profile name.

5. Once you've selected your options, click on **Print**.

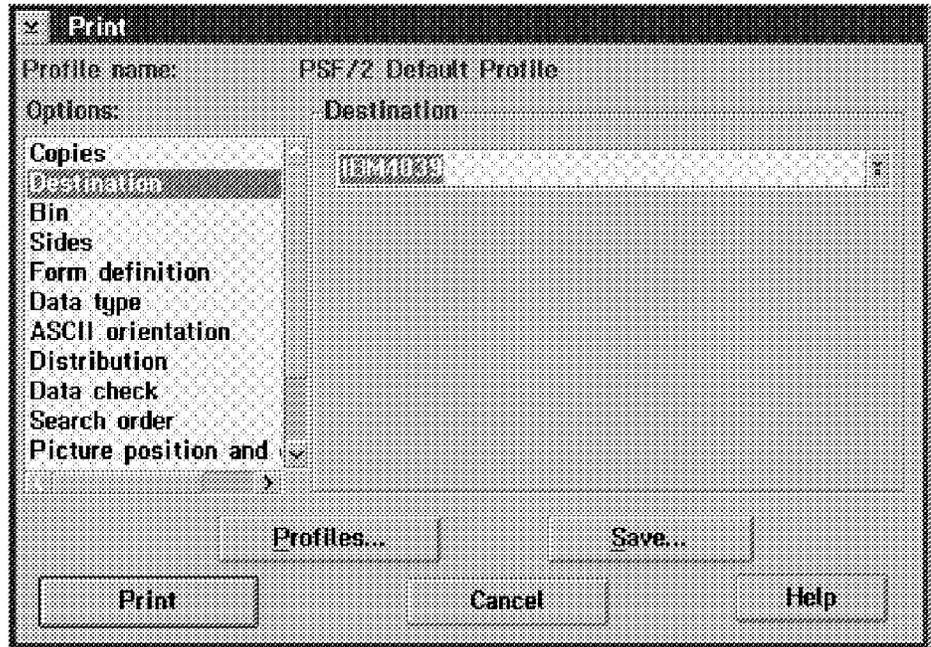


Figure 191. Print Window

3.4.12 PSF/2 Resource Library

Print resources are data objects that are referenced by a data stream to provide print information or data to be printed. PSF/2 uses the following types of resources:

- Fonts** The character sets used to print the text in a print job. A font is a collection of graphic characters that share the same type family, style, weight, width, and size.
- Overlays** Electronic forms that contain predefined, constant data (such as lines, boxes, shading, text or logos) that can be merged with variable data (such as customer name, address and account number) on a page while printing.
- Page Segments** Resources that contain text, graphics and/or images, and can be included at any addressable point on a page or overlay.
- Form Definitions** These resources define the characteristics of a print job. Form definitions contain descriptions of how composed text is positioned on a physical page as well as information such as the number of copies to print, what paper bin is to be used, and whether or not duplexing is desired.

The print resources a job needs can be packaged as part of the job, and in this case are called *inline resources*, or they can be stored in *resource libraries*.

Provided with PSF/2 is a large set of print resources. PSF/2 groups the print resources in *resource groups*. When you install PSF/2, all the resources provided are in a group called AINBASE. To manage the print resources and print groups, you can use the PSF/2 *Resource Librarian*, which can be started from the PSF/2 folder, or you can use a command line interface.

To use the Resource Librarian, click on its icon in the PSF/2 folder. Initially, you will see a list of all the resource groups. If you didn't add any new group, AINBASE will be the only one listed. To see a list of the resources in the AINBASE group, select the **List** menu; then select **AFP Resources....** The List AFP resources window shown in Figure 192 will open. On this window, you can select which resources you want to list, by Name, Type or Group.

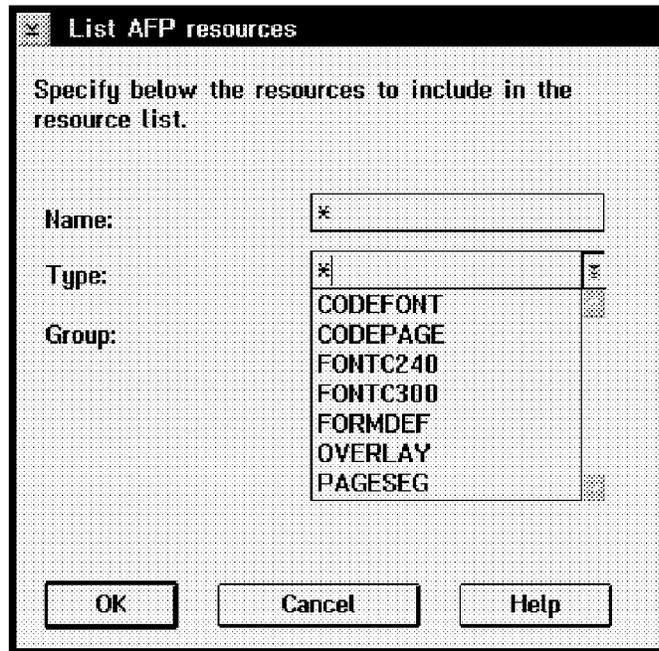


Figure 192. List AFP Resources Window

To list all the resources, leave all fields with asterisks; then select **OK**. The list will look like the one shown in Figure 193.

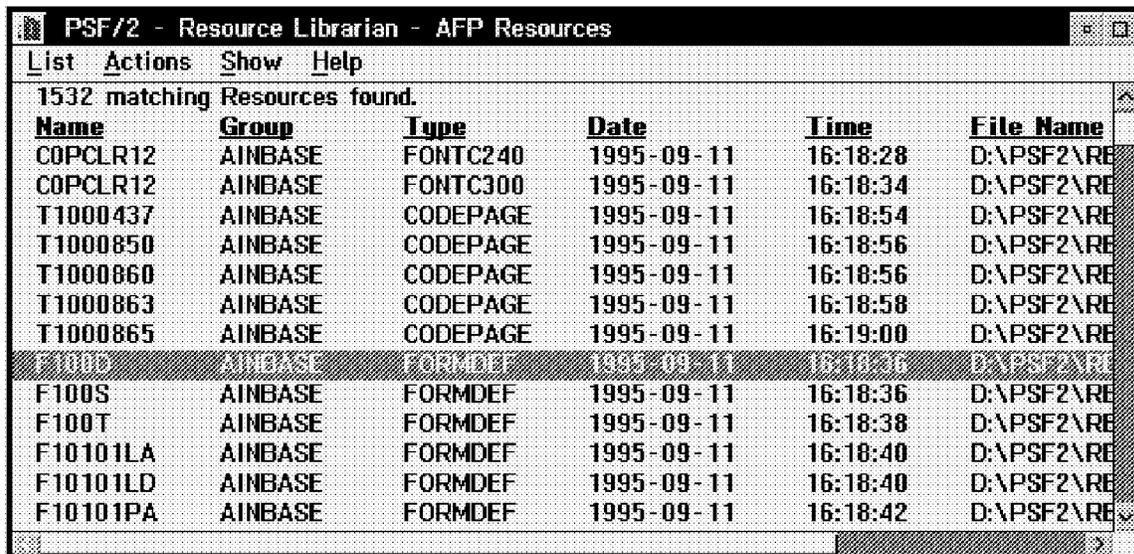


Figure 193. Resource Librarian - AFP Resources List

From the Actions pull-down menu, you can add, delete and rename any resource. You can also copy any resource to another group. If you're in the

Groups list, you can add or delete any group, or you can copy the contents from one group to another.

The same functions provided by the Resource Librarian can be executed from the OS/2 command line. All of the Resource Librarian commands start with the letters `RL`, so we have `RLADD` for adding groups or resources, `RLCOPY` for copying, and so on. See the Online help within Resource Librarian for additional information.

3.5 Bidirectional Print Support

Many modern printers are capable of two-way communication with the controlling system. These bidirectional (bidi) printers can send information to the system about their status, conditions requiring operator intervention, errors, statistics, and so on. The OS/2 Warp Server print spooler provides bidi printer support which provides better information for users and administrators. For example, when there's a problem in the printer, the printer object can show a message that describes the problem, such as *Load Paper*, instead of just indicating that the job is held in the queue.

Two GUI products that make use of bidi functions are provided with OS/2 Warp Server: MarkVision for OS/2 by Lexmark International, Inc. and HP JetAdmin for IBM OS/2 Warp Server by Hewlett-Packard Corporation. These products are discussed in the next sections.

3.6 MarkVision for OS/2

MarkVision for OS/2, by Lexmark International, Inc., combines with OS/2 Warp Server to enable users to easily install, configure, query, and troubleshoot network-attached printers. MarkVision supports the Lexmark Optra and 4039 Plus families of printers. These printers are capable of bidirectional communication with the print server using the Network Printing Alliance Protocol (NPAP).

MarkVision provides all of its status-monitoring capabilities without polling the printer. Since the printer initiates the alert message to the host where MarkVision is running, network traffic is kept to an absolute minimum. This is done by using an industry-developed protocol standard, IEEE P1284.1, for a transport-independent printer/system interface sometimes referred to as the Network Printing Alliance Protocol (NPAP). Lexmark is one of the founding members of the Network Printer Alliance.

MarkVision has no predetermined limit for the number of printers per server. However, for performance reasons, it is recommended that customers attempt to distribute their printers evenly among their available servers on their network.

By using MarkVision, network users and administrators will benefit from the following functions and features:

- Users can see the true status of their jobs (for example, Sending Job to Printer, Job in Printer, Job Printing) through the OS/2 Print Object. All users receive true end-of-job notification, thus avoiding wasted trips to the printer.
- Administrators can centralize setup and control of network printers on the OS/2 Warp Server print server. This allows an administrator to reduce

network traffic and to control access to network printers using OS/2 Warp Server's security services.

- Users can get the actual status of a printer from their OS/2 desktop. For example, a user can tell when a printer is out of paper or the printer's cover is open through the OS/2 Print Object or through visual and audio prompts in MarkVision.
- Users can remotely monitor, configure, and manage a network-attached printer from their OS/2 desktop. For example, an administrator can remotely lock the front panel of the printer to prevent others from changing the configuration of the printer or remotely press buttons to access and change settings on the printer's front panel.
- When a user creates a network print object on their OS/2 desktop, OS/2 automatically installs the correct OS/2 printer driver on the OS/2 Client from a shared path specified by an administrator.
- Users and administrators can view and manage printers and their jobs through a single view rather than through multiple printer views on their OS/2 desktop.
- Users can view the capabilities of network-attached printers through the graphical user interface of MarkVision on OS/2.
- Users can collect, store and view a summary of job statistics information for any job printed on their printers including:
 - Number of pages per job
 - Time and date the job completed
 - User and workstation that submitted the job
 - Time- and date-stamped error condition recording
 - Number of duplexed pages versus simplex pages
- Users can view printer statistics including:
 - User-controlled page count
 - Page count since last Power On Reset (POR)
 - Page count for life of printer
- MarkVision supports fast setup of printers based on a previously set up printer with the MarkVision *Quick Setup* feature.
- MarkVision provides convenient access to the Network Port Driver's settings and setting up of the Lexmark MarkNet XLe and XL Network Adapters.

3.6.1 Installing MarkVision on a Print Server

To install MarkVision, you can either run INSTALL.CMD from the OS/2 Warp Server CD-ROM 2 root directory, or run MarkVision's SETUP.EXE in the \BPIU\MARKVISN directory. If you run INSTALL.CMD, the first screen you'll see is the Warp Server CD-ROM 2 Panel shown in Figure 194 on page 257.

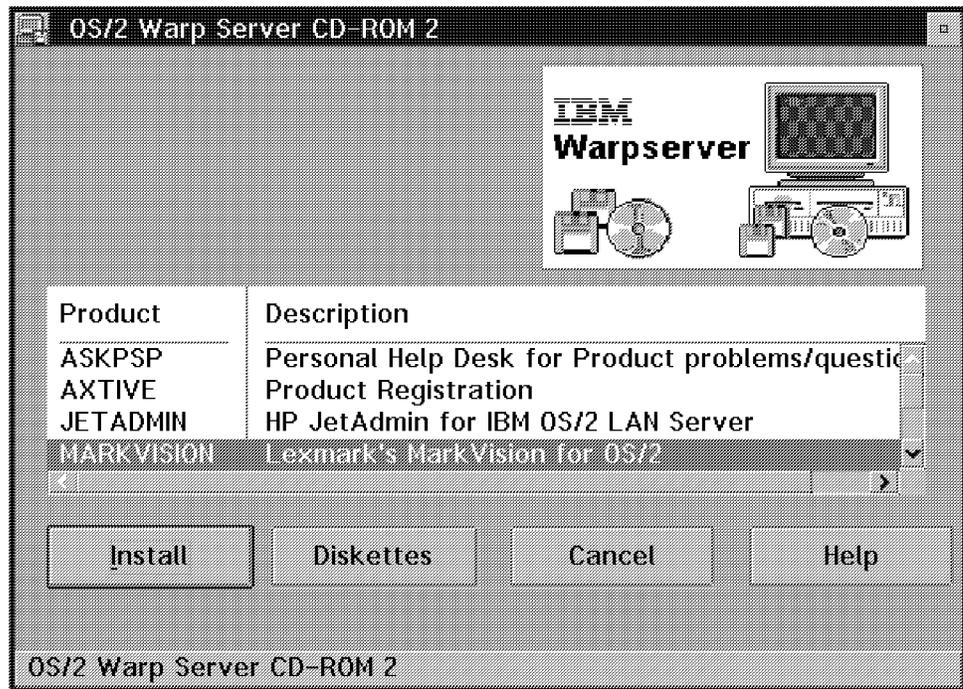


Figure 194. Warp Server CD-ROM 2 Panel

Protocol Required

The MarkVision Utility requires the 802.2 protocol to be configured for the adapter card being used. If this is not installed, use the Adapter and Protocol Service icon within the Startup Folder to do so. The MarkVision installation process can complete without 802.2 support, but configuration and usage of the utility requires 802.2.

By selecting MarkVision on this screen and clicking on the **Install** button, you will get to the MarkVision Setup screen shown in Figure 195 on page 258. If you run SETUP.EXE from the \BPIU\MARKVISN directory, this is the first screen you will see.

Select **Install MarkVision client components** to install the programs. Select **Local copy** to install MarkVision into your local computer. MarkVision finds and monitors printers that are LAN-attached if print servers in your domain are using the MarkNet port driver. MarkVision will also find printers on the LAN if you have the Print Server components installed locally.

Select **File server copy** to create a copy on a server disk from where other users can install MarkVision on their client machines. If you want the MarkNet port driver to be installed and accessible by others, also choose **Install Print server components**.

If you want to prevent users from installing the MarkNet port driver on their local systems when running this setup program from your server, select **Yes** when you are presented with this question. If users are allowed to install and use the port driver locally, you lose control over the management of your printers.

Select **Install Print server components** to install the MarkNet port driver and protocol converters. The MarkNet port driver enables you to monitor a printer

that's using a Lexmark network printer adapter (such as a MarkNet or MarkNet XLe adapter).

After selecting the components you want to install, click on the **Install** button. The installation process will continue.

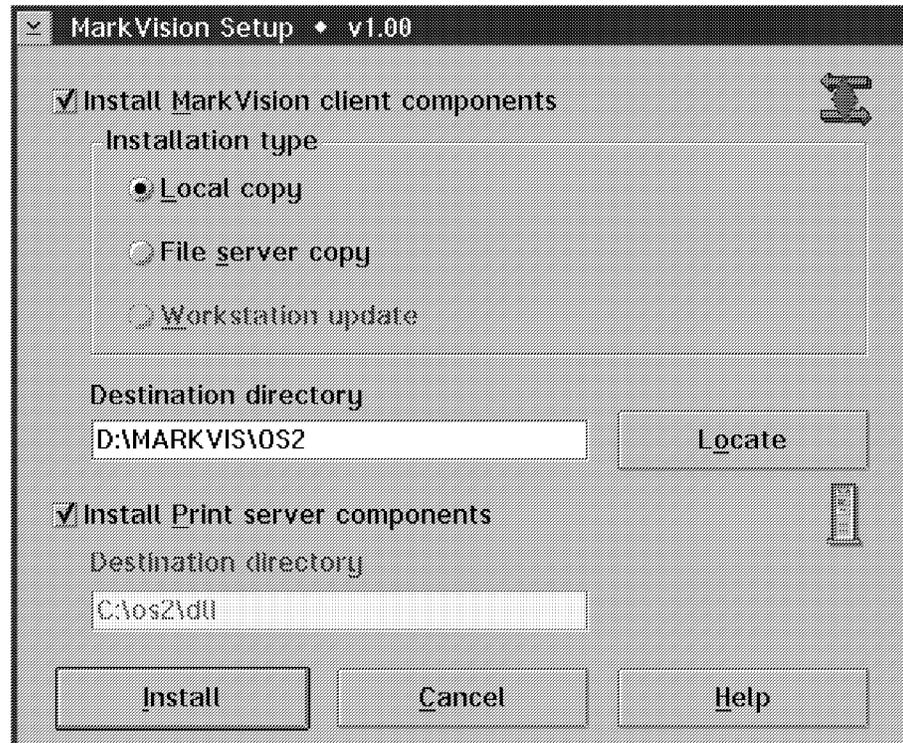


Figure 195. MarkVision Setup Screen

To install certain components, the installation program must disable the OS/2 spooler. When this happens, you will see the following prompt: `Jobs printed directly - spooler disabled`. Select **OK** in response to it. At the end of the installation, the spooler should be enabled. If for any reason the spooler is left in a disabled state, you'll have to enable it. To do this, click the right mouse button while on an empty area of the desktop and select **System setup**. On the System Setup window, click the right button on the Spooler icon; then select **Enable spooler**. You can also enable the spooler by typing `SPOOL` on a OS/2 command line.

When the installation is completed, there'll be a MarkVision icon on the OS/2 desktop.

3.6.2 Installing MarkVision on a Client Workstation

If you choose to install the file server copy of MarkVision in your server, users can install MarkVision in their workstations. To do this, a user must be accessing the network drive where the MarkVision server copy resides. To install MarkVision on a client workstation:

1. From the directory where the MarkVision server copy resides, type `SETUP`. The MarkVision Setup menu will open (see Figure 195).

Note: If during the server copy installation you chose to prevent the installation of printer server components, the menu will not show this option.

2. Select the type of installation. You can install a local copy of the MarkVision code by selecting **Local copy**, or you can select **Workstation update** for running MarkVision from the network drive. In this case, no code will be copied to the client workstation. A MarkVision program object will be created on the OS/2 desktop, and MarkVision will use the directory you specify to create a profile, MV.INI, the first time it is run.
3. After making all selections, click on the **Install** button to continue the installation.

3.6.3 Configuring MarkVision

The first time you click on the MarkVision object, a window will open, and you will see a message on the bottom bar of the window: *Enumerating Printers....* This message will be on while MarkVision is looking for printers it can identify. If no printers were previously defined for MarkVision, nothing will appear on the window. You need to configure MarkVision for the printers you want to control. Actually, what you will configure are *MarkNet Printer Port Drivers* for each printer you want MarkVision to control, and then you can use these printer ports as any other OS/2 printer port. To do this:

1. On the MarkVision window, click on **Install MarkNet port** on the Utilities pull-down menu. The MarkNet Port Driver Settings window shown in Figure 196 will open.

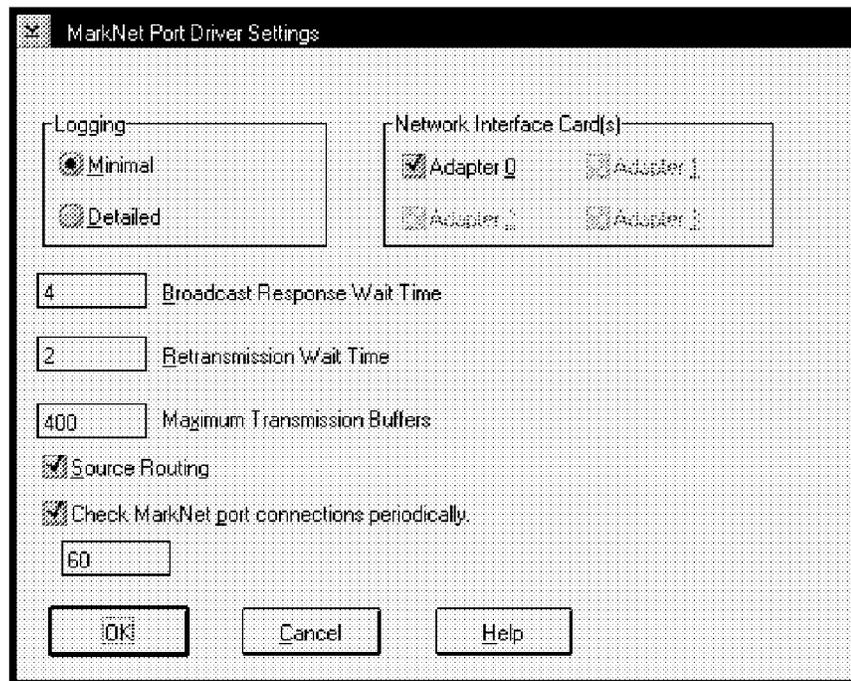


Figure 196. MarkNet Port Driver Settings Window

2. Usually you won't need to change its default settings; so just click on **OK**. You will see a message window: *Searching for adapters on the network. Please wait...*, while MarkVision interrogates the network to find all printers it can control. The time it takes depends on the size of the network and the number of printers.
3. Next, the MarkNet Network Port Driver notebook shown in Figure 197 on page 260 will open.

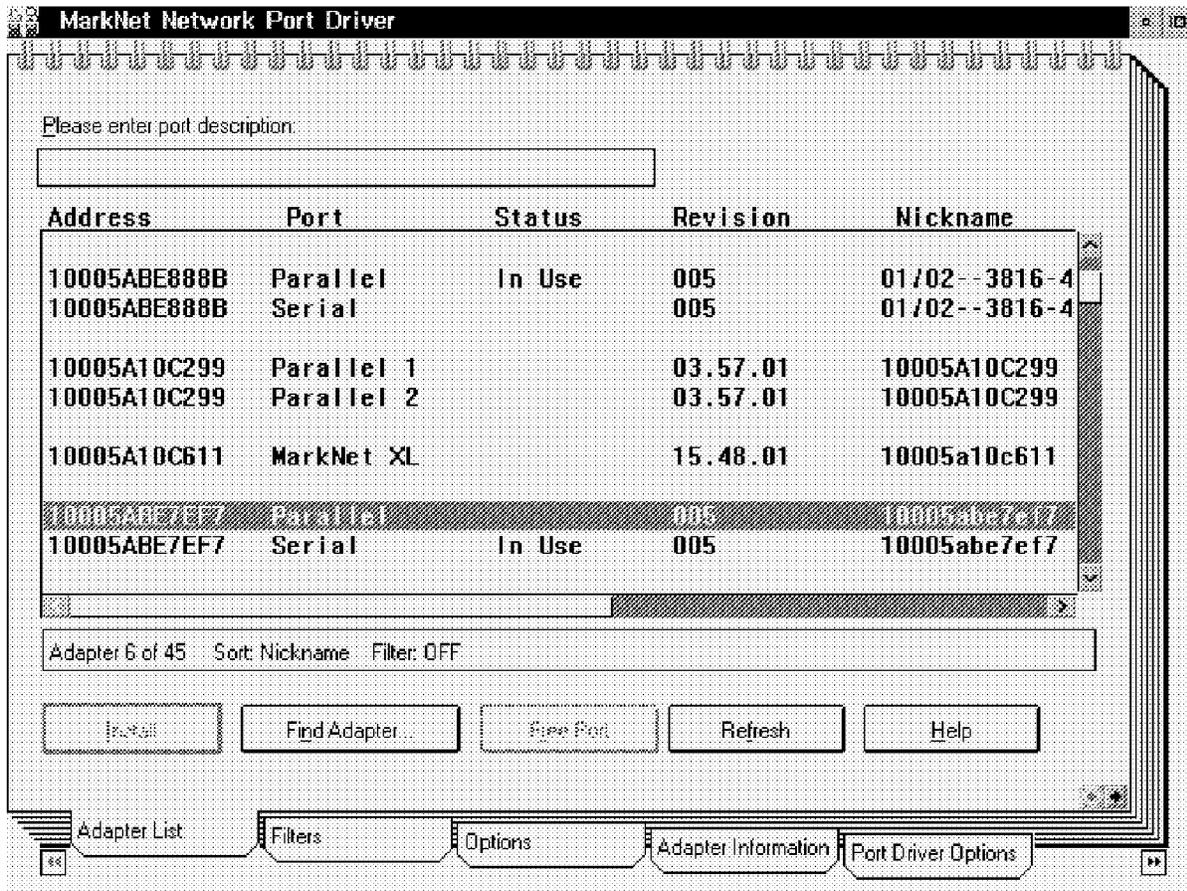


Figure 197. MarkNet Network Port Driver Notebook - Adapters List Page

Here you see a list of all printer adapters identified by MarkVision on the network. The adapter list shows:

- A set of entries for each MarkNet XLe adapter on the network (one entry for each parallel port, and one entry for the serial port, where supported)
- One entry for each Integrated Network Option adapter (MarkNet or MarkNet XL adapter) on the network
- A pair of entries for each 4033 adapter on the network (one entry for the parallel port and one entry for the serial port)

Each entry has up to five fields: Address, Port, Status, Revision, and Nickname. The meanings of these fields are as follows:

Address A unique address that refers to the network adapter itself. It does not refer to a specific adapter port because, for 4033 and MarkNet XLe adapters, there is more than one port at each address. Each address appears as 12 hexadecimal digits. This is either:

- The Universally Administered Address (UAA), or
- The Locally Administered Address (LAA), if you have assigned one

Port The adapter output ports which send data to printers, not the port connecting the adapter to the network. There are several types of output ports:

- Serial (for a 4033 adapter or a MarkNet XLe Model 301)
- Parallel (for a 4033 adapter)
- Parallel 1 (for MarkNet XLe parallel port 1)
- Parallel 2 (for MarkNet XLe parallel port 2)
- MarkNet (for Integrated Network Option adapter)
- MarkNet XL (for Integrated Network Option adapter)

Status Shows two possible states:

- <blank>. The port is available for use by any server on the network.
- In Use (for 4033s only) - Another server is associated with the 4033 port, making it unavailable. In Use does not mean that the attached printer is currently printing (although it may be).

Revision The revision number of the firmware (level of software) that the adapter is using.

Nickname A name you assign to an adapter. The Nickname field lists the nicknames you assigned to the adapters. The default nickname given to every adapter is the Universally Administered Address (the original address given at the factory). Therefore, when you view the nicknames, you may see some UAAs listed first, followed by nicknames you have assigned.

4. Select on the list a printer for which you want to create a MarkNet port driver. Now enter a description for it in the port description field. When you enter a description, the **Install** button will be unblocked. Click on it to install the MarkNet port driver.

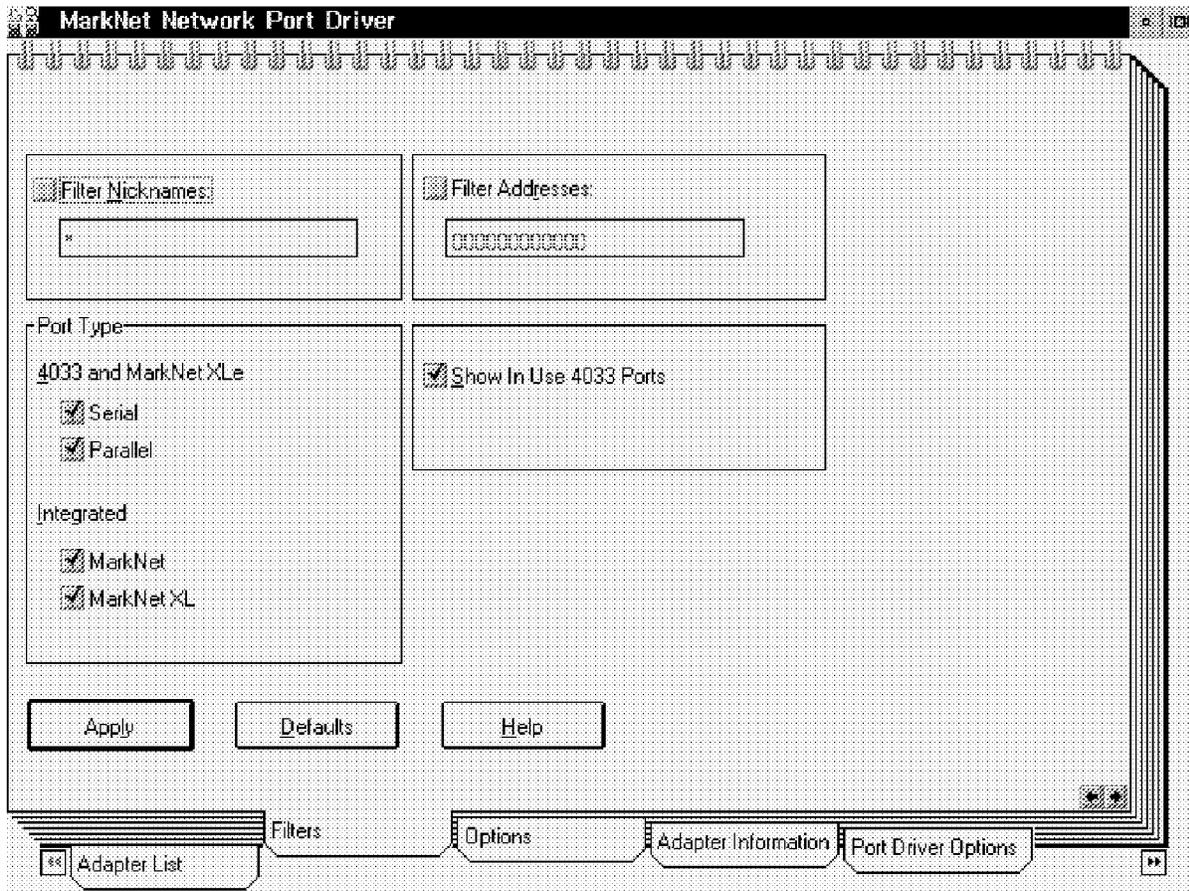


Figure 198. MarkNet Network Port Driver Notebook - Filters Page

The MarkNet Network Port Driver notebook has other pages besides the adapter list page. The Filters page shown in Figure 198 allows you to restrict the list of adapters to certain types, nicknames or addresses. This is useful when you have a large number of printers and want to reduce the size of the list you have to work with.

The Options page shown in Figure 199 on page 263 allows you to select certain options to make the list more readable. You can eliminate the firmware information and the spaces between adapters.

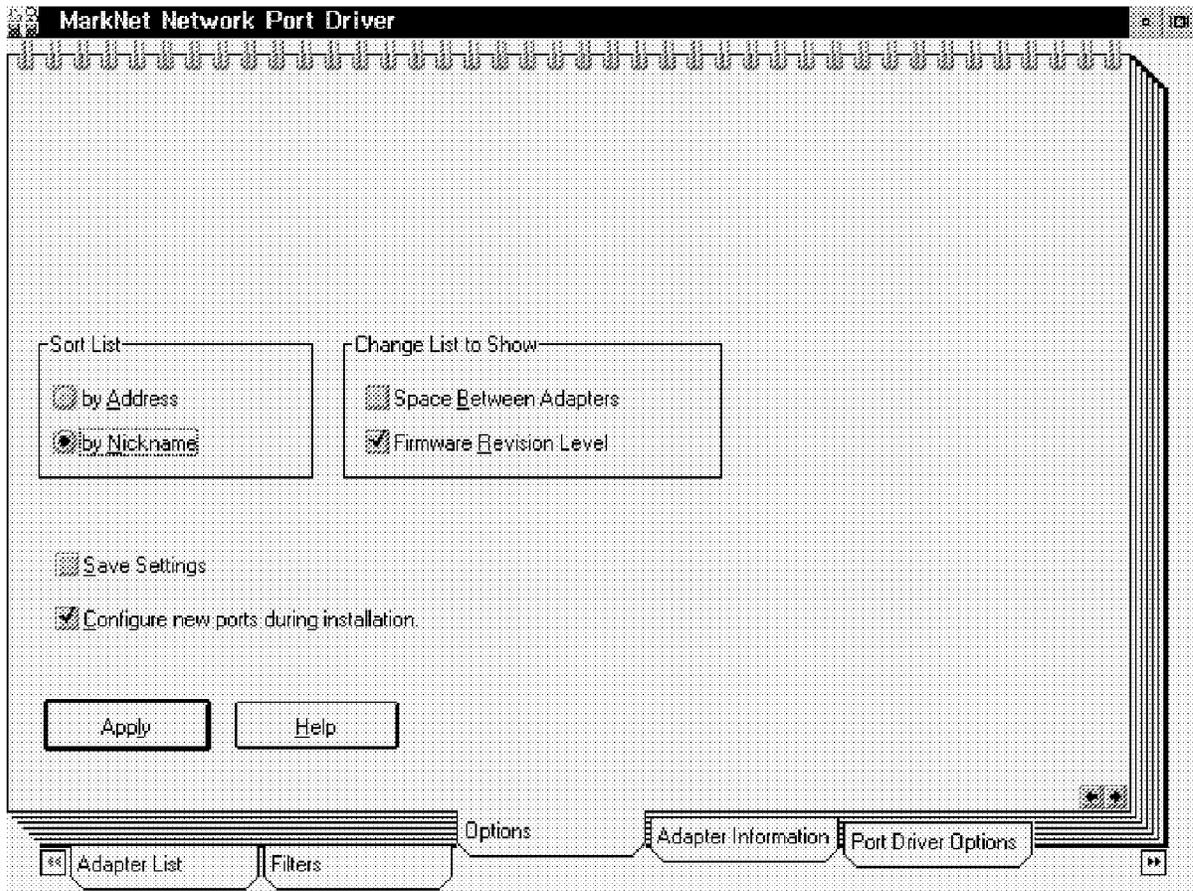


Figure 199. MarkNet Network Port Driver Notebook - Options Page

The Adapter Information page shows details about the selected adapter. The Port Driver Options page has the same information shown in Figure 196 on page 259.

3.6.4 MarkNet Port Driver on OS/2 Warp

Once the MarkNet port driver is created, it will be seen by OS/2 Warp as just another printer port. So, when you create a new printer object, or when you open the Settings window for an existing printer object, you will see in the printer ports list, a MarkNet port with the name you defined. This is shown in Figure 200 on page 264. By selecting this port for the printer object, all output sent to this printer object will be directed to the LAN printer connected to it.

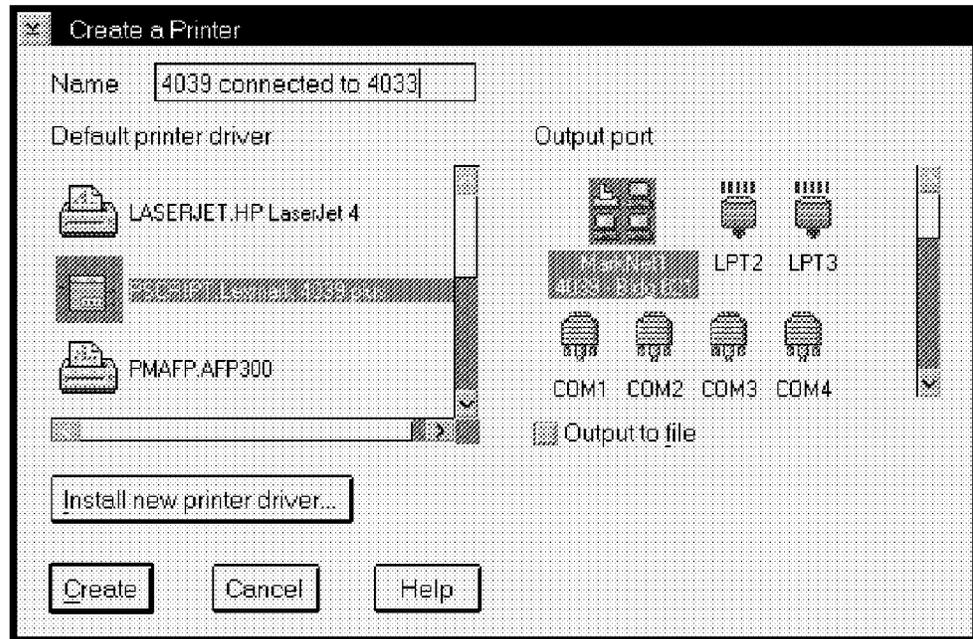


Figure 200. Printer Object with MarkNet Port Driver

3.6.5 Managing Network Printers with MarkVision

In addition to providing port drivers for LAN-connected printers, MarkVision provides a way of managing LAN printers from a centralized print server. The administrator can request and obtain information about the printer at any moment, and the printer can send information asynchronously to the print server when, for example, a paper input tray is empty, or the toner supply is low.

When you define a MarkNet port driver as seen in the previous section, a printer icon will appear in the MarkVision window, as shown in Figure 201 on page 265.

Note: All MarkNet port drivers will appear on this window, even if there are no OS/2 printer objects associated with them.

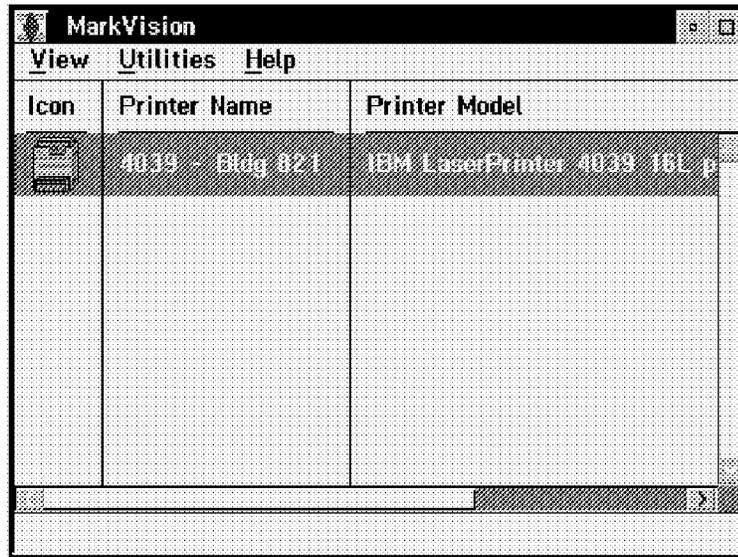


Figure 201. MarkVision Window

By selecting an icon on the list, a notebook for the selected printer will be opened. The contents of the notebook will depend on the model of the printer selected. Figure 202 shows a notebook for a LexMark 4039 Plus printer.

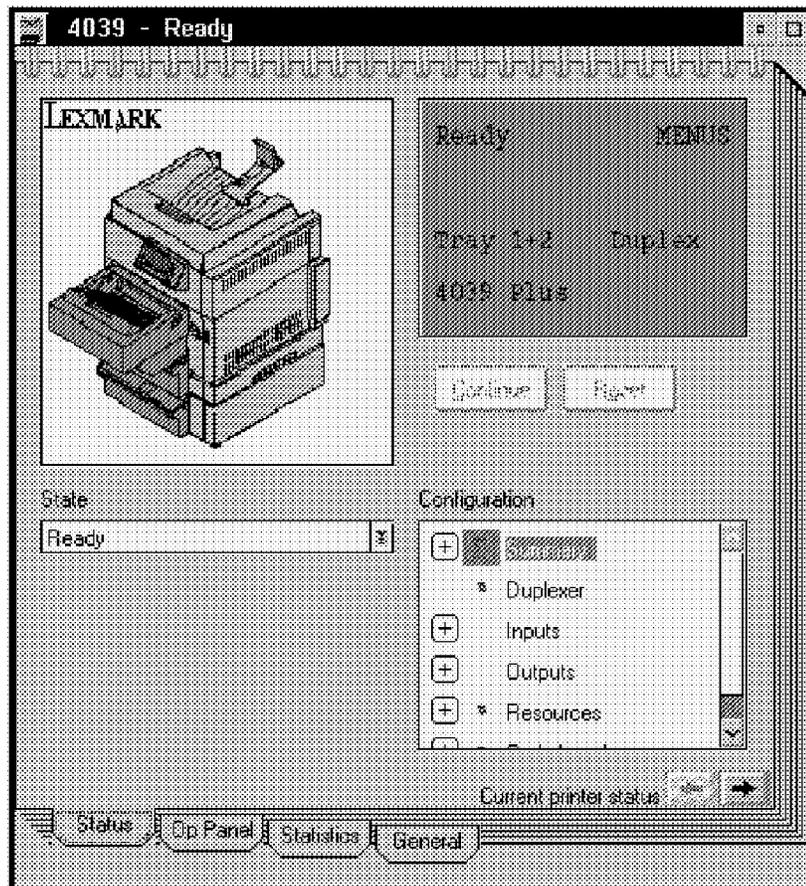


Figure 202. 4039 Notebook - Status Page

This first page of the notebook, shown in Figure 202, shows the printer status. You can see on the top left side a picture of the printer. On the top right side is a representation of the printer panel, with the same information you would see on the printer itself. On the bottom right side of the page, there's a menu with configuration parameters. By selecting a parameter, you can see its settings.

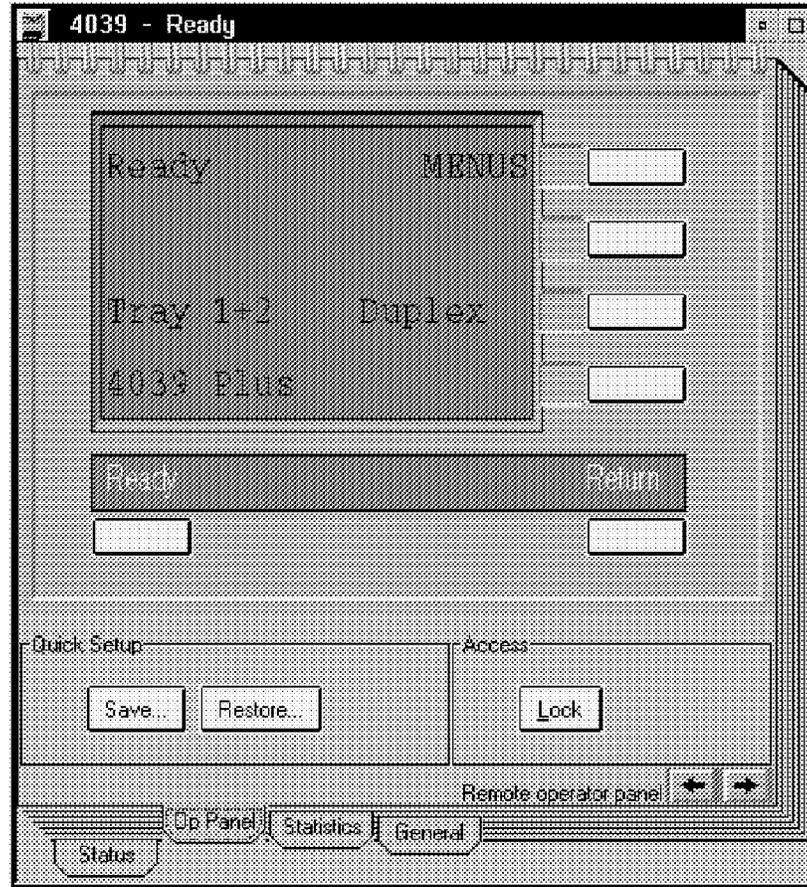


Figure 203. 4039 Notebook - Operator Panel Page

The second page of the 4039 notebook, shown in Figure 203 is the Operator Panel page. This is an exact representation of the 4039 operator panel, with its display and buttons. You can operate the 4039 remotely from here. For example, if you click on the button to the right of the word **MENU** on the display, you will see the display change to that shown in Figure 204 on page 267. From here, you can continue to any of the menus, or you can click on the **Return** button to return to the previous menu.

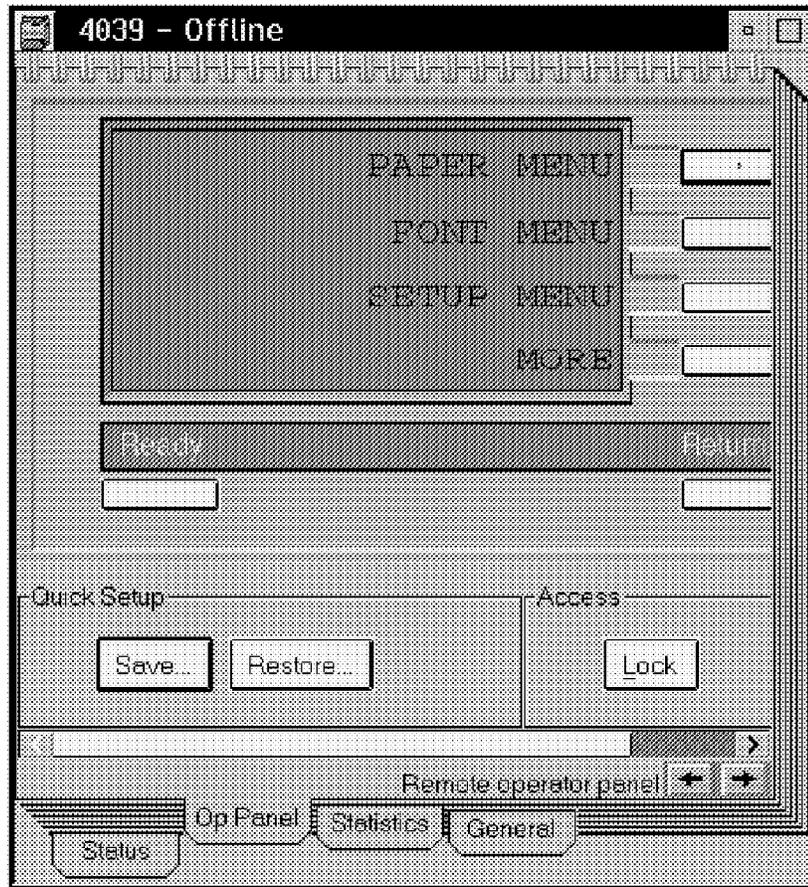


Figure 204. 4039 Op Panel Page - MENUS Selected

On the bottom-left of the page, you can see the Quick Setup buttons. You can save the printer setup data by clicking on the **Save...** button. You will be prompted for the file name. In this way, you can store different setup configurations for the printer, and load them any time you want by clicking on the **Restore...** button.

The last feature on this screen is the Access **Lock** button. By clicking on this button, the panel on the printer will be locked, and the printer can only be operated remotely via MarkVision. By clicking on the same button again, the panel will be unlocked (by the way, the button name will flip between *Lock* and *Unlock* as you click on it, so you'll know the present state of the panel).

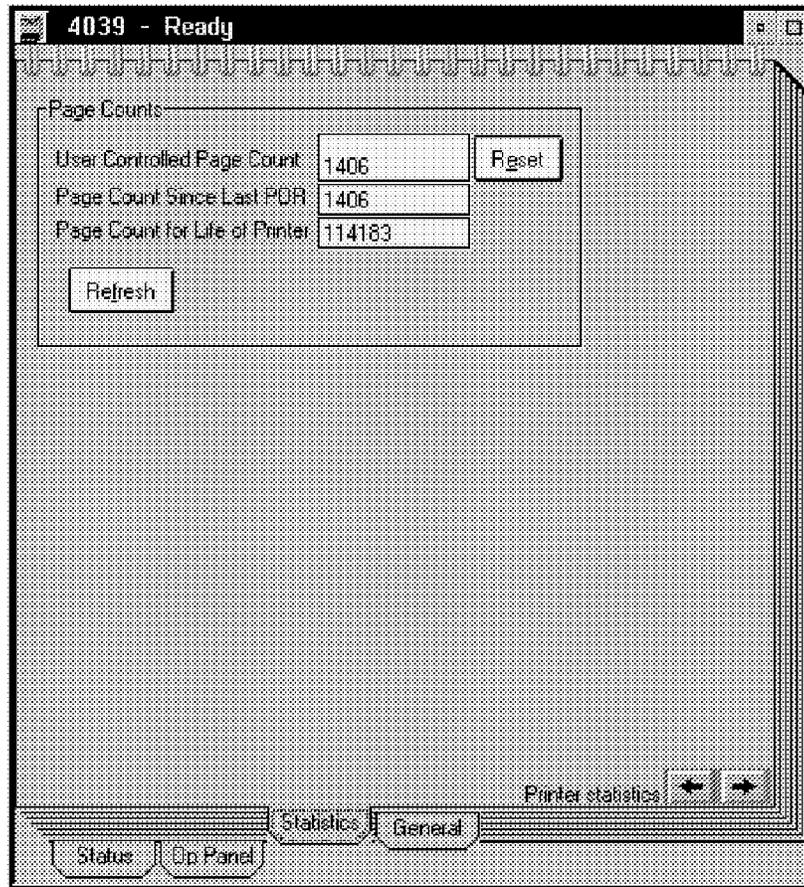


Figure 205. 4039 Notebook - Statistics Page

The third page on the 4039 notebook is the Statistics page shown in Figure 205. The **Reset** button will reset the User Controlled Page Count to zero. The second count is reset to zero on every Power-On Reset (POR). The third counter is never reset. The counts displayed will be updated when you click on the **Refresh** button.

The fourth and last page shows the name of the printer you assigned to it when you created the port driver. You can change it if needed.

When you have many printers on your network, the MarkVision main window may look like the example shown in Figure 206 on page 269.

MarkVision				
View Utilities Help				
Icon	Printer Name	Printer Model	Connection	Status
	Moe	Lexmark Optra LaserPrinter Lx	MarkNet13	Ready
	Larry	Lexmark Optra LaserPrinter Lx	MarkNet12	Ready
	Artie	Lexmark Optra LaserPrinter Lx	MarkNet11	Ready
	Chico	Lexmark Optra LaserPrinter Lx	MarkNet10	Ready
	Harpo	Lexmark Optra LaserPrinter Lx	MarkNet9	Ready
	Groucho	Lexmark Optra LaserPrinter Lx	MarkNet8	Ready
	4039 - Bldg. 800/1L045	IBM LaserPrinter 4039 12L plus	MarkNet7	Ready
	3116 - Bldg. 902/6E007	IBM 3116 Page Printer Lx	MarkNet6	Ready
	3116 - Bldg. 902/4E015	IBM 3116 Page Printer Lx	MarkNet5	Ready
	3116 - Bldg. 902/3E015	IBM 3116 Page Printer Lx	MarkNet4	Ready
	3116 - Bldg. 902/3E007	IBM 3116 Page Printer Lx	MarkNet3	Ready
	3116 - Bldg. 902/2D007	IBM 3116 Page Printer Lx	MarkNet2	Ready
	4039 - Bldg. 821	IBM LaserPrinter 4039 16L plus	MarkNet1	Load paper or envelope

Figure 206. Network with Many Printers

When you have a network with many printers, the advantages of using MarkVision become more evident. In this example, we can see many printers that are located in different buildings. The printer on the bottom has run out of paper, and this is indicated by the message on the Status field and by a visual indication over the icon on the left. If you select this printer, the status screen will be as shown in Figure 207 on page 270.

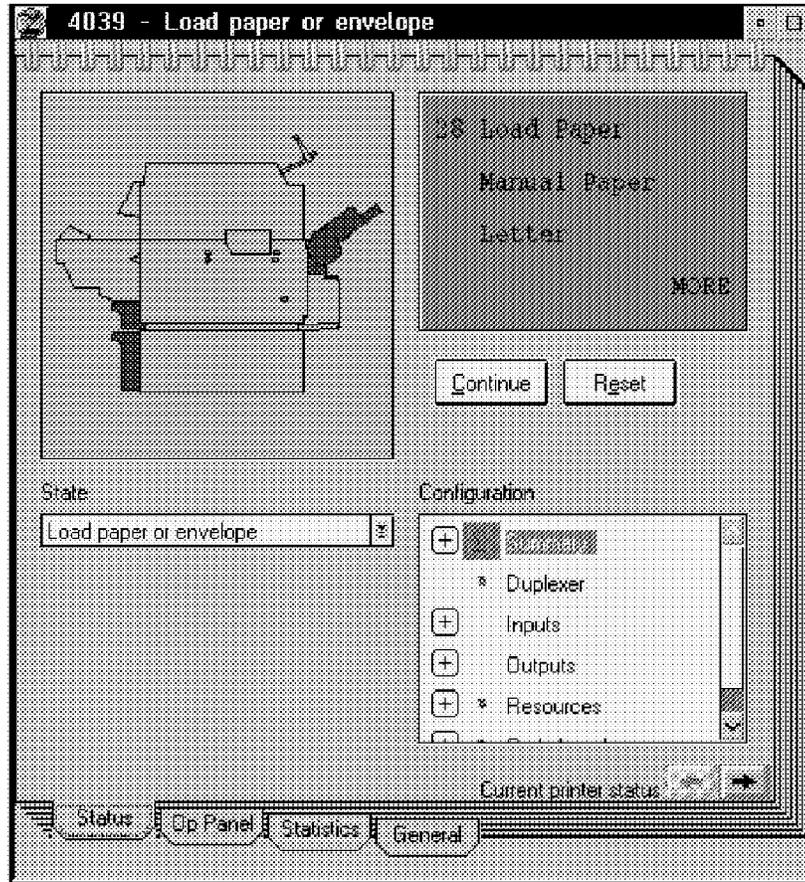


Figure 207. Printer Requiring Operator Intervention

You can see the parts of the printer requiring attention (in this case, the input paper bins) are highlighted - on a color display, they're shown in red.

3.7 HP JetAdmin for IBM OS/2 Warp Server

HP JetAdmin for IBM OS/2 Warp Server by Hewlett-Packard Corporation (HP) combines with IBM OS/2 Warp Server to enable users to easily install, configure, query, and troubleshoot network-attached printers. HP JetAdmin supports the most popular models of HP printers and plotters.

By using HP JetAdmin, network users and administrators will benefit from the following functions and features:

- Users see the true status of their jobs (for example, Sending Job to Printer, Job in Printer, Job Printing) through the OS/2 Print Object. All users receive true end-of-job notification. No more wasted trips to the printer!
- Administrators can centralize set up and control of network printers on the OS/2 Warp Server print server. This allows an administrator to reduce network traffic and to control access to network printers using OS/2 Warp Server's security services.
- Users can see the actual status of a printer from their OS/2 desktop. For example, a user can see when a printer is out of paper or the printer's cover is open through the OS/2 Print Object or through the graphical user interface of JetAdmin.

- Users can remotely monitor, configure, and manage a network-attached printer from their OS/2 desktop. For example, an administrator can remotely lock the front panel of the printer to prevent others from changing the configuration of the printer or remotely view and change settings on the printer's front panel.
- When a user creates a network print object on their OS/2 desktop, OS/2 automatically installs the correct OS/2 printer driver on the OS/2 Client from a shared path specified by an administrator.
- Users and administrators can view and manage printers and their jobs through a single view rather than through multiple printer views on their OS/2 desktop.
- Users can view the capabilities of network-attached printers through the graphical user interface of JetAdmin on OS/2.
- Administrators can assign up to 32 HP network-attached printers to an OS/2 Warp Server print server. To do this, set GDTS=80 and ELEMENTS=1400 in the LANDD_nif section of the PROTOCOL.INI file.
- When a printer error occurs while printing a job on a printer, a user can correct the problem, and OS/2 will automatically restart the job after the last successfully printed page. This saves valuable printer resources, such as paper and toner, and speeds throughput since users do not have to wait for a large job to be completely reprinted!
- Users can submit a print job to a printer and then specify a range of pages to print. For example, a user can submit a 100 page PostScript file to print and then choose to only print pages 10-20 rather than the entire document.
- JetAdmin provides convenient access and set up to the Network Port Driver's settings through the OS/2 Print Object.
- Network administrators can manage HP's network-attached printers from IBM's NetView product.

In summary, HP JetAdmin makes administrators more productive by giving them the tools to remotely manage network-attached printers from their OS/2 desktop. They are no longer required to go to the printer or print server to determine status or to isolate problems. Users increase their productivity by receiving true printer and job status on their OS/2 desktop.

3.7.1 HP Jetadmin Device Support

HP JetAdmin supports these HP printers and plotters with HP JetDirect print servers:

- MIO Devices
 - *HP LaserJet 4, 4M, 4 Plus, 4M Plus, 4V, 4MV, 4Si, 4Si MX printers
 - HP LaserJet IIISi printer
 - HP Color LaserJet printer
 - HP DeskJet 1200C and 1200C/PS printers
 - HP PaintJet XL300 and XL300 PostScript color printers
 - HP DesignJet 650C and 600 plotters
- XIO Devices
 - HP LaserJet IIID, III, IID, and II printers

- HP JetDirect EX and JetDirect EX Plus3 Connected
 - *HP LaserJet 5P, 5MP, 4P, 4MP, 4L and 4ML printers
 - HP LaserJet IIIP, IIP plus and IIP printers
 - HP DeskJet 510, 520, 55C and 560C printers
 - HP DesignJet 200/220 plotter
 - HP DraftPro Plus plotter

HP JetAdmin features vary depending on the level of functionality of the HP JetDirect print server or the peripheral devices. HP JetAdmin fully supports the functions of the advanced network printing in OS/2 Warp Server for all printers above preceded by an asterisk (*).

3.7.2 Installing HP JetAdmin

To install HP JetAdmin, you can run INSTALL.CMD from the OS/2 Warp Server CD-ROM 2 root directory. This allows you to install any program on the CD-ROM 2, including the HP JetAdmin Utility. Instead, you may also run the INSTALL.CMD in the \BPIU\HPJET directory. This INSTALL.CMD is specifically for the HP JetAdmin Utility. If you run the INSTALL.CMD from the boot directory of the CD-ROM 2, the screen shown in Figure 194 on page 257 will open. By selecting **JETADMIN** on this screen and clicking on the **Install** button, you will start the installation program, JETINST.EXE. The program will prompt you for three parameters:

- Source drive
- Destination drive
- Installation option. You may install HP JetAdmin as a client (which is the default) or as a print server, in which case you type HP.

To install certain components, the installation program must disable the OS/2 spooler. When this happens, you will see the following prompt: *Jobs printed directly - spooler disabled*. Select **OK** in response to it. At the end of the installation, the spooler should be enabled. If for any reason the spooler is left in a disabled state, you'll have to enable it. To do this, click the right mouse button while on an empty area of the desktop, and select **System setup**. On the System Setup window, click the right mouse button on the Spooler icon and select **Enable spooler**. You can also enable the spooler by typing *SPOOL* on a OS/2 command line.

There won't be any noticeable change on the OS/2 desktop when the installation is complete. JetAdmin provides port drivers that can be associated with an OS/2 Print Object.

Protocol Required

The HP JetAdmin Utility requires the 802.2 protocol to be configured for the adapter card being used. If this is not installed, use the Adapter and Protocol Services icon within the Startup Folder to do so. The HP JetAdmin installation process can complete without 802.2 support, but configuration and usage of the utility require 802.2.

3.7.3 Configuring JetAdmin

You can associate an OS/2 printer object with a JetAdmin port by doing the following:

1. Create a printer object, or use an existing one (see 3.1.1, "Creating a Printer Object on OS/2 Warp" on page 232).
2. Once the printer object is created, open its Settings notebook and select the **Output Port** page.
3. Select **Install New Port**.
4. On the Install New Port window, select **HP Network Port - Network Peripheral Interface**; then click on **Install**.
5. You will be prompted for the Port Name. Enter it, and select **OK**.

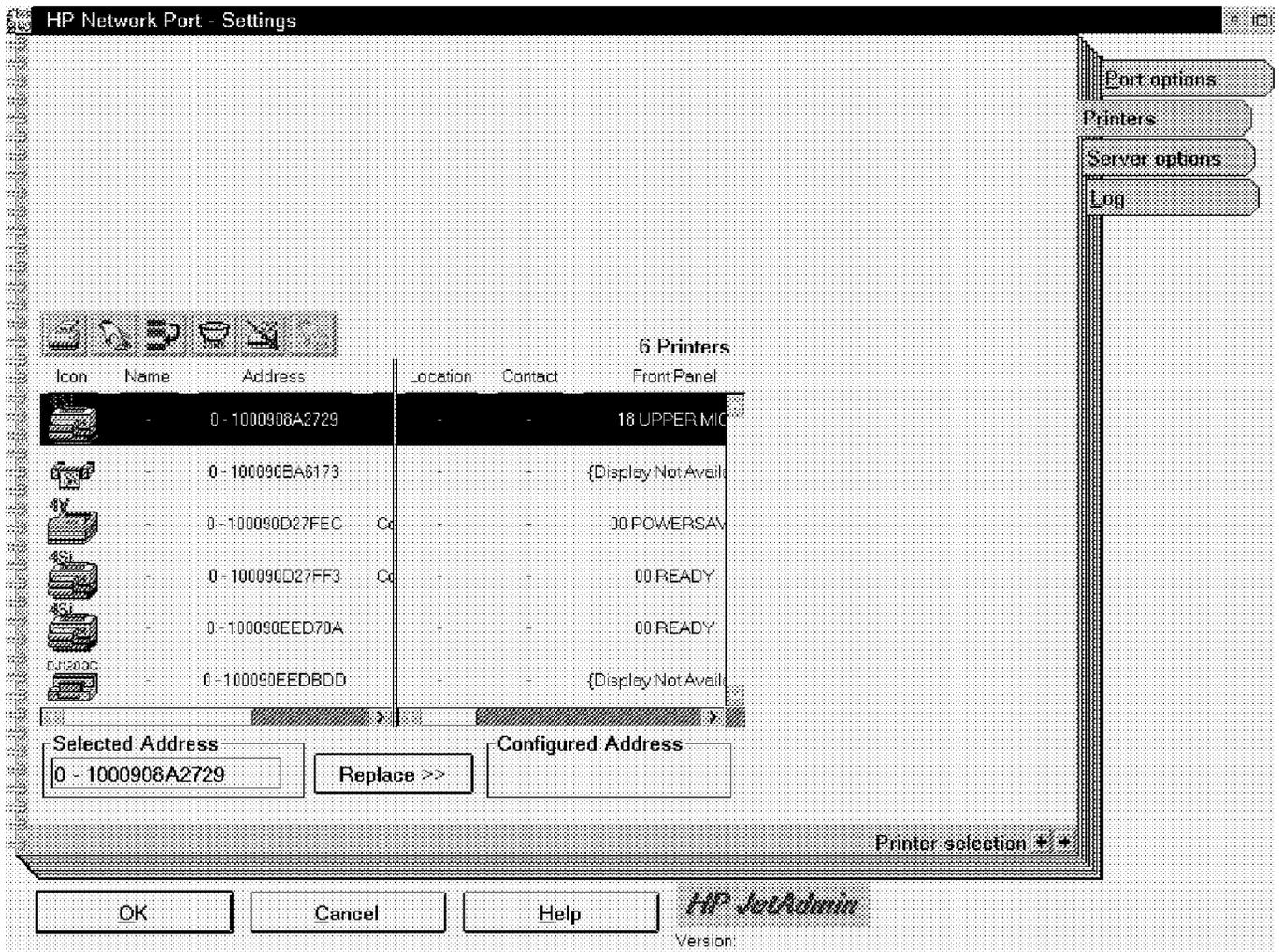


Figure 208. HP JetAdmin Settings Notebook

6. JetAdmin will interrogate the network looking for printers it can recognize. When it's done, you'll see the Settings notebook shown in Figure 208. On the Printers page, you see a list of all printers identified by JetAdmin. On the left side, the list shows for each printer: the Icon for that type of printer, the printer Name if there is one assigned to the printer, the LAN Address and whether it is connected to a controlling port driver. On the right side,

you see information such as the printer model, the state of its front panel, and inventory information (not visible in the figure).

7. When you select a printer from the list, its address will appear on the Selected Address field at the left bottom of the page. Select the printer you want to control; then click on the **Replace>>** button. The address will appear on the Configured Address field on the right. After selecting the printer, click on the **OK** button. The port will be installed.
8. On the Printer Port page of the printer object notebook, select the port you've just installed. Now this port will be used by this printer object. Close the notebook, and you're ready to send files to this printer.

3.7.4 Managing Printers with JetAdmin

To open the pop-up menu for a printer object that is using an HP network printer port, click on it with the right mouse button, and select **Printer Panel**. You will see the **HP Printer** option. Select it, and the HP remote control panel notebook shown in Figure 209 will open.

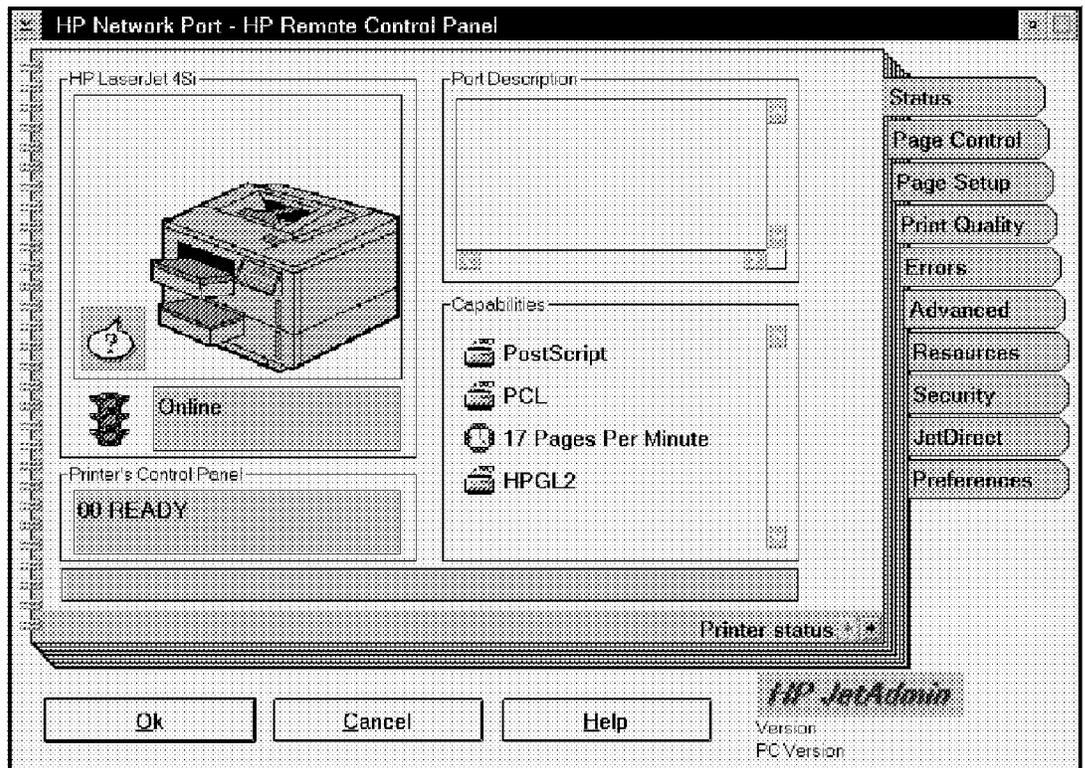


Figure 209. HP Remote Control Panel Notebook - Status Page

The number and contents of the pages in this notebook will vary depending on the information provided by that printer model. In this example, the HP LaserJet 4Si printer has many settings within the notebook pages that you can view and modify, such as: paper sizes, print resolution, security, and so on.

3.8 Related Publications

This section provides the reader with a list of selected publications for further reading on the topics discussed in this chapter.

- *Printing in OS/2*, online in the Information folder of OS/2 Warp Server
- *IBM Print Services Facility for OS/2: Online Reference*, in the PSF/2 folder of OS/2 Warp Server
- *IBM Print Services Facility for OS/2: What's New*, online in the PSF/2 folder of OS/2 Warp Server
- *IBM Print Services Facility for OS/2: A Guide To Using PSF/2*, G544-5225
- *IBM Print Services Facility for OS/2: Printer Attachments Guide*, G544-5215
- *OS/2 Warp Administrator's Survival Guide*, SR23-7222

Chapter 4. Backup and Recovery Services

Local area networks (LANs) have evolved to the extent that they invariably provide the information backbone of both large and small businesses. Key business applications are now running in LAN-based client/server environments for the following reasons:

- Flexibility to respond to fast changing business needs
- Sharing of resources
- Cost reduction

OS/2 Warp Server provides you the ideal base from which to build new, or enhance existing, LAN-based client/server environments and provides built-in functions to address the resulting business requirement of system availability and accessibility in the form of OS/2 Warp Server Backup/Restore.

When you are designing a backup and recovery plan, you must consider the following factors:

- How long can your business operate without access to OS/2 Warp Server services?
- What is the probability of losing data through operational error?
- How much effort and expense can be justified to minimize downtime?

We look at how to define a recovery strategy in 4.6, "Defining your Backup/Recovery Strategy" on page 291.

4.1 OS/2 Warp Server Fault Tolerance Features

Even without the benefit of OS/2 Warp Server Backup/Restore, OS/2 Warp Server features the following inherent OS/2 LAN Server recovery related services and features:

- DCDB Replicator Service

The Domain Control Database Replicator (DCDBREPL) service enables a backup domain controller to maintain a copy of the primary domain controller's Domain Control Database (which contains application definitions, logon assignment, and so on). This allows the backup domain controller to process logons and provide logon assignments should the primary fail. This is a highly optimized subset of the Replicator service, which is operated completely independently; so they may run concurrently.

- Replicator Service

The Replicator service allows you to maintain backup copies of key files by exporting them to other servers or OS/2 requesters.

- Fault Tolerance for Fixed Disks

The disk fault tolerance features provided with File and Print Sharing Services include disk mirroring, disk duplexing and hotfix support.

In addition, the built-in systems management features, such as Predictive Failure Analysis, provided with Systems Management Services, are designed to provide

maximum system availability by alerting you of possible failures before they actually occur.

4.2 Overview

OS/2 Warp Server Backup/Restore provides features which enable you to safeguard your system against possible loss of information by taking backups of your OS/2 files and folders. It has the facilities to take backups of files automatically or manually and can restore these files selectively. Once you designate how backups are stored, OS/2 Warp Server Backup/Restore manages their backup and retrieval for you. The background execution of OS/2 Warp Server Backup/Restore means normal work can continue with minimal interruption.

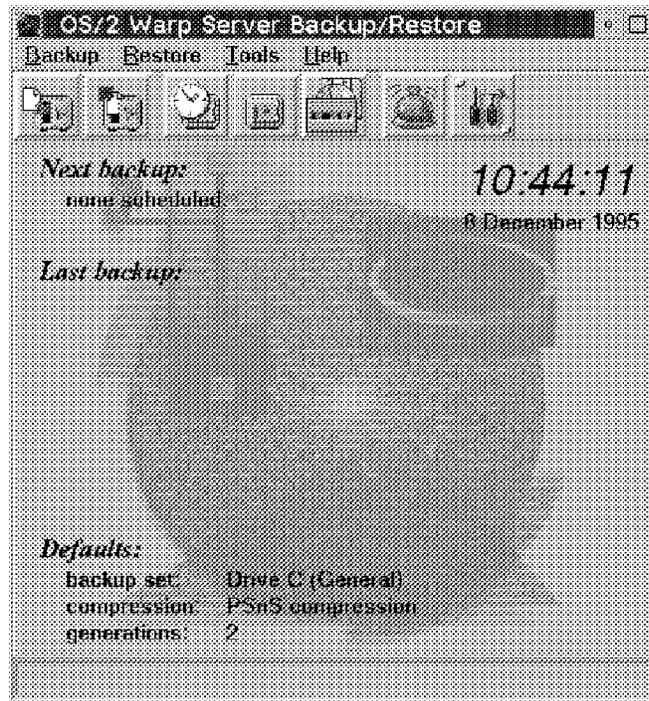


Figure 210. OS/2 Warp Server Backup/Restore Main Panel

OS/2 Warp Server Backup/Restore remembers where it has backed up data by using special index files. These files are automatically backed up by OS/2 Warp Server Backup/Restore whenever it does a backup, ensuring your data will always be recoverable, even after a catastrophic disk crash.

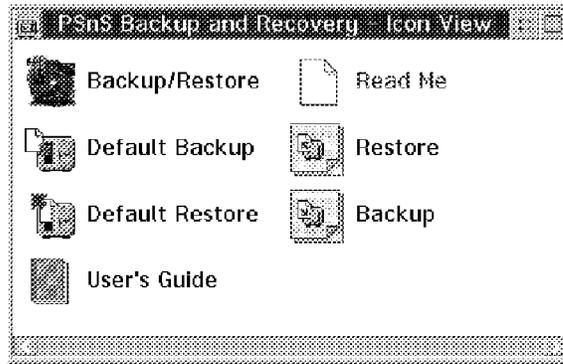


Figure 211. OS/2 Warp Server Backup/Restore

OS/2 Warp Server Backup/Restore has the following features:

- Supports backup and recovery of files and Access Control Lists (ACLs).
- Backup media supported: diskette, tape, optical, hard disk, and LAN drives (via aliases only, *not* UNC names).
- When used in conjunction with IBM's ADSTAR Distributed Storage Manager (ADSM), backups can be sent to a separate server using one of the many communication protocols available (NetBIOS, TCP/IP, APPC, IPX/SPX, and Named Pipes).
- Supports IBM SCSI tape drives and a wide range of popular industry SCSI tape drives (see Table 22 on page 282 for a complete list of supported devices).
- Backups can be scheduled to occur automatically with a highly flexible scheduling subsystem.
- Manual backups can be taken at any time.
- Supports compression of backed up data.
- Manages backup volumes without the need to create an administration system for backups.
- Disaster Recovery Utility enables you to build a set of bootable diskettes from which you can fully recover an OS/2 Warp Server server and all its files and ACLs from any removable media.
- Multimedia enabled - sounds, in the form of .WAV files, can be associated with any system event, providing you with the flexibility to audibly describe the events. Sample .WAV files are included.
- Object oriented, drag-and-drop technology seamlessly integrates with the OS/2 Warp Server desktop.

4.2.1 Positioning

The OS/2 Warp Server Backup/Restore component of OS/2 Warp Server is derived from a product called Personally Safe 'n' Sound (PSnS). PSnS has been greatly modified, updated, and improved to the extent that it may be viewed as a powerful, easy-to-use ADSTAR Distributed Storage Manager (ADSM) entry product.

If your requirements are limited to backing up individual OS/2 Warp Server server workstations, then OS/2 Warp Server Backup/Restore is the

recommended solution. However, if you need to centrally administer multiple server workstations and/or want to perform server initiated backups of data located on clients, it is recommended that you upgrade to ADSM.

ADSTAR Distributed Storage Manager is a complete client/server storage management system that uses a central server to store data. The ADSM Server supports multiple hardware platforms. The central server can run on the same machine as OS/2 Warp Server Backup/Restore or on an entirely different machine, such as an IBM System/390, IBM AS/400, or IBM RS/6000. In addition, ADSM provides automatic backup and archive services to multivendor workstations, personal computers, and file servers.

To upgrade to ADSM, you need to first purchase the relevant licenses, specify in the OS/2 Warp Server Backup/Restore Restore destination field that data will now go to ADSM rather than diskette, tape drive, and so on. A notebook will appear which allows you to configure your communications protocol between the server workstation and ADSM (essentially creating DSM.OPT).

However, using OS/2 Warp Server this way eliminates it from being a true ADSM client, which would allow it to be controlled with an ADSM schedule and policy. You can however, install the ADSM code on the OS/2 Warp Server and make it appear as an ADSM client.

4.3 OS/2 Warp Server Backup/Restore Device Support

If you are installing or reconfiguring OS/2 Warp Server Backup/Restore, clicking on the **More** button allows you to select the associated options. The panel you will see is shown below, in Figure 212.

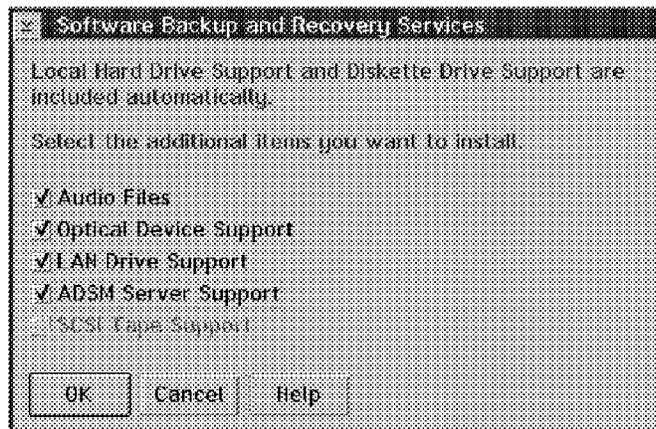


Figure 212. OS/2 Warp Server Backup/Restore Device Support

OS/2 Warp Server Backup/Restore supports backup to the following storage devices:

- Hard Disks

You may backup files to any locally attached hard disk that is formatted for any of the following file systems:

- FAT
- HPFS

- 386HPFS

Restoring from hard disk drives provides one of the fastest methods of accessing backed up data.

- Diskette Drive

You may back up to any locally attached diskette drive that is supported by OS/2. Diskettes must be formatted for the FAT file system.

Backing up to diskette is suited to small amounts of data.

- LAN Alias Drive

You can use an alias defined under OS/2 Warp Server or any version of LAN Server as the target for a backup. OS/2 Warp Server Backup/Restore can use the alias name to refer to this storage device and does not need a drive letter (although one may already be assigned with the `NET USE` command).

Restoring from an alias provides fast access to backed up data, assuming the network is not congested.

- Remote Drives

Remote drives that you have connected to (which are shared at the server workstation as an alias), and assigned a drive letter to, are supported. They must be compatible with the FAT 8.3 file system.

Restoring from a remote drive also provides fast access to backed-up data.

- Optical Drives

Read/write optical drives that are supported by OS/2 can be used as targets for backups providing the optical disk has been formatted for either FAT, HPFS, or 386HPFS, and has a large storage capacity.

- ADSTAR Distributed Storage Manager (ADSM)

You may back up to an ADSM server which provides centralized storage management.

- Tape Drives

Attention

Please be aware that:

1. The OS/2 Warp Server Backup/Restore online documentation states the tape device driver only supports SCSI II hardware, but SCSI-I tape devices can be defined and used successfully.
2. OS/2 Warp Server Backup/Restore and ADSM/2 support an identical set of tape drives. This is because OS/2 Warp Server Backup/Restore uses the ADSM/2 tape device drivers. There is, however, an exception in that ADSM/2 supports some tape auto-changers, while OS/2 Warp Server Backup/Restore supports only manual-change tape drives. If you require automated backup of vast quantities of data, then it is advisable to use ADSTAR Distributed Storage Manager in place of OS/2 Warp Server Backup/Restore.

Tape drives typically have the capacity to store large amounts of data and the media is relatively inexpensive compared to read/write optical disks.

The following locally attached tape drives are supported:

<i>Table 22. 8mm Tape Drives Supported by OS/2 Warp Server Backup/Restore</i>		
Device Name	Supported Formats	Estimated Capacity
ANDATACO ENCORE 8205	8200, 8200C	2.3 GB
ANDATACO ENCORE 8505	8200, 8200C, 8500, 8500C	5.0 GB
CYBERNETICS CY8205	8200, 8200C	2.3 GB
CYBERNETICS CY8500	8200, 8500	5.0 GB
CYBERNETICS CY8505	8200, 8200C, 8500, 8500C	5.0 GB
DYNATEK HSB 2300	8200, 8200C	2.3 GB
DYNATEK HSB 10.0	8200, 8200C, 8500, 8500C	5.0 GB
DYNATEK HSB 5000	8200, 8200C, 8500, 8500C	5.0 GB
EXABYTE 8200	8200	2.3 GB
EXABYTE 8205	8200, 8200C	2.3 GB
EXABYTE 8205XL	8200, 8200C	3.5 GB w/XL tape
EXABYTE 8500	8200, 8500	5.0 GB
EXABYTE 8500C	8200, 8200C, 8500, 8500C	5.0 GB
EXABYTE 8505	8200, 8200C, 8500, 8500C	5.0 GB
EXABYTE 8505XL	8200, 8200C, 8500, 8500C	7.0 GB w/ XL tape
IBM 3532-023	8200	2.3 GB
IBM 3445-001	8200, 8200C, 8500, 8500C	5.0 GB
SUN 8505XL	8200, 8200C, 8500, 8500C	7.0 GB w/ XL tape
TTI CTS-8000H	8500, 8500C	5.0 GB
TTI CTS-8519H	8200, 8200C, 8500, 8500C	5.0 GB
Notes:		
1. Greater capacity might be achieved with compression		
2. OS/2 Warp Server Backup/Restore only supports mirrored mode operations		
3. Also supported by ADSM/2		

<i>Table 23 (Page 1 of 2). 4mm Tape Drives Supported by OS/2 Warp Server Backup/Restore</i>		
Device Name	Supported Formats	Estimated Capacity
HP 35470A	DDS1	2.0 GB
HP 35480A	DDS1, DDS1C	2.0 GB
HP C1553A	DDS1, DDS1C, DDS2, DDS2C	4.0 GB
HP Jetstore 2000e	DDS1	2.0 GB
HP Jetstore 5000e	DDS1, DDS1C	2.0 GB
IBM 3440-001	DDS1, DDS1C	2.0 GB
IBM (74G8632/8191339)	DDS1, DDS1C, DDS2, DDS2C	4.0 GB
IBM (74G8631/8191359)	DDS1, DDS1C, DDS2, DDS2C	4.0 GB
IBM 4326NP/RP	DDS1, DDS1C, DDS2, DDS2C	4.0 GB
WANGDAT 3300DX	DDS1, DDS2	4.0 GB
WANGDAT 3400DX	DDS1, DDS1C, DDS2, DDS2C	4.0 GB

<i>Table 23 (Page 2 of 2). 4mm Tape Drives Supported by OS/2 Warp Server Backup/Restore</i>		
Device Name	Supported Formats	Estimated Capacity
SONY SDT5000	DDS1, DDS1C, DDS2, DDS2C	4.0 GB
Notes:		
1. Greater capacity might be achieved with compression		

<i>Table 24. QIC Tape Drives Supported by OS/2 Warp Server Backup/Restore</i>		
Device Name	Supported Formats	Estimated Capacity
IBM 3450-001	QIC120 QIC150 QIC525 QIC1000	1.19 GB
TECMAR QT525ES	QIC525	525 MB
WANGTEK 5525ES	QIC525	525 MB

<i>Table 25. DLT Tape Drives Supported by OS/2 Warp Server Backup/Restore</i>		
Device Name	Supported Formats	Estimated Capacity
Quantum DLT 2000	DLT10 DLT10C	10 GB
Quantum DLT 4000	DLT10 DLT10C DLT20 DLT20C	20 GB
Notes:		
1. Greater capacity might be achieved with compression		

If you want to add support for a new storage device after installation, you may do so from the **Control Panel**:

1. From the OS/2 Warp Server Backup/Restore main windows, select **Tools**.
2. Select **Storage Devices**.
3. In the Storage Devices container, press mouse button 2, and select **New** followed by the type of storage device you wish to add from the menu.
4. Fill in the appropriate values, and select **OK**.

Newer Version

Since the release of OS/2 Warp Server Backup/Restore, IBM has made changes and enhancements to this program. An update to OS/2 Warp Server Backup/Restore is included in OS/2 Warp Server SMP, but this update can also be installed over OS/2 Warp Server. IBM employees can download the update from the Web site listed below:

<http://www.wdg.uk.ibm.com/psns>

For a brief description of these changes and enhancements, please refer to 6.8, "Backup and Recovery Services" on page 310.

4.3.1 OS/2 Warp Server Backup/Restore Features

Once you have installed OS/2 Warp Server Backup/Restore and selected the type of storage device(s) you wish to use, you are in a position to perform your first backup of your system files and folders.

You must decide which drives, folders or directories, and files to back up. This set of data is backed up to a *Backup Set*. A Backup Set is a logical collection of backed up files which resides on a *storage device*. With backup sets, you can specify a file that you want restored, and OS/2 Warp Server Backup/Restore takes care of determining where that file was backed up and how to restore it. This simplifies the restore process for the administrator.

Now that you know what a Backup Set is, you can define a *Backup Method*. A Backup Method is the manner in which files are backed up to the Backup Set. For example, the Backup Method specifies the source files to be backed up, use of compression, number of generations, incremental or full backup, and the Backup Set utilized.

The steps you need to take to complete a backup are best described by following the flow of the Pipeline shown in Figure 213.

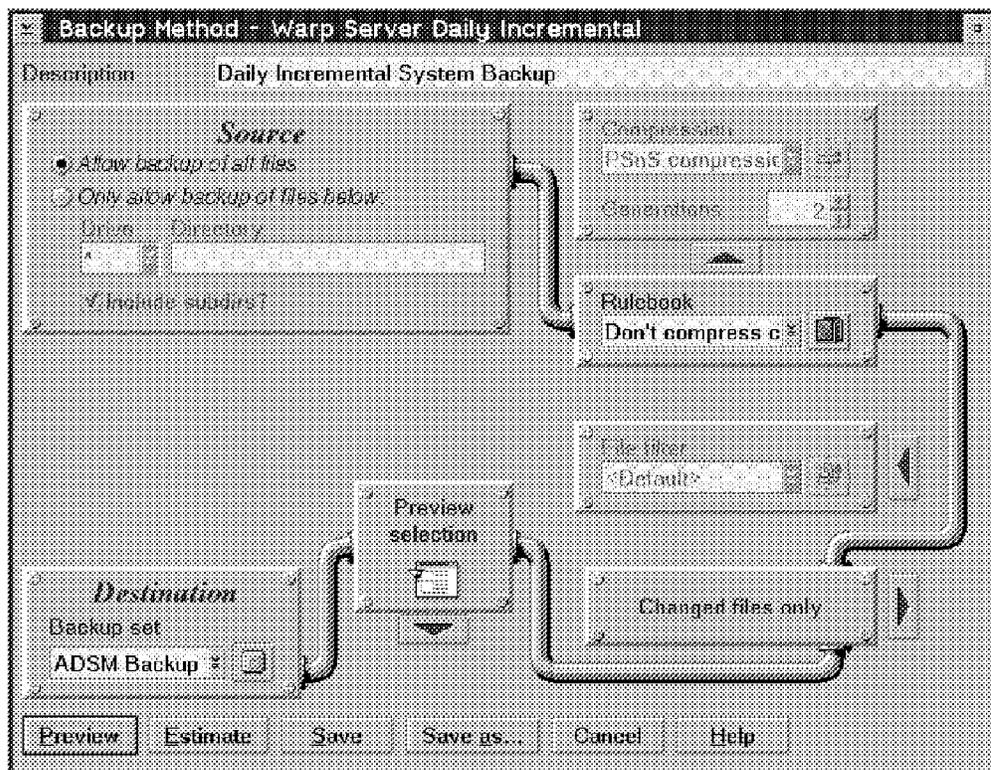


Figure 213. OS/2 Warp Server Backup/Restore Pipeline

The window shown in Figure 213 is displayed by selecting the **Backup** menu bar item from the OS/2 Warp Server Backup/Restore graphical user interface; then select **Edit new method....** It enables you to define a backup method which may then be saved and used again in the future.

If we follow the flow of the Pipeline from the top left of the window down to the bottom left, we see the available options that OS/2 Warp Server Backup/Restore provides to enable you to create a highly flexible backup/restore solution.

4.3.1.1 Source

A set of objects, the *Source*, starts at the top of the Pipeline and flows through it. As each object progresses along the Pipeline, it may be filtered out by certain choices or have attributes set which define how it is backed up.

The Pipe Source is the set of files and folders which are to be considered for backup. There are two ways of defining the Source:

Allow backup of all files:

This option will include all objects to be found on all the source drives which are currently checked for backup

Only allow backup of files below:

This allows you to specify a particular drive or subdirectory for backup

Drive

The letter of the source drive to back up. Select * (asterisk, sometimes called *wild card*) for all source drives checked for backup

Directory

The name of the directory to back up

Include subdirs?

Select this option to include all objects in subdirectories of the directory specified above

You may also drag folders from the Workplace Shell onto the source to choose which files and folders are going to be considered for backup. The folder must be on one of the source drives checked for backup.

4.3.1.2 Compression

Compression allows OS/2 Warp Server Backup/Restore to use a software-based algorithm to store files in the backup set in a compressed format. This allows the storage media to hold a greater amount of data than it normally supports. For example, it may be possible to store 3.0 GB of data on a tape that has a 2.0 GB capacity. The actual amount stored depends on the nature of the data and can vary greatly. The compression options are:

No compression

Files are stored without any compression mechanism.

PSnS Compression

Files are stored using native compression provided by OS/2 Warp Server Backup/Restore. The compression algorithm is a specially developed version of the Arithmetic Coding algorithm.

<Default>

Files are compressed according to the defaults for all backups, which can be configured from *Tool* icon on the OS/2 Warp Server Backup/Restore Main Panel (see Figure 210 on page 278).

The number of generations to keep can also be specified. A *Generation* is a specific instance of a file that has been backed up. The default is two

generations. This means that two backed-up versions of the file are maintained during successive backups. For example, if you discover a corrupted file on your system, you can restore the version that was most recently backed up. However, if this restored file is also corrupted, you can restore the next previous backed-up version. Generations give you a powerful feature, allowing you to maintain multiple versions of a given file. Of course, OS/2 Warp Server Backup/Restore allows you to specify which generation you want during the restore process.

4.3.1.3 Rulebook

The first option in the Pipeline specifies *how* files and folders are backed up. You can either specify a Compression Method and number of generations for all the files and folders which are backed up, or you can select a **Rulebook** which allows you to specify the Compression Method and Generations individually for each file and folder. Use the arrow button to make the Pipeline flow through the option you want, then select the specific items.

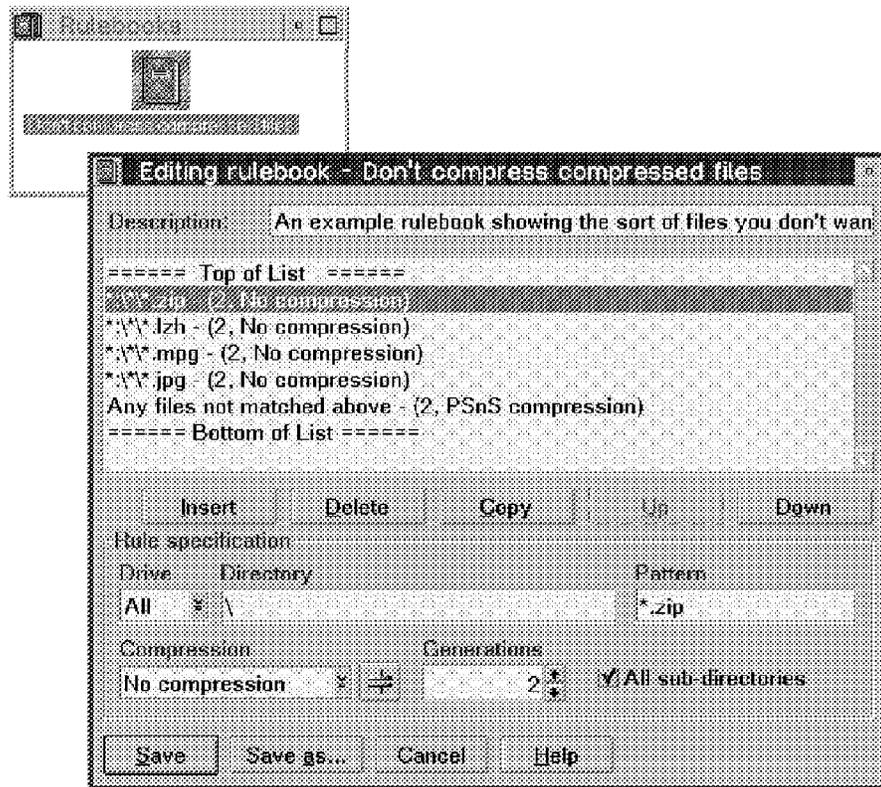


Figure 214. OS/2 Warp Server Backup/Restore Rulebook

Note: It is possible to select the Default option in both the Compression Method and Rulebook fields.

4.3.1.4 File Filter

The second option in the Pipeline allows you to include a *File Filter* to filter out specific source files which you don't want to back up. Use the appropriate arrow button to select whether the Pipeline will flow through a File Filter, and then select either a specific File Filter or Default for the default File Filter.

You also have the option of defining a *tree* file filter. Whereas the File Filter allows you to specify file names and types, the tree file filter allows you to view

drives, folders and individual files. You can select or deselect these objects for backup at the folder level or even at the drive level. This flexibility ensures that you can quickly select the correct set of files to be processed.

4.3.1.5 Changed Files Only

If this option is selected, then the Backup Method will perform incremental backups. OS/2 Warp Server Backup/Restore compares each file and folder to the existing one on the same backup set. If the file has changed, the file is backed up. This method allows the backup set to have the latest backup data and also saves time by ignoring files that have not changed.

The first time that an incremental backup is run, it is actually a full backup, since no backup set exists to compare to.

If the Changed Files Only option is not selected, all files and folders specified are backed up. Use the appropriate arrow button to either include or exclude this option in the pipe.

4.3.1.6 Preview Selection

Before you run a backup, you can preview the objects which will be backed up. This allows you to verify the right files and folders are backed up and to deselect any you do not want to include.

To get a preview, select **Preview Selection** on the Edit Backup Method panel, and press the **Preview** button. A tree will appear with a list of files and folders included in the backup. You can select and deselect files in the usual way.

To view statistics relating to the backup, click on the **Estimate** button.

Note: The first estimate is provided by the device interface. For example, the hard disk storage device has a default data rate which is used for initial estimating.

Select **Backup** to start the backup with the current selection or **Cancel** to end the backup operation.

Note: You can change which fields are displayed in the container of file objects by selecting and deselecting options from its container context menu.

4.3.1.7 Destination

This tells OS/2 Warp Server Backup/Restore *where* data is backed up by this backup method. You can select a specific Backup Set, use the Default or create a new Backup Set. If you create a new Backup Set, the related storage device must already be defined. Figure 215 on page 288 and Figure 216 on page 288 show examples of defining a new storage device to enable an OS/2 Warp Server workstation to back up to an ADSM/2 server.

At the end of the Pipeline, only the files which have not been filtered out will remain to be backed up to a Backup Set.

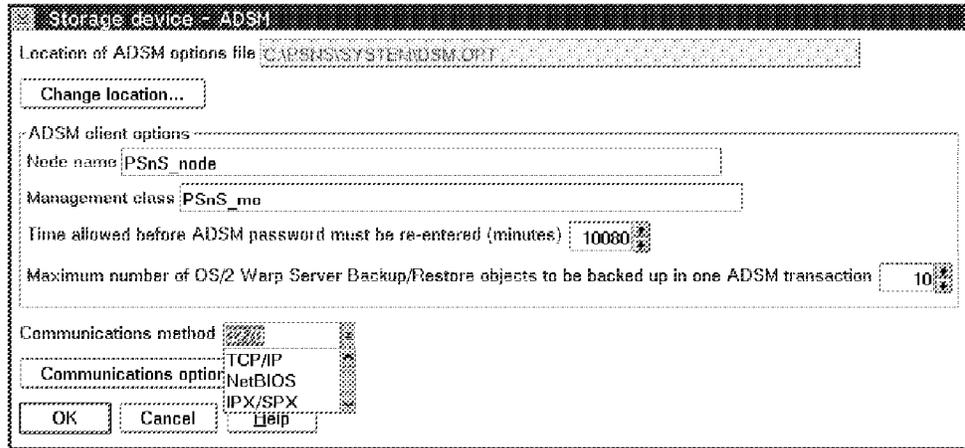


Figure 215. Defining a Storage Device (ADSM)

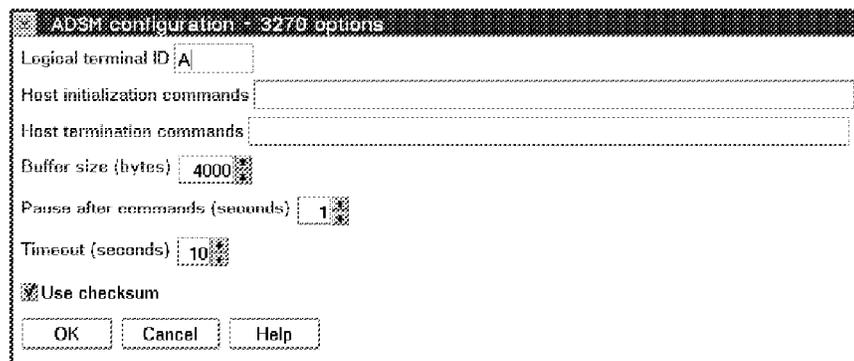


Figure 216. Defining the Communications Options for an ADSM Backup Set

4.4 OS/2 Warp Server Backup/Restore Scenarios

In this section, we look at a few scenarios which you are likely to encounter and some suggested solutions to address each environment's software backup and recovery requirements.

Notes:

1. Each installation has different requirements. The following scenarios simply illustrate how you may use OS/2 Warp Server Backup/Restore in typical OS/2 Warp Server environments.
2. You may also refer to a typical backup scenario illustrated in the online documentation (PSNS.INF file).

4.4.1 Single Server Scenario

In an environment where you only have a single OS/2 Warp Server workstation, you probably have the most straightforward scenario since you do not have to consider backing up additional servers. This scenario usually has a local storage device on the server, such as a tape drive. OS/2 Warp Server Backup/Restore is an excellent option in this scenario.

4.4.2 Multiple Server Scenario

In a multiple server scenario, you must consider how you will manage the security of data which is spread across a number of server workstations.

To add further complexity to the scenario, while server workstations may be members of the same OS/2 Warp Server domain, they may be installed at different locations and connected using a variety of protocols.

One option is to provide a storage device on each server and use OS/2 Warp Server Backup/Restore as in the single server scenario. This is certainly feasible.

OS/2 Warp Server Backup/Restore by itself can also be used to efficiently back up multiple servers and small groups of machines connected via a LAN. You can define drive letters to aliases representing the drive resources on the other servers, and have OS/2 Warp Server Backup/Restore back up the information using the drive letters. This method works for a small number of servers. However, you may find the network will eventually grow beyond your ability to easily manage the backup of all the data from a single server. Remember, the most successful backup strategy is one which requires little or no human intervention and stores data in the most secure place possible. A network of computers poses unique, and sometimes frustrating, problems for keeping its data safe and secure.

IBM's ADSTAR Distributed Storage Manager (ADSM) should be considered as an integral part of your backup strategy. It makes backing up a network easy and efficient through its centrally managed client/server design. ADSM can also be of great help if you have systems that run operating systems other than OS/2. ADSM features a unique *open* system design that allows you to easily manage the storage requirements of many different operating environments (Apple MacIntosh, Microsoft Windows, DEC VMS, AIX/6000, DEC ULTRIX, DOS, HP-UX, MVS TSO, VM CMS, OS/2, SCO, and SunOS) using a wide range of communications protocols (NetBIOS, TCP/IP, IPX/SPX, Named Pipes, and APPC (SNA LU6.2)).

4.4.3 Enterprise Scenario

In addition to the complexity introduced in the multiple server scenario, an enterprise scenario may provide additional factors to be considered.

For instance, most enterprises have backup and recovery procedures in place to protect mid-range and mainframe data. Often, the host environment is managed by one group, and the LAN is managed by another group. Because of this split, separate backup management schemes arise. For example, the host may be backed up via ADSM, and the LAN is backed up by local storage devices on the servers, using OS/2 Warp Server Backup/Restore. It may make better sense to integrate your OS/2 Warp Server backup and recovery procedures with these existing host procedures by utilizing ADSM on an existing host system.

4.5 Disaster Recovery Utility

Normally, if a server suffers a failure such that it cannot be restarted, you are faced with the task of first reinstalling the operating system and installing the backup utility before you can restore.

However, in the event of a catastrophic failure, OS/2 Warp Server Backup/Restore can completely restore an OS/2 Warp Server server workstation from *locally attached* devices, such as tape drive, hard disk or diskette, without the need for you to reinstall OS/2 Warp. The ADSM client program allows a disaster recovery restore from an ADSM Server, but this function is not supported when using the OS/2 Warp Server Backup/Restore as the client program to an ADSM Server.

This is achieved by using the OS/2 Warp Server Backup/Restore Disaster Recovery Utility, which creates a set of diskettes from which you can boot your server workstation after a disaster independent of the operating system configuration that is on the server workstation. After booting the server from these diskettes, you can restore an entire Backup Set to recover your system. The Disaster Recovery Panel is shown in Figure 217 on page 291.

4.5.1 Preparing the Disaster Recovery Utility

To prepare your workstation for recovery from a disaster, you can follow the procedure below. First, go to the OS/2 Warp Server Backup/Restore Main Panel and select **Tools, Guides**, and then **Disaster Recovery Guide**. From the resulting panel, you can configure the appropriate parameters to enable the proper drivers to be loaded on the boot diskettes. See Figure 217 on page 291.

1. Create three bootable diskettes.

These diskettes contain OS/2 Warp system files, 386HPFS drivers (if 386HPFS support is selected) and OS/2 Warp Server Backup/Restore program files.

Note: The Disaster Recovery Utility is designed to work with 1.44 MB diskettes. If you choose to use 2.88 MB diskettes, you must:

- Insert the first diskette whenever you are asked for diskette 1 or 2.
 - Insert the second diskette whenever you are asked for diskette 3.
2. Ensure that the workstation has been backed up to a supported storage device.

Supported storage devices for disaster recovery purposes are:

- Diskette
- Locally attached hard disk drive
- Locally attached read/write optical drive
- Locally attached tape drive

Once the three boot diskettes have been created, you are prepared for a disaster recovery of your system. You will be able to restore the data in the backup set that you specified. The following options are presented:

1. Run FDISK
2. Format a disk drive
3. Proceed with disaster recovery
4. Run CHKDSK on a disk drive
5. OS/2 command line

6. Exit

After selecting option 3, the disaster recovery process stores temporary files on the fixed disk you specify. This enables the restore process to begin, and the files from your Backup Set are copied to their original locations.

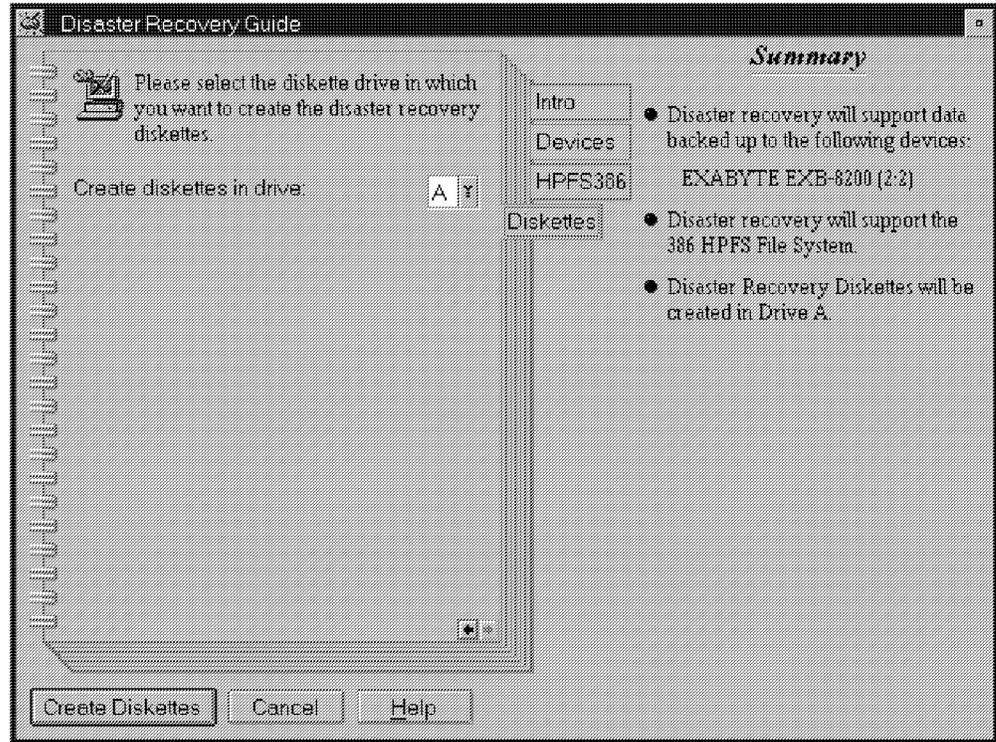


Figure 217. OS/2 Warp Server Backup/Restore Disaster Recovery Options Panel

4.6 Defining your Backup/Recovery Strategy

When faced with a system failure, it is very easy to approach the situation in a rushed, unstructured fashion since a large number of users may be directly affected, and you will be under extreme pressure to restore services as soon as possible.

Although it may be in difficult circumstances, you must adopt a methodical approach to recover the system. Having a well thought out, tried and tested recovery strategy will ensure you get the system up and running with the minimum amount of downtime.

The actions that you need to perform to define a recovery strategy can be summarized as follows:

1. Analyze the strengths and weaknesses of the environment.
2. Identify requirements based on the business needs.
3. Compare the recovery options available to you with the requirements.
4. Decide on a recovery method or combination of them.
5. Plan the recovery scenario(s).

6. Try out the recovery method(s) in a test environment.
7. If you obtained the required results in a test environment, prepare the production environment and transfer the recovery process.
8. Document the recovery strategy.

Note: It is important that you review your environment and business requirements at regular intervals to ensure that your recovery strategy remains valid.

The following IBM-internal Web site has more information on backup and recovery strategies that may be useful in production:

<http://www.wdg.uk.ibm.com/psns>

4.7 Related Publications

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

- *Using ADSM to Back Up OS/2 LAN Server and OS/2 Warp Server*, SG24-4682
- *ADSM General Information*, GH35-0114
- *ADSM V1 User for OS/2*, SH35-0122
- *ADSM V1 User for DOS*, SH35-0123
- *ADSM V1 User for Microsoft Windows*, SH35-0125
- *ADSM/2 Administrator's Guide*, SH26-4003
- *ADSM/2 Administrator's Reference*, SH26-4004
- *ADSM/2 Installing the Server and Administrative Client*, SH26-4014
- *Getting Started with ADSM/2*, GG24-4321
- *ADSM Advanced Implementation Experiences*, GG24-4221
- *ADSM Storage Management Services: Implementation Examples*, (available only on CD-ROM SK2T-2177-09).

Chapter 5. Comparing Adapter and Protocol Services to AnyNet/2

This chapter describes the differences between the features offered by OS/2 Warp Server Adapter and Protocol Services and the additional functions that are offered by the IBM AnyNet product functions. This chapter also includes a brief introduction to the IBM Multiprotocol Transport Networking architecture around which the IBM AnyNet family products are designed. Finally, a list of publications is included for further reading on this topic.

5.1 Any Application - Any Network

In 1993, IBM introduced the IBM Multiprotocol Transport Networking (MPTN) architecture as part of the IBM Networking Blueprint. The main purposes of MPTN are:

1. To break the binding between the upper-layer application support and the underlying transport service provider
2. To provide for end-to-end communication crossing multiple transport service providers

All this should be implemented in a way that will leave existing applications unchanged wherever possible.

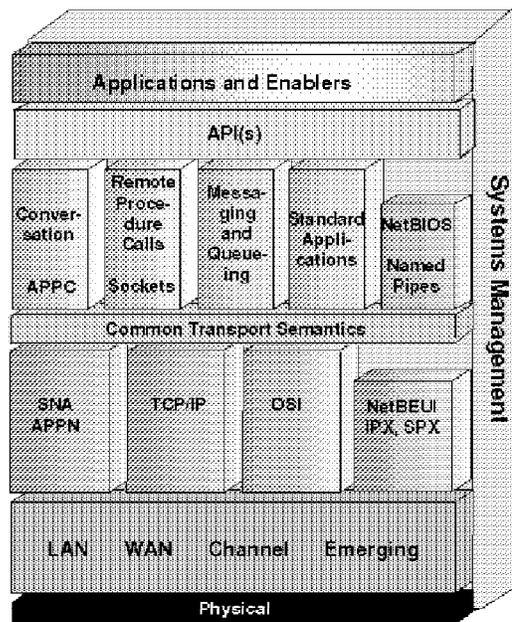


Figure 218. IBM Networking Blueprint

In general terms, this means applications which have been written to a specific API that would normally require a certain underlying transport network (native) can now communicate over a different transport network (non-native) which they would normally not be able to utilize. For example, a Sockets application that would require TCP/IP as its transport service provider can now communicate over an SNA network.

Referring to the Open Systems Interconnection (OSI) layer model, MPTN would be situated between layers 4 and 5. This intermediate layer is referred to as the Common Transport Semantics (CTS) in the IBM Networking Blueprint which is shown in Figure 218.

MPTN is just one implementation of CTS functions. Other functions may be provided or defined by vendors or standard bodies, such as NetBIOS over TCP/IP, as defined in RFCs 1001 and 1002.

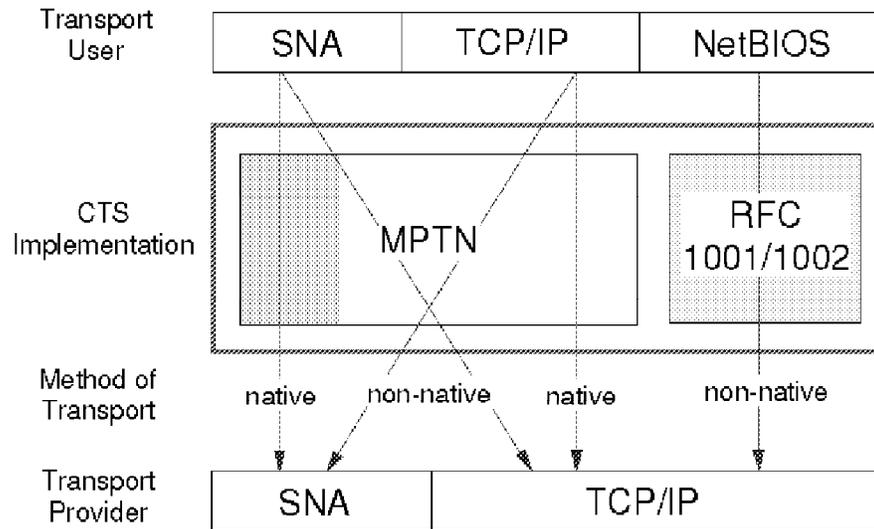


Figure 219. Common Transport Semantics (CTS) Layer

Two MPTN functions must be implemented in order to successfully separate an application from its native transport network:

Function compensation If the non-native transport cannot provide certain functions of the native transport, the MPTN component must compensate for this in order to satisfy application requests. This can be achieved by combining specific functions of the non-native transport to match missing functions.

Address mapping As address schemes and address spaces vary from one transport network to the other, the MPTN component must provide for a unique and reversible translation of network addresses. This can be done in three ways:

1. Algorithmic mapping
2. Using a protocol-specific directory for mapping
3. Using an MPTN address mapper

There are three types of MPTN nodes that can be distinguished:

Access Node Provides MPTN functions in itself. Typically, it has only non-native network connections, but also supports a combination of native and non-native transport providers. The decision about which transport to use for an application can be made either dynamically via routing algorithms or statically via routing preference tables or configuration lists.

Gateway Node

Provides MPTN functions for a set of native nodes to communicate over a non-native backbone. MPTN access nodes or more MPTN gateways can be on the other end. An MPTN gateway must have both native and non-native network connections and thus, support applications that require either kind of transport services. MPTN gateways can also be parallel, meaning the same system can act, at the same time, as a gateway between transport user A and transport provider B, and vice versa.

Address Mapper Node

Provides mapping of native to non-native network addresses if algorithmic address mapping is not possible (native address space is larger than non-native), and a protocol specific (non-native) directory does not exist.

Figure 220 shows a functional diagram of AnyNet access and gateway nodes in conjunction with a native node.

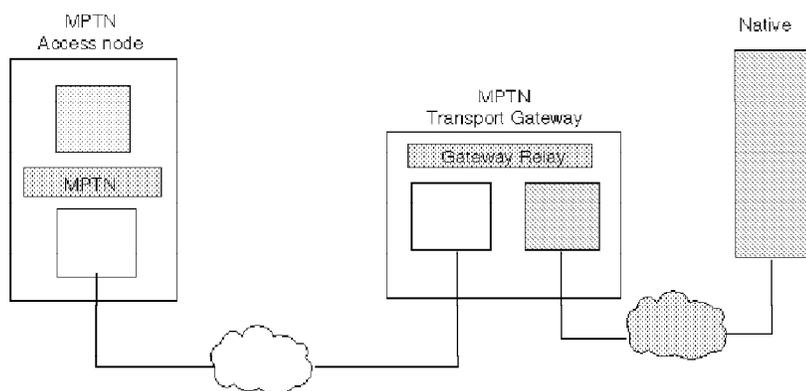


Figure 220. AnyNet Access and Gateway Nodes

MPTN can convert between transport protocols, but it cannot convert between application protocols; so at either end of an MPTN connection, matching applications and APIs must exist.

The following sections list the combinations of application and non-native transport protocols that are implemented in IBM AnyNet products today.

AnyNet Product Changes

The AnyNet/2 Version 1 and Version 2 products were available separately in the past, but IBM has now included the AnyNet/2 functions within the IBM Communications Server for OS/2 Warp, Version 4.0 and Version 4.1. The standalone products are no longer available.

Some of the functions described in this chapter were available in the AnyNet/2 Version 2 product, but are not included in the AnyNet function within IBM Communications Server. This difference will be noted where appropriate. Please refer to IBM Announcement #296-389 for specifics on IBM Communications Server Version 4.1.

5.1.1 SNA over TCP/IP

SNA over TCP/IP is implemented as MPTN access and MPTN gateway nodes, and it uses a protocol-specific directory (DNS) for mapping of SNA LU names to IP Addresses. It enables applications which are written to the APPC, CPI-C, and LUA APIs, as well as SNA LU1, LU2, and LU3-type applications, to communicate over TCP/IP networks instead of SNA networks. SNA over TCP/IP is available as an MPTN access node on OS/2 and MVS. It is available as an MPTN gateway node on OS/2, MVS and the 2217 Nways Multiprotocol Concentrator. APPC over TCP/IP, a subset of the above including only APPC, CPI-C and LUA-type applications, is available as an MPTN access node on AIX, OS/400 and DOS/Windows.

Figure 221 shows a scenario for SNA over TCP/IP.

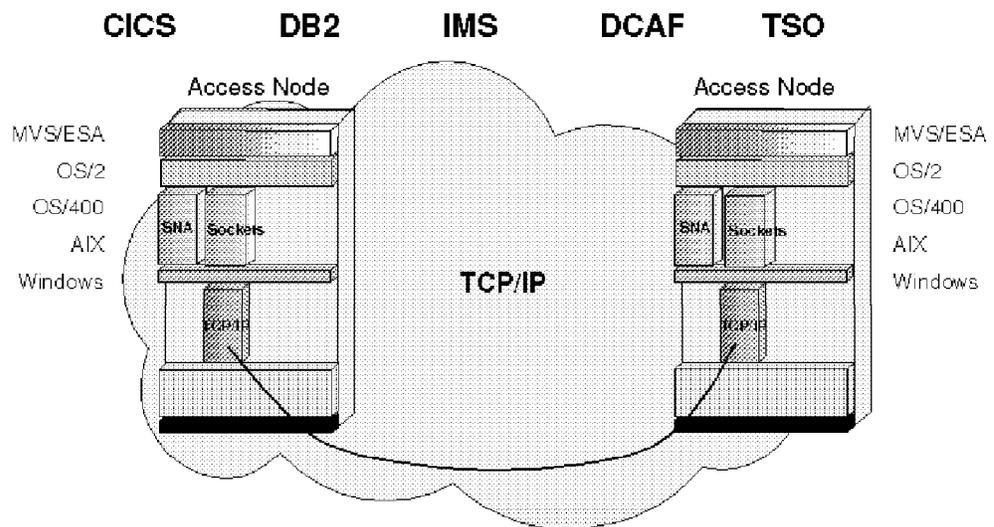


Figure 221. SNA over TCP/IP

5.1.2 Sockets over SNA

Sockets over SNA is implemented as MPTN access and MPTN gateway nodes, and it uses algorithmic mapping of IP Addresses to SNA LU names. It enables applications which are written to the Sockets, RPC and SNMP DPI APIs to communicate over SNA networks instead of TCP/IP networks. Sockets over SNA is available as an MPTN access node on OS/2, AIX, OS/400, and MVS. It is available as an MPTN gateway node on OS/2 and the 2217 Nways Multiprotocol Concentrator.

Figure 222 on page 297 shows a scenario for Sockets over SNA.

5.1.4 Sockets over IPX

AnyNet Function

The function described in this section was available in the AnyNet/2 Version 2 standalone product, but is not included in the AnyNet function of IBM Communications Server, Version 4.1.

Sockets over IPX is implemented as an MPTN access node, and it uses algorithmic mapping of IP Addresses to IPX network addresses. It enables applications which are written to the Sockets, RPC and SNMP DPI APIs to communicate over IPX networks instead of TCP/IP networks. Sockets over IPX is available as an MPTN access node on OS/2.

5.1.5 NetBIOS over SNA (Access Node)

NetBIOS over SNA is implemented as an MPTN access node. It uses an MPTN address mapper for mapping NetBIOS names to SNA LU names. It enables applications which are written to the NetBIOS NB30 and LM10 APIs to communicate over SNA networks instead of NetBIOS networks. NetBIOS over SNA is available as an MPTN access node on OS/2.

Figure 224 shows a scenario for NetBIOS over SNA.

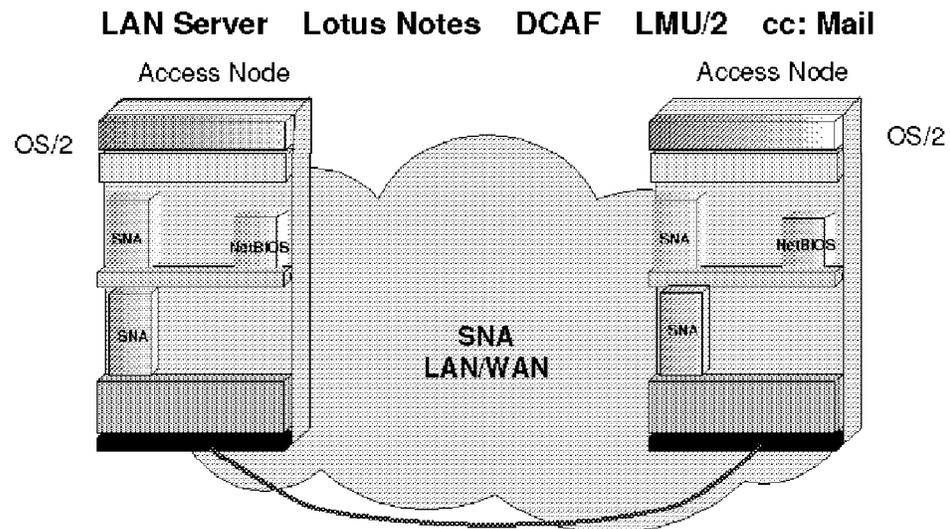


Figure 224. NetBIOS over SNA

5.1.6 NetBIOS over SNA and IPX over SNA (Gateways)

NetBIOS over SNA and IPX over SNA gateways are implemented the same way as the LAN-to-LAN-over-WAN (LTLW) gateways. They use NetBIOS name qualifiers and IPX routing techniques and additional name qualifiers between gateway systems.

Note: The NetBIOS over SNA and IPX over SNA gateways are not MPTN gateway implementations. They use a protocol encapsulation technique in contrast to the MPTN techniques.

They enable applications that are written to the NetBIOS and NetWare APIs to communicate over SNA networks instead of IEEE 802.2 and IPX/SPX networks.

NetBIOS over SNA and IPX over SNA gateways are available on OS/2 and the 2217 Nways Multiprotocol Concentrator.

Figure 225 shows a scenario for IPX over SNA and NetBIOS over SNA gateways.

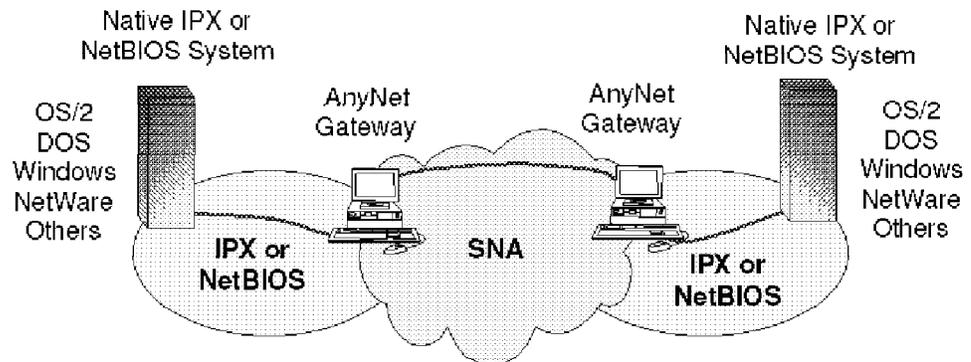


Figure 225. IPX over SNA and NetBIOS over SNA Gateways

5.2 Summarizing Native and Non-native Sockets Services

There has been some confusion in the past as to what the differences are between native and non-native support for applications that use the Sockets API, and what support was provided by which IBM product. This section is dedicated to the purpose of clarifying the differences and discussing the current product implementations of native and non-native Sockets services.

5.2.1 Common Transport Semantics (CTS) Functions of Adapter and Protocol Services

The main purpose of Adapter and Protocol Services in OS/2 Warp Server is to provide software support for LAN, communication adapters and networking protocols for applications (please see page 125, "Adapter and Protocol Services" in the redbook titled *Inside OS/2 Warp Server, Volume 1*, SG24-4602, for a more detailed discussion of those aspects of Adapter and Protocol Services). In addition, Adapter and Protocol Services offers the following CTS functions.

1. Non-native NetBIOS over TCP/IP (RFC 1001/1002)
2. Native Sockets services

5.2.1.1 NetBIOS over TCP/IP

This function allows NetBIOS applications to use TCP/IP as a transport provider. This is especially useful for large networks and WAN communications since NetBIOS lacks any support for routed networks; so it would normally be confined to LAN environments.

The RFCs 1001 and 1002 specify how NetBIOS operation and names are mapped to TCP/IP operation and host names and what modes of operation are possible.

NetBIOS over TCP/IP is currently only available in an access-node type of implementation. A gateway function will be available by IBM, but was not released at the time this redbook was written.

5.2.1.2 Native Sockets Services

Socket/MPTS provides the support for three kinds of address families for the Sockets application programming interfaces (APIs):

1. TCP/IP Address family (AF_INET)
2. NetBIOS Address family (AF_NB)
3. NetBIOS OS/2 Address family (AF_OS2)

It also provides a local IPC transport for Sockets applications (inter-process communications support that does not issue any calls to the network).

If a Sockets application has been coded to use a certain address family, it would normally be bound to the transport protocol this address family supports. For example, an application using the AF_INET Address family would also use TCP/IP as its transport protocol. This is called *native* transport.

Please see page 132 of the redbook titled *Inside OS/2 Warp Server, Volume 1*, SG24-4602, for an overview and a diagram of the structure of the Sockets/MPTS component of Adapter and Protocol Services.

5.2.2 Non-native Sockets Services Provided with AnyNet/2

If you need to run a Sockets application over a different transport and there is only support for native transport, you will have to rewrite the application to use the address family that is native to the other transport protocol. With the Multiprotocol Transport Network architecture and the AnyNet product family, however, IBM introduces the capability of *non-native* networking. This means an application can use any transport network, even if that transport is not natively supported by the application. In that case, a program which has been coded to use the AF_INET Address family could use the NetBIOS, IPX, or SNA protocol without having to be rewritten to use the respective Address family. Figure 226 on page 301 shows a functional diagram of non-native Sockets services provided with AnyNet/2.

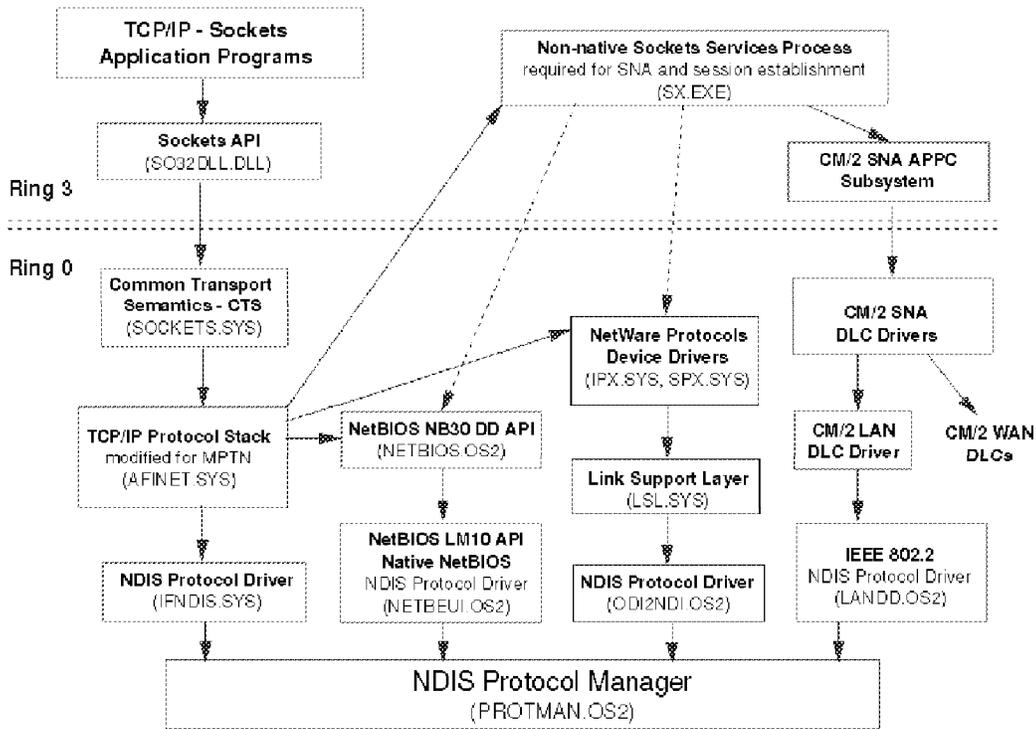


Figure 226. Sockets over NetBIOS - Native and Non-native

Notes:

1. Following the path from the TCP/IP - Sockets application program right down to the NDIS protocol manager represents the native support for AF_INET Sockets applications.
2. All the non-native support paths start at the modified TCP/IP protocol stack driver (AFINET.SYS) and are directed to the respective APIs (NetBIOS or IPX/SPX) or to the non-native Sockets services process (SX.EXE).
3. In case of Sockets over NetBIOS and Sockets over IPX, the non-native Sockets services process is employed for session establishments only. Application data will not have to perform additional ring transitions. This is indicated by using a broken line for the arrows in the path.

AnyNet Changes

Please note that in Figure 226, the Sockets over NetBIOS and Sockets over IPX functions were available with the AnyNet/2 Version 2 product, but are not available in the IBM Communications Server.

5.3 Benefits of Adding AnyNet Function to OS/2 Warp Server

Looking at corporate networks today, many of them are still based on the IBM System Network Architecture (SNA), or at least include SNA systems and backbone networks. This may be the result of historic growth, reliability over several decades, and the ease of centralized systems management.

With the evolution of LANs and client/server computing, other communication protocols and architectures have been developed which better suit the task of

workgroups and distributed applications and which are also somewhat easier to understand, install, and configure than SNA used to be. These protocols include TCP/IP, NetBIOS, IPX, and AppleTalk, just to name a few. It is mainly in this area the OS/2 Warp Server product is targeted and can bring its full strengths to bear. SNA capabilities are not part of OS/2 Warp Server, but can be added to it.

Based on our experience, LANs often evolved in areas where either no communication infrastructure existed before or where the centralized networking structure did not meet the needs for individual computing. Following a trend in the early '90s, many corporations also decided to down-size their computing environments from mainframes to workgroup servers, from centralized databases and management to distributed client/server computing. It was a surprise to many of them that there were sometimes even more costs involved in making such changes than there was money saved by making them.

This leads to the necessity of finding the right combination of workgroup and corporate computing. Here are some considerations:

- Though many protocols may coexist on a LAN, not all of them are designed for WAN communications.
- If a backbone network is already in place, it may be wise to employ it to interconnect workgroup LANs in order to preserve investments in skills and technology infrastructure.
- If corporate applications are already in use, it may turn out to be too expensive to replace them to fit into the new computing environment; so there will be a need to run applications unchanged over new protocols.
- Departments and branches of an organization may require a high degree of independence and flexibility in choosing applications and network operating systems - and the protocols that go along with them - to meet the specific needs of their users and business objectives.
- Such more or less autonomous networks may still need to have access to resources from other parts of that organization or from external sources which should be provided for.
- Last but not least, such an amalgamation of networks should remain manageable; this is especially true of the interconnection backbone and can be more easily achieved if the number of protocols on the backbone can be reduced.

Figure 227 on page 303 shows a scenario for a corporate network.

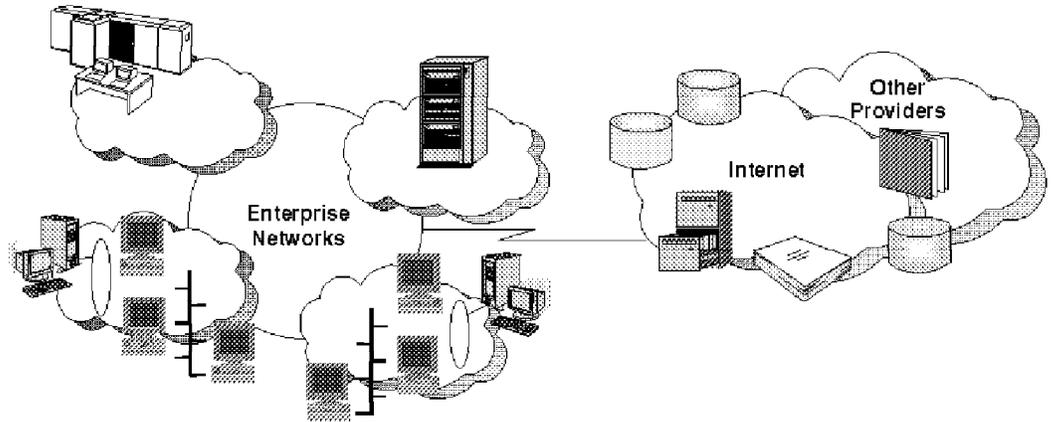


Figure 227. AnyNet and Corporate Networks

This is the point where AnyNet joins the game. It provides:

- Single backbone protocol concentration eliminates the complexity of multiple protocol stacks.
- Applications can communicate over non-native networks without the need to be modified.
- AnyNet access nodes provide mobile users with an easy attachment to distributed applications via a corporate network.
- AnyNet gateway nodes provide easy connection of workgroup LANs via a corporate backbone network.
- Non-SNA applications running over SNA benefit from SNA networking features, such as:
 - Cost-effective bandwidth utilization
 - Predictable response times
 - Traffic prioritization
 - Data compression
 - High-performance routing
- AnyNet protects SNA backbone from LAN broadcast storms by:
 - Filtering IPX, NetBIOS, TCP/IP broadcasts
 - Caching names
- Non-TCP/IP applications running over TCP/IP benefit from TCP/IP networking features, such as:
 - Router-based networks
 - Access to worldwide Internet

Figure 228 on page 304 outlines the convergence between LAN and WAN networking as provided by AnyNet.

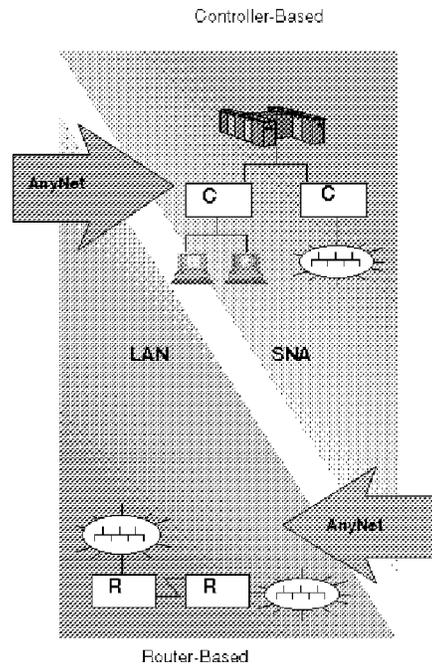


Figure 228. AnyNet LAN - WAN Convergence Benefits

In the sections before, we talked about the great variety of application and networking protocols that AnyNet can combine. This combination of OS/2 Warp Server and AnyNet function, such as that in the IBM Communications Server, into a very complete solution for integrating workgroup computing and corporate backbone networks.

5.4 Related Publications

This section provides the reader with a list of selected publications for further reading on the topics discussed in this chapter.

- *Communications Server for OS/2 Warp V4.0 Enhancements*, SG24-4587
- *Communications Server for OS/2 V4 Up and Running*, GT01-1310
- *Communications Server for OS/2 V4.1 Up and Running*, GC31-8189
- *MPTN Architecture - Technical Overview*, GC31-7073
- *AnyNet Sockets over SNA User's Guide*, GV40-0376
- *AnyNet Sockets over SNA Gateway User's Guide*, GV40-0374
- *AnyNet Sockets over NetBIOS User's Guide*, SV40-0111
- *AnyNet Sockets over IPX User's Guide*, SV40-0112
- *AnyNet SNA over TCP/IP User's Guide*, GV40-0375
- *AnyNet SNA over TCP/IP Gateway User's Guide*, GV40-0216
- *AnyNet NetBEUI over SNA Administrator's Guide*, GV40-0402
- *AnyNet IPX over SNA Gateway User's Guide*, GV40-0405
- *2217 Nways Multiprotocol Concentrator - User's Guide*, GC30-3706
- *MPTN Architecture and Product Implementations*, SG24-4170
- *AnyNet SNA over TCP/IP - Installation and Interoperability*, GG24-4395
- *AnyNet Sockets over SNA and NetBIOS over SNA - Installation and Interoperability*, GG24-4396

Chapter 6. Brief Look at OS/2 Warp Server SMP

During the development of this redbook, the OS/2 Warp Server Advanced, Symmetric Multiprocessing (SMP) Feature was announced and became generally available. It is our intent to cover OS/2 Warp Server SMP in much greater detail in an upcoming ITSO redbook publication. However, we have included some information in this chapter so the OS/2 Warp Server administrator can understand some of the changes and enhancements that have been included in OS/2 Warp Server SMP. It is up to the administrator to evaluate these new features and understand the benefits before implementing OS/2 Warp Server SMP in a production environment.

This chapter introduces OS/2 Warp Server SMP and lists the supported hardware platforms. We also discuss some of the changes and enhancements for each component of OS/2 Warp Server SMP. A list of related publications is included at the end of the chapter for more in-depth information.

6.1 Introducing OS/2 Warp Server SMP

OS/2 Warp Server Advanced, SMP Feature contains all the major components and capabilities that were present in OS/2 Warp Server. This includes File and Print Services, Remote Access Services, System Management Services, Backup and Recovery Services, Advanced Print Services and TCP/IP Services. Ask your IBM representative about the procedures for obtaining a copy of OS/2 Warp Server SMP. You may also refer to the following Web page for additional information:

<http://www.austin.ibm.com/pspinfo/warp-server/>

One of the major enhancements over the existing version of OS/2 Warp Server is the exploitation of Intel-based systems with *Symmetric Multiprocessing* support, also known as *SMP*. SMP is the capability of a computer system to contain more than one processor, or CPU. With the corresponding software support, two or more CPUs can work together to execute programs, analyze data and process information at the same time. This is possible because the CPUs share the same memory and are running under a single operating system. The actual SMP architectural specifics are well-defined and are discussed in greater detail in publications listed at the end of this chapter.

What kind of software support is needed for SMP? First of all, the operating system must explicitly support SMP. It must be capable of dispatching units of work, called *threads*, to each individual processor. The original version of OS/2 Warp Server supported the Intel single-processor platform, but did not provide SMP support. IBM has stated in the past that it would provide this capability, and the availability of OS/2 Warp Server SMP is the product that accomplishes this.

What about applications? Do they need to be rewritten to take advantage of SMP systems? Luckily, the answer is *no*. Although the programmer must understand threads to write a multi-threaded application (that is, an application that can have several events happening concurrently), it is the operating system that interfaces with the SMP hardware. Applications are not aware that the hardware being used is SMP-capable. Although an application has no knowledge of SMP, it can still benefit from SMP capabilities. An existing

application may run much faster on an SMP hardware platform than it did on the single-processor platform. The actual performance gains are dependent on many variables, such as the nature of the application, how much I/O is done, and the amount of threading being done.

6.2 Supported SMP Hardware Platforms

OS/2 Warp Server SMP requires hardware that is SMP-enabled, including systems with Pentium Pro, Pentium and 80486 processors. The systems must conform to the Intel Advanced Programmable Interrupt Controller (APIC) standard, Version 1.1 or 1.4. OS/2 Warp Server SMP also includes support for some proprietary SMP systems and are also listed below.

Currently, support for up to six-processor systems is tested, although the OS/2 Warp Server SMP architecture will allow up to 64-processor support. For the latest information on the supported hardware platforms, please refer to the following Web Page:

<http://www.austin.ibm.com/pspinfo/wssmp.htm>

The following systems have been tested and are supported with OS/2 Warp Server SMP. They are listed here for your convenience:

<i>Table 26 (Page 1 of 2). Systems Supported by OS/2 Warp Server SMP</i>				
Vendor	Model	CPU	Speed	# CPUs
Pentium Pro Systems				
IBM	PC Server 704	P6	166MHz	1-4
Compaq	ProLiant 5000	P6	166MHz	1-4
HP	NetServer LX	P6	166MHz (200)	1-4
Olivetti	SNX 460	P6	166MHz	1-4
ALR	Dual 6	P6	200MHz	1-2
Pentium / 486 Systems				
IBM	PC Server 720	P5	100MHz (166)	1-6
IBM	PC Server 520	P5	100MHz (133)	1-2
IBM	PC Server 320	P5	90MHz (133)	1-2
Compaq	ProLiant 4500	P5	100MHz (133)	1-4
Compaq	ProLiant 4500	P5	100MHz (133)	1-4
Compaq	ProLiant 1500	P5	100MHz (133)	1-2
Compaq	ProLiant 4000	P5	66MHz	1-4
Compaq	ProLiant 2000	P5	66MHz	1-2
Compaq	ProLiant 4500	P5	100MHz (133)	1-4
Compaq	ProLiant 4500	P5	100MHz (133)	1-4
HP	NetServer LS	P5	133MHz (166)	1-4
HP	NetServer LH	P5	100MHz	1-2
Unisys	PW2 Premier SXE	P5	100MHz (166)	1-4
Dell	OptiPlex DGX 5166	P5	166MHz	1-2
Dell	PC PowerEdge XE5100-2	P5	100MHz	1-2
Dell	PowerEdge XE590-2	P5	90MHz	1-2

Digital	Prioris XL 5100DP	P5	100MHz	1-2
Olivetti	SNX 400	P5	166MHz	1-2
Olivetti	SNX 160S	P5	166MHz	1-2
ALR	Revolution Q-SMP	P5	166MHz	1-2
ALR	ProVEISA SMP	486	66MHz	1-2
NCR (AT&T)	3416XL	P5	133MHz	1-2
DFI	E525	P5	133MHz	1-2
SAG	1462	P5	166MHz	1-2
AST	Manhattan	P5	60MHz	1-6
AST	Manhattan	486	60MHz	1-6
Tricord	PowerFrame Mod 30/40	486	66MHz	1-2
Wyse	Series 70001 Mod 760	Not Supported (see note 1)		
Note:				
1. The Wyse Series 70001 Model 760 is not supported by OS/2 Warp Server SMP.				
2. A number in parentheses after the speed indicates that OS/2 Warp Server SMP supports this model with the processors upgraded to that speed.				

6.3 New Base Features

OS/2 Warp Server SMP has introduced some enhancements for applications that use large amounts of disk space or memory. A subset of them are listed below:

- Extended APIs for High Memory Support

In the previous implementations of OS/2, including OS/2 V3 and OS/2 Warp Connect, applications were limited to the first 512MB of the OS/2 32-bit virtual address space. OS/2 Warp Server SMP has enabled *High Memory Support (HMS)*, which allows OS/2 32-bit applications to address and allocate memory in the areas from 512 MB to 3 GB. This allows greater freedom and performance for those applications which make extensive use of RAM.

- Raw I/O File System

Normally, when an application running under OS/2 makes a request to read or write to a disk, this request is handled by the corresponding component in the OS/2 disk subsystem. With a RAW I/O file system, it is now possible for an *application* to directly manage a logical partition or physical disk, instead of having the operating system execute I/O requests. Applications that make use of the Raw I/O capability can see this partition or drive as a single file. Usually, these applications manage large amounts of data and handle many concurrent requests, such as a database. Allowing the applications to directly control I/O results in greater performance, since the overhead of OS/2 serialization of I/O is avoided.

In addition, the Raw File System allows access to physical drives or partitions using a Universal Naming Convention (UNC) name. Since a drive letter is not needed, this allows access to more than 26 partitions when using the Raw File System.

- Tracing and Monitoring

OS/2 Warp Server SMP has included a software trace tool called STRACE, which allows ring 3 applications to store timing and tracing information in a software trace buffer. Also, trace hooks have been added to OS/2 which give software developers an effective mechanism for accessing and monitoring system performance and processor status information.

OS/2 Warp Server SMP includes three kernels (core operating system function):

Type	Description
Retail	This is the default kernel for the OS/2 Warp Server SMP installation. It has the smallest memory requirements of the three kernels provided.
H-Strict	This kernel includes debugger function, but not all of the debug checks that are included in the debug kernel. This is useful for OS/2 timing-related problems which cannot be reproduced using the debug kernel.
Debug	This kernel includes debugger function as well as all debug checks. It has the largest memory requirements due to the additional debug support.

The IBM Software Support Centers may use the H-strict or Debug kernel when working with IBM Customers on difficult OS/2 problems. OS/2 Warp Server SMP now includes the serial dial protocols and support necessary to work remotely with the IBM Software Support Centers.

Compared to the OS/2 in OS/2 Warp Server (Version 3.01, SYSLEVEL XR_x3005), the OS/2 in OS/2 Warp Server SMP is at a slightly higher revision level (Version 3.02, SYSLEVEL XR_x3006). The version of OS/2 included in OS/2 Warp Server SMP is at FixPak 22.

6.4 Adapter and Protocol Services

The Adapter and Protocol Services provided in OS/2 Warp Server were not SMP-enabled. IBM has written a version of Adapter and Protocol Services that is SMP-specific, and is included in OS/2 Warp Server SMP. The SYSLEVEL Version of Adapter and Protocol Services is WR_x8500. (The x will vary, depending on the language version. In the United States, the SYSLEVEL is WR08500.)

The total number of NetBIOS connections has been increased to 3000, configurable within the MPTS Configuration program. Note that the system is still limited to about 1000 concurrent NetBIOS sessions.

Beginning with MPTS FixPak WR_x8210, IBM added new functionality in the TCPBEUI (NetBios over TCP/IP) protocol driver. TCPBEUI allows NetBIOS to be remapped according to the Internet RFC 1001/1002 specifications. This allows NetBIOS applications to communicate over a TCP/IP network. This mechanism is *not* encapsulation, as were previous implementations of NetBIOS over TCP/IP.

The new functions of the Adapter and Protocol Services in OS/2 Warp Server SMP add Hybrid node (H-node) and Point-to-Point-node (P-node) support, which enable the use of a NetBIOS Name Server and a NetBIOS Datagram Distributor. Without this support, TCPBEUI must use a broadcast in order to resolve NetBIOS names to IP addresses. Using H-node and/or P-node make network usage more

efficient and allow for greater scalability of the TCPBEUI environment. For more information on TCPBEUI, refer to *Inside OS/2 Warp Server, Volume 1: Exploring the Core Components*, Chapter 6, SG24-4602.

With each new release of Adapter and Protocol Services within a product, IBM continues to expand the number of adapters supported. MPTS FixPak WRx8210 added support for 22 more adapters. The following is a list of adapters whose support has been newly added in OS/2 Warp Server SMP (beyond WRx8210):

- 3Com EtherLink III LAN+Modem PC Card for OS2 v1.5 - Card Services
- 3Com EtherLink III PC Card OS/2
- 3Com TokenLink III PC Card Adapter - OS/2
- AMD PCNet Family Ethernet Adapter
- Digital Semiconductor DC21X4-based Ethernet Adapter
- IBM 100/10 PCI Ethernet Adapter
- IBM EtherJet ISA Ethernet Adapter
- IBM PCI Ethernet Adapter Driver
- Kingston EtheRx LC ISA Ethernet Adapter
- Kingston EtheRx PCI Ethernet Network Adapter
- Olicom Token-Ring PCMCIA Card

6.5 File and Print Services

The File and Print Sharing Services in OS/2 Warp Server SMP, also known as LAN Services, are at a slightly higher level than OS/2 Warp Server (Version 5.03, SYSLEVEL IPx8500). OS/2 Warp Server SMP includes the LAN Server Advanced function of File and Print Sharing Services, including 386HPFS support, Fault Tolerance and Local Security.

The Tuning Assistant, which allows you to automatically configure various system resources, such as NetBEUI, has been modified. Normally, the File and Print component tries to allocate a large amount of available RAM for the HPFS386 cache of the Advanced Server. If you are running other IBM Software Servers, such as the DB2/2 or Transaction Server on the same system, you may need to specify a smaller cache size so that the performance of the other applications is acceptable. The Tuning Assistant limits the HPFS386 cache size to 25% of memory as a default in order to allow for other IBM Software Servers.

6.6 TCP/IP Services

The TCP/IP protocol stack (Version 3.5, SYSLEVEL UN00000) included with OS/2 Warp Server SMP has the following enhancements:

- SMP-enablement

The TCP/IP protocol stack in OS/2 Warp Server SMP is designed to function specifically with SMP-enabled systems. This version does not function on non-SMP Intel machines. SMP systems with only one processor *are* supported.

- Based on OS/2 Warp Version 4 TCP/IP protocol stack

This protocol stack is nearly identical to the OS/2 Warp Server stack. There are a few enhancements:

- Variable subnet routing

The IFCONFIG and the TCP/IP Configuration programs allow the specification of a unique subnet mask for each lan interface defined to the system.

- Aliasing

The HOSTS file can be used for host name address resolution. This file lists the IP address and name of a TCP/IP host, and it now allows one or more *alias* name to be specified for a given host.

Note: Variable subnet routing and aliasing functions are included in the TCP/IP stack with OS/2 Warp Server SMP, but these functions are *not* officially supported by IBM in the OS/2 Warp Server SMP environment. They are only supported with OS/2 Warp Version 4.

- Defect fixes

Two notable problems, which are resolved in this version of TCP/IP, are:

- Intel 100 MB PCI Ethernet adapter compatibility
- ARP requests not being received by sender

The standard TCP/IP applications included are functionally identical to the previous version included in OS/2 Warp Server. Minor changes were made to the TCP/IP stack for better communications performance and throughput.

6.7 Remote Access Services

Remote Access Services has been enhanced to work on SMP-enabled systems. The product functions have not changed significantly from the version in OS/2 Warp Server. The SYSLEVEL version is now LD08600.

6.8 Backup and Recovery Services

OS/2 Warp Server Backup/Restore has a higher revision level and SYSLEVEL (V5.01, SYSLEVEL 3009011) compared to the version in OS/2 Warp Server. In addition, OS/2 Warp Server Backup/Restore has several changes and enhancements. Some of them are:

- Locked files support

In the previous release, when a locked file was encountered, OS/2 Warp Server Backup/Restore skipped the file and continued. The backup log showed that the file was not backed up. This release adds support to back up files currently locked by applications or even by OS/2 itself. For example, the LOG0001.DAT file (held open by OS/2) can be backed up successfully.

- New Tape Device Support

- Archive Python (4mm)
- Archive 4326NP/RP (4mm)
- Archive 4586NP/RP (4mm)
- HP Jetstore 6000e (4mm)
- SONY SDT7000 (4mm)
- DEC TZ87/TZ87N (DLT)
- DEC TZ88/TZ88N (DLT)
- Quantum DLT 2000XT (DLT)

- Defect fixes

Several of these fixes provide enhancements for performance and capacity. For example, read/write optical drive performance has been improved, and index file manipulation at the end of a backup has been enhanced. See the Web site referenced on page 283 for more information.

- *Generic* device support

OS/2 Warp Server Backup/Restore can now utilize storage devices that are not on the list of supported devices. The Storage Devices panel will show any storage device reported by OS/2, and this drive may be utilized by OS/2 Warp Server Backup/Restore. You may also select Refresh in the Storage Devices panel to view new devices.

- Disaster Recovery changes

The diskette creation mechanism has changed. The administrator now uses the MAKEDISK utility to create the OS/2 Boot diskettes. The Disaster Recovery Utility adds the PSnS drivers and places utilities on a third diskette, but does not create the OS/2 diskettes 1 and 2 anymore.

6.9 System Management Services

In OS/2 Warp Server, the SystemView product provided much of the functionality for System Management Services. In OS/2 Warp Server SMP, the TME10 NetFinity Server component now provides these same capabilities and more. TME10 NetFinity Server now supports the following clients:

- OS/2 V3 and above
- Windows 3.1
- Windows for Workgroups (new)
- Windows 95 (new)
- Windows NT (new)
- NetWare (new)

The original SystemView clients included with OS/2 Warp Server will still function with TME10 NetFinity Server, but the new clients included with TME10 NetFinity Server, such as Windows NT and Netware, will not function with the SystemView Server. The TME10 NetFinity Server should be used instead.

TME10 NetFinity Server has several features not included in the SystemView product, including:

- Communications

TME10 NetFinity Server can use APPC to communicate with NetView Distribution Manager for MVS.

- Web-based administration

TME10 NetFinity Server includes a NetFinity Server Web Manager, which allows the administrator to use a Web Browser to access and control TME10 NetFinity Server-managed systems. This capability greatly extends the administrator's reach. The URL used to manage a host whose name is `hostname` is `http://hostname:411/main`. The TCP/IP port number for administration is 411. We also recommend that you use a Java-enabled browser.

6.10 Advanced Print Services

Advanced Print Services has been enhanced to function in an SMP-enabled environment. The Version number and SYSLEVEL (V2.00, SYSLEVEL UR00000) and product functionality have not changed compared to PSF/2 included in OS/2 Warp Server. Advanced Print Services in OS/2 Warp Server SMP now supports host printers that handle up to 708 pages per minute.

6.11 Client License Management

In order for a user to access OS/2 Warp Server and OS/2 Warp Server SMP resources, that user requires a use-based feature. In other words, IBM no longer charges for the client code, but it does charge for accessing servers. There is no software-based mechanism that enforces this requirement. It is the responsibility of the administrator or license tracker within a company to ensure compliance with these license agreements.

OS/2 Warp Server SMP now includes a utility which allows the administrator to maintain a database of users who are authorized to access the server. The information kept for each user includes user serial number, File & Print ID, Remote Access ID, System Management machine ID, and Server ID. The administrator can check this information against the databases for File & Print and Remote Access. Also, the license database can be easily imported to and exported from Lotus Notes or any other database that supports structured text formats. This utility allows the administrator to easily track users and ensure voluntary compliance with the OS/2 Warp Server SMP license agreements.

6.12 Related Publications

The following publications are suitable for additional information on some of the topics discussed in this chapter.

- *OS/2 Warp Server Advanced Easy Start Version 4*, S28H-0151
- *OS/2 Warp Server Advanced Up and Running! Version 4*, S28H-0152
- *TME10 NetFinity Server Up and Running!*, Online document shipped with OS/2 Warp Server
- *TME10 NetFinity Server Scenarios*, Online document shipped with OS/2 Warp Server
- *OS/2 Warp Server: A Network Operating System Study*, SG24-4786 (in press)

Appendix A. SystemView in Warp Server and Software Distribution: Sample Configuration Files

A.1 System Information Tool: SCSI Subsystem Information

```
***** System Information Tool - W4602S16 *****
***** SCSI Subsystem Information *****
***** SCSI Adapter Information *****
IBM SCSI Adapter
Physical Unit Number (PUN) : 7
Logical Unit Number (LUN) : 0
Bus Type : SCSI 2
Location : Slot 5
Bus Attributes : 8 Bit
I/O Access : Bus Master
Host Bus : Micro Channel Bus
Host Bus Width : 32 Bit Bus Width
Arbitration level : 12
Fairness : On
ROM Wait State : Enabled
Adapter Attributes : Supports addresses above 16 MB
Adapter Attributes : Supports IBM SCB commands
Adapter Attributes : Supports scatter/gather in hardware
Adapter Attributes : Supports CHS addressing in hardware
Maximum Scatter Gather List : 16
Maximum CDB Length : Not Applicable
ADD Major Level : 1
ADD Minor Level : 0
Device(s) connected : 5
Fixed Disk
Fixed Disk
Fixed Disk
CD ROM Device
Optical Device

***** SCSI Devices For Adapter *****

Device Type : Fixed Disk
Device Size : 210,944 Kilobytes
Device Unit PUN : 6
Device Unit LUN : 0
ANSI Level Supported : ANSI SCSI-2
Unit Status : Ready and Powered On
Media Status : Present
Vendor ID : IBM
Product ID : WDS-3200 !J
Product Revision Level : S560
Vendor Field : 7587218353G8000
Vendor Data : 0693 95F4749 S56C
Device Filter ADD : Present
Device Attributes : Device supports synchronous data transfers
Device Attributes : Device supports linked commands
Device Attributes : Prefetch Not Supported
Device Attributes : Device Not Defective
```

Figure 229 (Part 1 of 3). Output of SCSI System Information

```

***** SCSI Devices For Adapter *****
Device Type       : Fixed Disk
Device Size      : 391,168 Kilobytes
Device Unit PUN  : 5
Device Unit LUN  : 0
ANSI Level Supported : ANSI SCSI-2
Unit Status      : Ready and Powered On
Media Status     : Present
Vendor ID        : IBM
Product ID       : 0661467
Product Revision Level : G 1
Vendor Field     : 0517628955F8335
Vendor Data      : 098092289 00022273F8955      894756      73F9121      894766
Device Filter ADD : Present
Device Attributes : Device supports synchronous data transfers
Device Attributes : Device supports linked commands
Device Attributes : Prefetch Not Supported
Device Attributes : Device Not Defective
***** SCSI Devices For Adapter *****
Device Type       : Fixed Disk
Device Size      : 391,168 Kilobytes
Device Unit PUN  : 4
Device Unit LUN  : 0
ANSI Level Supported : ANSI SCSI-2
Unit Status      : Ready and Powered On
Media Status     : Present
Vendor ID        : IBM
Product ID       : 0661467
Product Revision Level : G 1
Vendor Field     : 0524288655F8335
Vendor Data      : 098092244 00022273F8955      894756      73F9121      894766
Device Filter ADD : Present
Device Attributes : Device supports synchronous data transfers
Device Attributes : Device supports linked commands
Device Attributes : Prefetch Not Supported
Device Attributes : Device Not Defective
***** SCSI Devices For Adapter *****
Device Type       : CD ROM Device
Device Size      : 457,398 Kilobytes
Device Unit PUN  : 2
Device Unit LUN  : 0
ANSI Level Supported : ANSI SCSI-1
Unit Status      : Ready and Powered On
Vendor ID        : TOSHIBA
Product ID       : CD-ROM DRIVE:XM
Product Revision Level : 3232
Device Filter ADD : Present
Device Attributes : Media can be removed
Device Attributes : Media Change Line not supported
Device Attributes : Prefetch Not Supported
Device Attributes : Device Not Defective

```

Figure 229 (Part 2 of 3). Output of SCSI System Information

```
***** SCSI Devices For Adapter *****
Device Type       : Optical Device
Device Size       : Not Available
Device Unit PUN   : 1
Device Unit LUN   : 0
ANSI Level Supported : ANSI SCSI-2
Unit Status       : Unknown
Vendor ID         : IBM
Product ID        : MD3125B EH140!B
Product Revision Level : 0
Device Filter ADD : Not Present
Device Attributes : Device supports synchronous data transfers
Device Attributes : Device supports linked commands
Device Attributes : Media can be removed
Device Attributes : Media Change Line not supported
Device Attributes : Prefetch Not Supported
Device Attributes : Device Not Defective
***** System Information Tool - W4602S16 *****
```

Figure 229 (Part 3 of 3). Output of SCSI System Information

A.2 Software Inventory

The Software Inventory section shows an example of the Software Inventory Report, detailing the software found on a test system.

A.2.1 Software Inventory Report Example

```
System Name: silverdancer
Dictionary Name: E:\SYSVIEW2\BIN\DEFAULT.SID
=====
Product Name: IBM OS/2 LAN Adapter and Protocol Support
Vendor Name: IBM Corp.
Version: 2.70
Revision: WR08000_
Location: C:\IBMCOM
Application Type: Network
=====
Product Name: IBM OS/2 LAN Requester
Vendor Name: IBM Corp.
Version: 4.00
Revision: IP08000_
Location: C:\IBMLAN
Application Type: Network
=====
Product Name: IBM OS/2 User Profile Management
Vendor Name: IBM Corp.
Version: 4.00
Revision: WR08000_
Location: C:\MUGLIB
Application Type: Network
=====
Product Name: IBM OS/2 User Profile Management - Extended
Vendor Name: IBM Corp.
Version: 4.00
Revision: IP08000_
Location: C:\MUGLIB
Application Type: Network
```

Figure 230 (Part 1 of 3). Software Inventory Report Example

```

=====
Product Name: IBM NetFinity Manager for OS/2
Vendor Name: IBM Corp.
Version: 3.00
Revision: NM00210_
Location: C:\NETFIN
Application Type: System Management
=====
Product Name: IBM NetFinity Services for OS/2
Vendor Name: IBM Corp.
Version: 3.00
Revision: NS00210_
Location: C:\NETFIN
Application Type: System Management
=====
Product Name: Lotus Notes for OS/2
Vendor Name: Lotus Development Corp.
Location: C:\NOTES32
Application Type: Mail
=====
Product Name: IBM OS/2 First Failure Support Technology/2
Vendor Name: IBM Corp.
Version: 1.20
Revision: WR00485_
Location: C:\OS2
Application Type: Default
=====
Product Name: IBM C/C++ Tools (Compiler)
Vendor Name: IBM Corp.
Version: 3.00
Revision: CTC301
Location: C:\IBM CPP\SYSLEVEL
Application Type: Software Development
=====
Product Name: IBM C/C++ Tools (Utilities)
Vendor Name: IBM Corp.
Version: 3.00
Revision: CTU300
Location: C:\IBM CPP\SYSLEVEL
Application Type: Software Development
=====
Product Name: IBM C/C++ Tools (Class Libraries)
Vendor Name: IBM Corp.
Version: 3.00
Revision: CTO301
Location: C:\IBM CPP\SYSLEVEL
Application Type: Software Development
=====
Product Name: IBM OS/2 32-bit Graphics Engine
Vendor Name: IBM Corp.
Version: 3.00
Revision: XR03003_
Location: C:\OS2\INSTALL
Application Type: Operating System
=====
Product Name: IBM OS/2
Vendor Name: IBM Corp.
Version: 3.00
Revision: XR03003_
Location: C:\OS2\INSTALL
Application Type: Operating System

```

Figure 230 (Part 2 of 3). Software Inventory Report Example

```

=====
Product Name: IBM TCP/IP BASE for OS/2 2.0 and 2.1
Vendor Name: IBM Corp.
Version: 3.00
Revision: IC00000_
Location: C:\tcPIP\BIN
Application Type: Network

```

Figure 230 (Part 3 of 3). Software Inventory Report Example

A.2.2 Exporting Software Inventory Data to a Database

```

Table=SOFTWARE_INVENTORY[0]
SYSTEM_ID="silverdancer"
MANAGING_ID="TESTINIENRIQUED"
GROUP_NAME="All Systems"
PROGRAM_TITLE="IBM OS/2 LAN Adapter and Protocol Support"
VERSION="2.70"
RELEASE_LEVEL="WR08000_"
VENDOR_NAME="IBM Corp."
LOCATION="C:\IBMCOM"
SOFT_INV_DATETIME="1995-09-22-09.23.43.000000"
Table=SOFTWARE_INVENTORY[1]
SYSTEM_ID="silverdancer"
MANAGING_ID="TESTINIENRIQUED"
GROUP_NAME="All Systems"
PROGRAM_TITLE="IBM OS/2 LAN Requester"
VERSION="4.00"
RELEASE_LEVEL="IP08000_"
VENDOR_NAME="IBM Corp."
LOCATION="C:\IBMLAN"
SOFT_INV_DATETIME="1995-09-22-09.23.43.000000"
Table=SOFTWARE_INVENTORY[2]
SYSTEM_ID="silverdancer"
MANAGING_ID="TESTINIENRIQUED"
GROUP_NAME="All Systems"
PROGRAM_TITLE="IBM OS/2 User Profile Management"
VERSION="4.00"
RELEASE_LEVEL="WR08000_"
VENDOR_NAME="IBM Corp."
LOCATION="C:\MUGLIB"
SOFT_INV_DATETIME="1995-09-22-09.23.43.000000"
Table=SOFTWARE_INVENTORY[3]
SYSTEM_ID="silverdancer"
MANAGING_ID="TESTINIENRIQUED"
GROUP_NAME="All Systems"
PROGRAM_TITLE="IBM OS/2 User Profile Management - Extended"
VERSION="4.00"
RELEASE_LEVEL="IP08000_"
VENDOR_NAME="IBM Corp."
LOCATION="C:\MUGLIB"
SOFT_INV_DATETIME="1995-09-22-09.23.43.000000"

```

Figure 231 (Part 1 of 3). Exporting Software Inventory Data to a Database

```

Table=SOFTWARE_INVENTORY[4]
  SYSTEM_ID="silverdancer"
  MANAGING_ID="TESTINIENRIQUED"
  GROUP_NAME="All Systems"
  PROGRAM_TITLE="IBM NetFinity Manager for OS/2"
  VERSION="3.00"
  RELEASE_LEVEL="NM00210_"
  VENDOR_NAME="IBM Corp."
  LOCATION="C:\NETFIN"
  SOFT_INV_DATETIME="1995-09-22-09.23.43.000000"
Table=SOFTWARE_INVENTORY[5]
  SYSTEM_ID="silverdancer"
  MANAGING_ID="TESTINIENRIQUED"
  GROUP_NAME="All Systems"
  PROGRAM_TITLE="IBM NetFinity Services for OS/2"
  VERSION="3.00"
  RELEASE_LEVEL="NS00210_"
  VENDOR_NAME="IBM Corp."
  LOCATION="C:\NETFIN"
  SOFT_INV_DATETIME="1995-09-22-09.23.43.000000"
Table=SOFTWARE_INVENTORY[6]
  SYSTEM_ID="silverdancer"
  MANAGING_ID="TESTINIENRIQUED"
  GROUP_NAME="All Systems"
  PROGRAM_TITLE="Lotus Notes for OS/2"
  VERSION=NULL
  RELEASE_LEVEL=NULL
  VENDOR_NAME="Lotus Development Corp."
  LOCATION="C:\NOTES32"
  SOFT_INV_DATETIME="1995-09-22-09.23.43.000000"
Table=SOFTWARE_INVENTORY[7]
  SYSTEM_ID="silverdancer"
  MANAGING_ID="TESTINIENRIQUED"
  GROUP_NAME="All Systems"
  PROGRAM_TITLE="IBM OS/2 First Failure Support Technology/2"
  VERSION="1.20"
  RELEASE_LEVEL="WR00485_"
  VENDOR_NAME="IBM Corp."
  LOCATION="C:\OS2"
  SOFT_INV_DATETIME="1995-09-22-09.23.43.000000"
Table=SOFTWARE_INVENTORY[8]
  SYSTEM_ID="silverdancer"
  MANAGING_ID="TESTINIENRIQUED"
  GROUP_NAME="All Systems"
  PROGRAM_TITLE="IBM C/C++ Tools (Compiler)"
  VERSION="3.00"
  RELEASE_LEVEL="CTC301"
  VENDOR_NAME="IBM Corp."
  LOCATION="C:\IBM CPP\SYSLEVEL"
  SOFT_INV_DATETIME="1995-09-22-09.23.43.000000"
Table=SOFTWARE_INVENTORY[9]
  SYSTEM_ID="silverdancer"
  MANAGING_ID="TESTINIENRIQUED"
  GROUP_NAME="All Systems"
  PROGRAM_TITLE="IBM C/C++ Tools (Utilities)"
  VERSION="3.00"
  RELEASE_LEVEL="CTU300"
  VENDOR_NAME="IBM Corp."
  LOCATION="C:\IBM CPP\SYSLEVEL"
  SOFT_INV_DATETIME="1995-09-22-09.23.43.000000"

```

Figure 231 (Part 2 of 3). Exporting Software Inventory Data to a Database

```

Table=SOFTWARE_INVENTORY[10]
  SYSTEM_ID="silverdancer"
  MANAGING_ID="TESTINIENRIQUED"
  GROUP_NAME="All Systems"
  PROGRAM_TITLE="IBM C/C++ Tools (Class Libraries)"
  VERSION="3.00"
  RELEASE_LEVEL="CT0301"
  VENDOR_NAME="IBM Corp."
  LOCATION="C:\IBMCP\SYSEVEL"
  SOFT_INV_DATETIME="1995-09-22-09.23.43.000000"
Table=SOFTWARE_INVENTORY[11]
  SYSTEM_ID="silverdancer"
  MANAGING_ID="TESTINIENRIQUED"
  GROUP_NAME="All Systems"
  PROGRAM_TITLE="IBM OS/2 32-bit Graphics Engine"
  VERSION="3.00"
  RELEASE_LEVEL="XR03003_"
  VENDOR_NAME="IBM Corp."
  LOCATION="C:\OS2\INSTALL"
  SOFT_INV_DATETIME="1995-09-22-09.23.43.000000"
Table=SOFTWARE_INVENTORY[12]
  SYSTEM_ID="silverdancer"
  MANAGING_ID="TESTINIENRIQUED"
  GROUP_NAME="All Systems"
  PROGRAM_TITLE="IBM OS/2"
  VERSION="3.00"
  RELEASE_LEVEL="XR03003_"
  VENDOR_NAME="IBM Corp."
  LOCATION="C:\OS2\INSTALL"
  SOFT_INV_DATETIME="1995-09-22-09.23.43.000000"
Table=SOFTWARE_INVENTORY[13]
  SYSTEM_ID="silverdancer"
  MANAGING_ID="TESTINIENRIQUED"
  GROUP_NAME="All Systems"
  PROGRAM_TITLE="IBM TCP/IP BASE for OS/2 2.0 and 2.1"
  VERSION="3.00"
  RELEASE_LEVEL="IC00000_"
  VENDOR_NAME="IBM Corp."
  LOCATION="C:\tcpip\BIN"
  SOFT_INV_DATETIME="1995-09-22-09.23.43.000000"

```

Figure 231 (Part 3 of 3). Exporting Software Inventory Data to a Database

A.3 CASSETUP Profile Files

The following sections provide sample profiles for some IBM products.

A.3.1 OS/2 Warp 3.0 (WIN-OS/2 Version) Profile File

```

* CASSETUP application profile for: OS/2 Warp 3.0 (WIN-OS2 version)
*****
*
* APPLICATION DESCRIPTION SECTION
*****
* APPNAME is a long descriptive name.
* It can contain blanks. It should be
* unique among all the Application
* Profiles.
APPNAME = OS/2 Warp Server with WIN-OS/2Version 3.05 CD-ROM

```

Figure 232 (Part 1 of 5). CASSETUP Profile for OS/2 Warp Version 3 (OS2WS.PRO)

```

APPNICK = OS2F305
PROGTYPE = 1
ICON = CASSETUP:#111
OS = 1
PACKAGE = 1
* FIXTO =
* FIXLEVEL =
LOADPREREQS = <LCU>

* APPNICK is a short nickname. It is
* used to identify this application in
* other scripts and profiles. It MUST
* be unique among all the App Profiles.
* Case is ignored for this parameter,
* so KILLER10 and killer10 are
* considered equal.

* PROGTYPE tells what kind of
* application this is:
*   Operating System (1),
*   Transport (2),
*   Redirector(3),
* or other (4).

* ICON is the icon to be displayed to
* represent this application in CASSETUP
* A restriction in Release 1.1 of
* CASSETUP is that this must be a
* bitmap (bmp) file or DLL resource.
* The path is relative to the directory
* where cassetup is installed.

* OS tells whether the program runs
* under OS/2 (1) or DOS (2)

* PACKAGE tells whether it is a complete
* application (1) or a fix (2)

* If it is a fix, FIXTO is the APPNICK
* of the application it fixes.

* And FIXLEVEL specifies the relative
* fix level. It can be -1 to indicate
* it is an unsequenced fix.

* Some products required that
* prerequisite products be installed on
* the code server before images can
* be loaded. Put the nicknames of
* the prereq products on this line.
* The special nickname <LCU> indicates
* that Remote Install Support must first
* be installed on the code server.

```

Figure 232 (Part 2 of 5). CASSETUP Profile for OS/2 Warp Version 3 (OS2WS.PRO)

```

*****
*                               *
*           IMAGE LOAD SECTION           *
* (elements in this section describe how the application's *
* install image is put onto a Code Server -- usually by being *
* copied from install diskettes or CD-ROM) *
*****
* The directories below are set up when the application's
* install images are loaded onto the code server.
* APPDIR is the subdirectory (relative
* to the CID mount point) where
* the app's install images will be
* stored. The directory will be created
* if it does not exist.
* The CID Mount Point is specified
* in the CASSETUP gui.

APPDIR =OS2IMAGE

* WORKDIR is a subdirectory (relative
* to the WORK alias) where various
* application-required programs may be
* placed. It is optional, but almost
* every application will need one. The
* directory will be created if it
* does not exist.
* Some CID documentation refers to this
* as the EXE directory.
* The WORK alias is specified in the GUI.

WORKDIR = EXE\OS2F305

* DLLDIR is the directory (relative to
* the DLL alias) where DLLs for
* the product will be placed. Not all
* applications will need one.
* The DLL alias is specified in the GUI.

DLLDIR = DLL\OS2F305

* RSPDIR is the directory (relative to
* the RESP alias) where response
* files will be placed.

RESPDIR = RSP\OS2F305

* LOGDIR is the directory (relative
* to the LOG alias) where log files
* will be placed.

LOGDIR = LOG\OS2F305
* The parameters below describe the methods to be
* used to put the applications's images on the Code Server.
* METHOD defines whether XCOPY or an
* application-supplied program will be
* used to load the images.
* Methods are 1=XCOPY-is-used
*           2=Application-supplied

METHOD = 2

* NUMDSKT is the number of diskettes
* (or CD-ROMS) in the package. It is
* required when the XCOPY method is
* being used, but optional otherwise.

NUMDSKT = 1

```

Figure 232 (Part 3 of 5). CASSETUP Profile for OS/2 Warp Version 3 (OS2WS.PRO)

```

* The next parameter deals with loading the images
* using an application-provided program.
* If METHOD==2 the IMAGELOAD keywords
* specify the commands to be run and
* the meaning of their return codes.
* IMAGELOAD.0 specifies the number of
* commands to be run.

IMAGELOAD.0 = 0

* IMAGELOAD.n is a template for the
* nth command that will be executed.
* Templates may contain Symbolic
* Substitution Parameters, which will be
* replaced by actual values when the
* command line is executed.
* The Symbolic Substitutions supported
* for IMAGELOAD are
* $T      which is replaced by the
*         target path (the path to
*         which code images are to
*         be moved).
* $S      which is replaced by the
*         source drive (and,
*         possibly, path) from which
*         the code images will be
*         copied.
* $W      which is replaced by the
*         fully-qualified path of
*         the Work directory.
* $D      which is replaced by the
*         fully-qualified path of
*         the DLL directory.
* $F      which applies only to CSDs
*         and is replaced by the
*         fully-qualified path of
*         the Work directory of the
*         application being fixed.

IMAGELOAD.1 = XCOPY $$\OS2IMAGE $T /s /e /v /h /o /t /r
IMAGELOAD.2 = GetOSCID $T $W
IMAGELOAD.3 = GetRExx $T $D
IMAGELOAD.4 = GetBoot $T $W

* The next parameter deals with commands to be
* run _before_ the image loading command. They
* are run regardless of the Method selected.
* The work directory, will be put at the front of the
* path and dpath during execution of these steps
* The SETUP keywords specify steps
* to be performed before image
* loading. Commands to unpack the
* load image program, for example, might
* go here.
* SETUP.0 says how many steps there
* are

SETUP.0 = 1

```

Figure 232 (Part 4 of 5). CASSETUP Profile for OS/2 Warp Version 3 (OS2WS.PRO)

```

* SETUP.n gives the prompt text for
* step n. If it is blank, then the
* step is done immediately
SETUP.1 = OS/2 Warp Server 3.05 CD-ROM
* If there is a diskette prompt, then
* the diskette can be verified either by
* Volume Label or presence of a file.
* These elements are optional.
SETUP.1.0MarkerFile = OS2IMAGE\DISK_0\OS2KRNL1
* For each step, there can be as many
* commands as needed. SETUP.n.0 parm
* tells how many commands make up
* step n.
SETUP.1.0 = 0
*****
*
*          INSTALL SECTION
*
* (elements in this section deal with how the application is
* remotely installed).
*****
* INSTCMD is the template of the
* install command. Symbolic
* substitution is supported for $T, $S,
* $D and $W as described above, but
* also for
*   $B (boot drive)
*   $M (Maint dir)
*   $R (response file dir)
*   $V (server name)
*   $F (directory for the /S2 parm)
*   $C (client name)
*   $O (boot drive)
INSTCMD = $W\seinst /b:$B /s:$S /t:$T /l1:$L"client".log /r:
* DEFRESPFILE is the default response
* file name. It is used during
* creation of LCU command files
* to specify a "rspdir/default"
* block for the install command line.
* If it is specified then the response
* file (usually /R) parameter in
* INSTPROG must be at the end of the
* string and be empty. For example:
*   myinstpg /S:something /R:
DEFRESPFILE = default.rsp
* MAINTSYSREQ tells whether the install
* command must be run under a
* maintenance system (1 is yes, 0 no)
MaintSysReq = 1
*****
*
*          MAINTENANCE SYSTEM SECTION
*
* (applications that have a PROGTYPE of 1 (OS), 2 (transport)
* or 3 (redirector) have associated commands that allow them
* to be installed as part of Maintenance Systems. This section
* describes those commands.
*****
* MSCMD.0 tells how many commands
* follow
MSCmd.0 = 2
* MSCMD.n is the template for the nth
* command. Symbolic substitution for
* $T, $W, $D and $S is always supported
* and other translation is available
* during processing of Boot Diskette
* Build scripts.
MSCmd.1 = $W\semaint /s:$S /t:$M /b:$B
/l1:$L"client".log
MSCmd.1.0CmdName = semaint
MSCmd.2 = $W\sedisk /S:$S /T:$T
MSCMD.2.0CmdName = sedisk
MaintSysBuild = 1

```

Figure 232 (Part 5 of 5). CASSETUP Profile for OS/2 Warp Version 3 (OS2WS.PRO)

A.3.2 MPTS 5.0 Profile File

```
* CASSETUP application profile for MultiProtocol Transports, 1.0
* NOTE: lines that begin with an asterisk (*) and blank lines are
* treated as comments

* ALSO NOTE: The format of this file and the syntax of its elements
* are subject to change.

*****
*                APPLICATION DESCRIPTION SECTION                *
*****

* APPNAME is a long descriptive name.
* It can contain blanks. It should be
* unique among all the Application
* Profiles.
APPNAME = Multi-Protocol TransportServices 5.0 from Warp Server
* APPNICK is a short nickname. It is
* used to identify this application in
* other scripts and profiles. It MUST
* be unique among all the App Profiles.
* Case is ignored for this parameter,
* so KILLER10 and killer10 are
* considered equal.
APPNICK = mpts50

* PROGTYPE tells what kind of
* application this is:
*   Operating System (1),
*   Transport (2),
*   Redirector(3),
* or other (4).
PROGTYPE = 2

* ICON is the icon to be displayed to
* represent this application in CASSETUP
* A restriction in Release 1.1 of
* CASSETUP is that this must be a
* bitmap (bmp) file or DLL resource.
* The path is relative to the directory
* where cassetup is installed.
ICON = CASSETUP:#107

* OS tells whether the program runs
* under OS/2 (1) or DOS (2)
OS = 1

* PACKAGE tells whether it is a complete
* application (1) or a fix (2)
PACKAGE = 1

* If it is a fix, FIXTO is the APPNICK
* of the application it fixes.
* FIXTO =

* And FIXLEVEL specifies the relative
* fix level. It can be -1 to indicate
* it is an unsequenced fix.
* FIXLEVEL =
```

Figure 233 (Part 1 of 4). CASSETUP Profile for MPTS 5.0

```

*****
*          IMAGE LOAD SECTION          *
* (elements in this section describe how the application's      *
* install image is put onto a Code Server -- usually by being   *
* copied from install diskettes or CD-ROM)                      *
*****

* The directories below are set up when the application's
* install images are loaded onto the code server.
* APPDIR is the subdirectory (relative
* to the CID mount point) where
* the app's install images will be
* stored. The directory will be created
* if it does not exist.
* The CID Mount Point is specified
* in the CASSETUP gui.

APPDIR = MPTS

* WORKDIR is a subdirectory (relative
* to the WORK alias) where various
* application-required programs may be
* placed. It is optional, but almost
* every application will need one. The
* directory will be created if it
* does not exist.
* Some CID documentation refers to this
* as the EXE directory.
* The WORK alias is specified in the GUI.

WORKDIR = EXE\mpts50

* DLLDIR is the directory (relative to
* the DLL alias) where DLLs for
* the product will be placed. Not all
* applications will need one.
* The DLL alias is specified in the GUI.

DLLDIR = DLL\mpts50

* RSPDIR is the directory (relative to
* the RESP alias) where response
* files will be placed.

RESPDIR = RSP\mpts50

* LOGDIR is the directory (relative
* to the LOG alias) where log files
* will be placed.

LOGDIR = LOG\mpts50

* The parameters below describe the methods to be
* used to put the applications's images on the Code Server.

* METHOD defines whether XCOPY or an
* application-supplied program will be
* used to load the images.
* Methods are 1=XCOPY-is-used
*           2=Application-supplied

METHOD = 2

* NUMDSKT is the number of diskettes
* (or CD-ROMS) in the package. It is
* required when the XCOPY method is
* being used, but optional otherwise.

NUMDSKT = 1

* The next parameter deals with loading the images
* using an application-provided program.

* If METHOD==2 the IMAGELOAD keywords
* specify the commands to be run and
* the meaning of their return codes.
* IMAGELOAD.0 specifies the number of
* commands to be run.

IMAGELOAD.0 = 0

```

Figure 233 (Part 2 of 4). CASSETUP Profile for MPTS 5.0

```

* IMAGELOAD.n is a template for the
* nth command that will be executed.
* Templates may contain Symbolic
* Substitution Parameters, which will be
* replaced by actual values when the
* command line is executed.
* The Symbolic Substitutions supported
* for IMAGELOAD are
* $T      which is replaced by the
*         target path (the path to
*         which code images are to
*         be moved).
* $S      which is replaced by the
*         source drive (and,
*         possibly, path) from which
*         the code images will be
*         copied.
* $W      which is replaced by the
*         fully-qualified path of
*         the Work directory.
* $D      which is replaced by the
*         fully-qualified path of
*         the DLL directory.
* $F      which applies only to CSDs
*         and is replaced by the
*         fully-qualified path of
*         the Work directory of the
*         application being fixed.
IMAGELOAD.1 = XCOPY $$\CID\SERVER\MPTS $T /s
* The next parameter deals with commands to be
* run _before_ the image loading command. They
* are run regardless of the Method selected.
* The work directory, will be put at the front of the
* path and dpath during execution of these steps

* The SETUP keywords specify steps
* to be performed before image
* loading. Commands to unpack the
* load image program, for example, might
* go here.
* SETUP.0 says how many steps there
* are

SETUP.0 = 1

* SETUP.n gives the prompt text for
* step n. If it is blank, then the
* step is done immediately

SETUP.1 = MPTS 5.0 WARP SERVER CD-ROM
* If there is a diskette prompt, then
* the diskette can be verified either by
* Volume Label or presence of a file.
* These elements are optional.

SETUP.1.0MarkerFile = CID\SERVER\MPTS\MPTS.EXE
* SETUP.1.1Volser = WARP SERVER

* For each step, there can be as many
* commands as needed. SETUP.n.0 parm
* tells how many commands make up
* step n.

SETUP.1.0 = 0

```

Figure 233 (Part 3 of 4). CASSETUP Profile for MPTS 5.0

```

*****
*
*          INSTALL SECTION
*
* (elements in this section deal with how the application is
* remotely installed).
*****

* INSTCMD is the template of the
* install command. Symbolic
* substitution is supported for $T, $S,
* $D and $W as described above, but
* also for
*   $B (boot drive)
*   $M (Maint dir)
*   $R (response file dir)
*   $V (server name)
*   $F (directory for the /S2 parm)
*   $C (client name)
*   $O (boot drive)
INSTCMD = $$\mpts /e:prod /s:$S /t:$B /l1:$L\"client\".log /r:
* INSTCMDM is used if we use a
* different install command when running
* under a maintenance system
INSTCMDM = $$\mpts /e:maint /s:$S /t:$B /l1:$L\"client\".log /r:

* block for the install command line.
* If it is specified then the response
* file (usually /R) parameter in
* INSTPROG must be at the end of the
* string and be empty. For example:
*   myinstpg /S:something /R:
DEFRESPFILE = default.rsp
* MAINTSYSREQ tells whether the install
* command must be run under a
* maintenance system (1 is yes, 0 no)
MaintSysReq = 0

*****
*
*          MAINTENANCE SYSTEM SECTION
*
* (applications that have a PROGTYP of 1 (OS), 2 (transport)
* or 3 (redirector) have associated commands that allow them
* to be installed as part of Maintenance Systems. This section
* describes those commands.
*****

* MSCMD.0 tells how many commands
* follow
MSCmd.0 = 2

* MSCMD.n is the template for the nth
* command. Symbolic substitution for
* $T, $W, $D and $S is always supported
* and other translation is available
* during processing of Boot Diskette
* Build scripts.
MSCmd.1 = $$\mpts /e:prep /s:$S /t:$M /tu:$B /l1:$L\"client\".log /r:
MSCmd.1.0DefRespFile = default.rsp
* MSCMD.n.0CmdName associates a name
* with the nth command. The name
* should contain only letters and
* numbers, and should be unique among
* all MSCMDs in all Application
* Profiles.
MSCmd.1.0CmdName = mpts_prep

* MAINTSYSBUILD is the ordinal(s) of the
* mscmd(s) that define how a
* disk-based maintenance system is
* built with this app.
MSCmd.2 = $$\thinlaps . $T $N
MaintSysBuild = 1

```

Figure 233 (Part 4 of 4). CASSETUP Profile for MPTS 5.0

A.3.3 SystemView in Warp Server Manager Profile File

```
* CASSETUP application profile for: OS/2 Warp 3.0 (WIN-OS2 version)
*****
*          APPLICATION DESCRIPTION SECTION          *
*****

* APPNAME is a long descriptive name.
* It can contain blanks. It should be
* unique among all the Application
* Profiles.
APPNAME = SystemView in Warp Server Manager
* APPNICK is a short nickname. It is
* used to identify this application in
* other scripts and profiles. It MUST
* be unique among all the App Profiles.
* Case is ignored for this parameter,
* so KILLER10 and killer10 are
* considered equal.
APPNICK = SYSVIEW2

* PROGTYPE tells what kind of
* application this is:
*   Operating System (1),
*   Transport (2),
*   Redirector(3),
* or other (4).
PROGTYPE = 4

* ICON is the icon to be displayed to
* represent this application in CASSETUP
* A restriction in Release 1.1 of
* CASSETUP is that this must be a
* bitmap (bmp) file or DLL resource.
* The path is relative to the directory
* where cassetup is installed.
ICON = CASSETUP:#111

* OS tells whether the program runs
* under OS/2 (1) or DOS (2)
OS = 1

* PACKAGE tells whether it is a complete
* application (1) or a fix (2)
PACKAGE = 1

* If it is a fix, FIXTO is the APPNICK
* of the application it fixes.
* FIXTO =

* And FIXLEVEL specifies the relative
* fix level. It can be -1 to indicate
* it is an unsequenced fix.
* FIXLEVEL =
```

Figure 234 (Part 1 of 5). CASSETUP Profile for SystemView in Warp Server Manager

```

* Some products required that
* prerequisite products be installed on
* the code server before images can
* be loaded. Put the nicknames of
* the prereq products on this line.
* The special nickname <LCU> indicates
* that Remote Install Support must first
* be installed on the code server.

LOADPREREQS = <LCU>
*****
*
*          IMAGE LOAD SECTION          *
* (elements in this section describe how the application's
* install image is put onto a Code Server -- usually by being
* copied from install diskettes or CD-ROM)
*****
* The directories below are set up when the application's
* install images are loaded onto the code server.

* APPDIR is the subdirectory (relative
* to the CID mount point) where
* the app's install images will be
* stored. The directory will be created
* if it does not exist.
* The CID Mount Point is specified
* in the CASSETUP gui.

APPDIR = SYSVIEW2\SERVER_2

* WORKDIR is a subdirectory (relative
* to the WORK alias) where various
* application-required programs may be
* placed. It is optional, but almost
* every application will need one. The
* directory will be created if it
* does not exist.
* Some CID documentation refers to this
* as the EXE directory.
* The WORK alias is specified in the GUI.

WORKDIR = EXE\SYSVIEW2

* DLLDIR is the directory (relative to
* the DLL alias) where DLLs for
* the product will be placed. Not all
* applications will need one.
* The DLL alias is specified in the GUI.

DLLDIR = DLL\SYSVIEW2

* RSPDIR is the directory (relative to
* the RESP alias) where response
* files will be placed.

RESPDIR = RSP\SYSVIEW2

* LOGDIR is the directory (relative
* to the LOG alias) where log files
* will be placed.

LOGDIR = LOG\SYSVIEW2

```

Figure 234 (Part 2 of 5). CASSETUP Profile for SystemView in Warp Server Manager

```

* The parameters below describe the methods to be
* used to put the applications's images on the Code Server.

METHOD = 2
    * METHOD defines whether XCOPY or an
    * application-supplied program will be
    * used to load the images.
    * Methods are 1=XCOPY-is-used
    *           2=Application-supplied

NUMDSKT = 1
    * NUMDSKT is the number of diskettes
    * (or CD-ROMS)in the package. It is
    * required when the XCOPY method is
    * being used, but optional otherwise.

IMAGELOAD.0 = 0
    * The next parameter deals with loading the images
    * using an application-provided program.

    * If METHOD==2 the IMAGELOAD keywords
    * specify the commands to be run and
    * the meaning of their return codes.
    * IMAGELOAD.0 specifies the number of
    * commands to be run.

    * IMAGELOAD.n is a template for the
    * nth command that will be executed.
    * Templates may contain Symbolic
    * Substitution Parameters, which will be
    * replaced by actual values when the
    * command line is executed.
    * The Symbolic Substitutions supported
    * for IMAGELOAD are
    * $T      which is replaced by the
    *          target path (the path to
    *          which code images are to
    *          be moved).
    * $S      which is replaced by the
    *          source drive (and,
    *          possibly, path) from which
    *          the code images will be
    *          copied.
    * $W      which is replaced by the
    *          fully-qualified path of
    *          the Work directory.
    * $D      which is replaced by the
    *          fully-qualified path of
    *          the DLL directory.
    * $F      which applies only to CSDs
    *          and is replaced by the
    *          fully-qualified path of
    *          the Work directory of the
    *          application being fixed.

IMAGELOAD.1 = XCOPY $$\OS2IMAGE $T /s /e /v /h /o /t /r
IMAGELOAD.2 = GetOScid $T $W
IMAGELOAD.3 = GetRExx $T $D
IMAGELOAD.4 = GetBoot $T $W

```

Figure 234 (Part 3 of 5). CASSETUP Profile for SystemView in Warp Server Manager

```

* The next parameter deals with commands to be
* run _before_ the image loading command. They
* are run regardless of the Method selected.
* The work directory, will be put at the front of the
* path and dpath during execution of these steps

* The SETUP keywords specify steps
* to be performed before image
* loading. Commands to unpack the
* load image program, for example, might
* go here.
* SETUP.0 says how many steps there
* are

SETUP.0 = 1

* SETUP.n gives the prompt text for
* step n. If it is blank, then the
* step is done immediately

SETUP.1 = OS/2 Warp Server 3.05 CD-ROM

* If there is a diskette prompt, then
* the diskette can be verified either by
* Volume Label or presence of a file.
* These elements are optional.

SETUP.1.0MarkerFile = OS2IMAGE\DISK_0\OS2KRNLI

* For each step, there can be as many
* commands as needed. SETUP.n.0 parm
* tells how many commands make up
* step n.

SETUP.1.0 = 0
*****
*                INSTALL SECTION                *
* (elements in this section deal with how the application is *
* remotely installed).                               *
*****

* INSTCMD is the template of the
* install command. Symbolic
* substitution is supported for $T, $S,
* $D and $W as described above, but
* also for
*   $B (boot drive)
*   $M (Maint dir)
*   $R (response file dir)
*   $V (server name)
*   $F (directory for the /S2 parm)
*   $C (client name)
*   $O (boot drive)

INSTCMD = $W\svinst /X /A:I /S:$S /T:$T /11:$L\C.11 /12:$L\C.12 /13:$L\C.
13
/r:

* DEFRESPFILE is the default response
* file name. It is used during
* creation of LCU command files
* to specify a "rspdir/default"
* block for the install command line.
* If it is specified then the response
* file (usually /R) parameter in
* INSTPROG must be at the end of the
* string and be empty. For example:
*   myinstpg /S:something /R:

DEFRESPFILE = default.rsp

* MAINTSYSREQ tells whether the install
* command must be run under a
* maintenance system (1 is yes, 0 no)

MaintSysReq = 0

```

Figure 234 (Part 4 of 5). CASSETUP Profile for SystemView in Warp Server Manager

```

*****
*           MAINTENANCE SYSTEM SECTION           *
* (applications that have a PROGTYPE of 1 (OS), 2 (transport) *
* or 3 (redirector) have associated commands that allow them *
* to be installed as part of Maintenance Systems. This section *
* describes those commands. *
*****

* MSCMD.0 tells how many commands
* follow

MSCmd.0 = 2

* MSCMD.n is the template for the nth
* command. Symbolic substitution for
* $T, $W, $D and $S is always supported
* and other translation is available
* during processing of Boot Diskette
* Build scripts.

MSCmd.1 = $W\semaint /s:$S /t:$M /b:$B /l:$L "client".log
MSCmd.1.0CmdName = semaint

MSCmd.2 = $W\sedisk /S:$S /T:$T
MSCMD.2.0CmdName = sedisk

MaintSysBuild = 1

```

Figure 234 (Part 5 of 5). CASSETUP Profile for SystemView in Warp Server Manager

Appendix B. Special Notices

This publication is intended to help IBM systems engineers and customers install and configure specific components of the IBM OS/2 Warp Server product. The information in this publication is not intended as the specification of any programming interfaces that are provided by IBM OS/2 Warp Server. See the PUBLICATIONS section of the IBM Programming Announcement for IBM OS/2 Warp Server 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, 500 Columbus Avenue, Thornwood, NY 10594 USA.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

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.

The following document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

ADSTAR	AIX
AnyNet	AS/400
BookManager	DB2/2
FFST/2	IBM
IMS	LAN Distance
Library Reader	Micro Channel
MVS/ESA	NetDoor
NetFinity	NetView
Nways	OS/2
OS/400	Presentation Manager
Print Services Facility	PS/2
PSF	RISC System/6000
RS/6000	S/390
SystemView	ThinkPad
WIN-OS/2	Workplace Shell

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Microsoft, Windows, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

Java and HotJava are trademarks of Sun Microsystems, Inc.

IPX/SPX, NetWare	Novell, Inc.
Lotus Notes	Lotus Development Corporation
Microsoft WORD	Microsoft Corporation
cc:Mail	cc:Mail, Inc., a wholly owned subsidiary of Lotus Development Corporation
MarkVision	Lexmark International, Inc.
SunOS, Network File System, NFS	Sun Microsystems, Inc.
PostScript	Adobe Systems, Inc.
AppleTalk	Apple Computer, Inc.
Laserjet, Laserjet Series II	Hewlett-Packard Company

Other trademarks are trademarks of their respective companies.

Appendix C. Related Publications

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

C.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see "How To Get ITSO Redbooks" on page 337.

- *Inside OS/2 Warp Server, Volume 1: Exploring the Core Components*, SG24-4602
- *Workgroup Management Using SystemView for OS/2*, SG24-2596
- *Software Distribution Using SystemView for OS/2 Version 1.1* SG24-4609
- *Using ADSM to Back Up OS/2 LAN Server and Warp Server*, SG24-4682
- *Inside OS/2 LAN Server 4.0*, SG24-4428
- *OS/2 Warp Generation, Volume 1: OS/2 Warp Version 3, OS/2 Warp with Windows and BonusPak*, SG24-4552
- *OS/2 Warp Generation, Volume 2: Exploring LAN Connectivity with OS/2 Warp Connect*, GG24-4505
- *TCP/IP V2.0 for OS/2 Installation and Interoperability*, available on the *Networking and Systems Management Redbooks Collection Kit*, SK2T-6022-06
- *Understanding IBM OS/2 LAN Server Performance Tuning*, GG24-4430

C.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year at significant savings.

CD-ROM Title	Subscription Number	Collection Kit Number
System/390 Redbooks Collection	SBOF-7201	SK2T-2177
Networking and Systems Management Redbooks Collection	SBOF-7370	SK2T-6022
Transaction Processing and Data Management Redbook	SBOF-7240	SK2T-8038
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RISC System/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RISC System/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
Application Development Redbooks Collection	SBOF-7290	SK2T-8037
Personal Systems Redbooks Collection	SBOF-7250	SK2T-8042

C.3 Other Publications

These publications are also relevant as further information sources:

- *OS/2 Warp Server Version 4 Easy Start*, S25H-8003
- *OS/2 Warp Server Version 4 Up and Running!*, S25H-8004
- *SystemView for OS/2 Version 1 Release 1*, SH19-4184

- *OS/2 LAN Server Network Administrator Reference, Volume 1: Planning, Installation, and Configuration*, S10H-9680
- *OS/2 LAN Server Network Administrator Reference, Volume 2: Performance Tuning*, S10H-9681
- *OS/2 LAN Server Network Administrator Reference, Volume 3: Network Administrator Tasks*, S10H-9682
- *LAN Server Command and Utilities*, S10H-9686
- *IBM LAN Distance Remote Guide*, S52G-8393
- *IBM LAN Distance Advanced Guide*, S52G-8394
- *IBM Multi-Protocol Transport - AnyNet for OS/2: Configuration Guide*, S25H-7867
- *IBM NetFinity Manager for OS/2 V3.0 - User's Guide*, S41H-6268-00
- *LAN Technical Reference IEEE 802.2 and NETBIOS APIs*, SC30-3587
- *IBM TCP/IP Version 2.0 for OS/2 Domain Name Server Guide*, SC31-7174

How To Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at URL <http://www.redbooks.ibm.com>.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **PUBORDER** — to order hardcopies in United States
- **GOPHER link to the Internet** - type `GOPHER.WTSCPOK.ITSO.IBM.COM`
- **Tools disks**

To get LIST3820s of redbooks, type one of the following commands:

```
TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
```

To get lists of redbooks:

```
TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET LISTSERV PACKAGE
```

To register for information on workshops, residencies, and redbooks:

```
TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
```

For a list of product area specialists in the ITSO:

```
TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
```

- **Redbooks Home Page on the World Wide Web**

<http://w3.itso.ibm.com/redbooks>

- **IBM Direct Publications Catalog on the World Wide Web**

<http://www.elink.ibm.link.ibm.com/pbl/pbl>

IBM employees may obtain LIST3820s of redbooks from this page.

- **REDBOOKS category on INEWS**
- **Online** — send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL
- **Internet Listserver**

With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibm.link.ibm.com with the keyword `subscribe` in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Online Orders** (Do not send credit card information over the Internet) — send orders to:

In United States:	IBMMAIL usib6fpl at ibmmail	Internet usib6fpl@ibmmail.com
In Canada:	caibmbkz at ibmmail	lmannix@vnet.ibm.com
Outside North America:	dkibmbsh at ibmmail	bookshop@dk.ibm.com

- **Telephone orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	(long distance charges apply)
(+45) 4810-1320 - Danish	(+45) 4810-1020 - German
(+45) 4810-1420 - Dutch	(+45) 4810-1620 - Italian
(+45) 4810-1540 - English	(+45) 4810-1270 - Norwegian
(+45) 4810-1670 - Finnish	(+45) 4810-1120 - Spanish
(+45) 4810-1220 - French	(+45) 4810-1170 - Swedish

- **Mail Orders** — send orders to:

IBM Publications Publications Customer Support P.O. Box 29570 Raleigh, NC 27626-0570 USA	IBM Publications 144-4th Avenue, S.W. Calgary, Alberta T2P 3N5 Canada	IBM Direct Services Sortemosevej 21 DK-3450 Alleroperating systemd Denmark
--	--	---

- **Fax** — send orders to:

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States)** or **(+1) 415 855 43 29 (Outside USA)** — ask for:

Index # 4421 Abstracts of new redbooks
Index # 4422 IBM redbooks
Index # 4420 Redbooks for last six months

- **Direct Services** - send note to softwareshop@vnet.ibm.com

- **On the World Wide Web**

Redbooks Home Page	http://www.redbooks.ibm.com
IBM Direct Publications Catalog	http://www.elink.ibm.link.ibm.com/pbl/pbl

- **Internet Listserver**

With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibm.link.ibm.com with the keyword `subscribe` in the body of the note (leave the subject line blank).

IBM Redbook Order Form

Please send me the following:

Title	Order Number	Quantity

First name Last name

Company

Address

City Postal code Country

Telephone number Telefax number VAT number

Invoice to customer number _____

Credit card number _____

Credit card expiration date Card issued to Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

DO NOT SEND CREDIT CARD INFORMATION OVER THE INTERNET.

List of Abbreviations

ACL	Access Control List	IBM	International Business Machines Corporation
ADF	Adapter Description File	IML	Initial Machine Load
ADF	Application Definition File	IP	Internet Protocol
ADP	Adapter Description File	IPC	Interprocess Communication
ADSM	ADSTAR Distributed Storage Manager	IPDS	Intelligent Printer Data Stream
AFP	Advanced Function Printing	IPF	Information Presentation Facility
APPC	Advanced Program-to-Program Communication	IPX	Internetwork Packet Exchange
CAE	X/OPEN Common Application Environment	I/S	Information Systems
CID	Configuration Installation and Distribution	IT	Information Technology
CTS	Common Transport Semantics	LAA	Locally Administered Address
DCAF	Distributed Console Access Facility	LLB	Local Location Broker
DCDBREPL	Domain Control Database Replicator	LTLW	LAN-to-LAN-over WAN
DGS	Diagnostic Generation System	LUN	Logical Unit Number
DLS	DOS LAN Services	MCF	Model Change File
DMI	Desktop Management Interface	MIB	Management Information Base
DMTF	Desktop Management Task Force	MIF	Management Information File
DPI	Distributed Protocol Interface	MPTN	Multiprotocol Transport Networking
DPI	Dots Per Inch	MPTS	Multiprotocol Transport Service
DSOM	Distributed System Object Model	MRF	Model Response File
ECC	Error Checking and Correction	NCK	Network Computing Kernel
EISA	Extended Industry Standard Architecture	NCS	Network Computing System
ESDI	Enhanced Small Device Interface	NDIS	Network Driver Interface Specification
FAT	File Allocation Table	NFS	Network File System
FFST	First Failure Support Technology	NFSD	Network File System Daemon
GLB	Global Location Broker	NIF	Network Information File
GUI	Graphical User Interface	NLM	NetWare Loadable Modules
H-Node	Hybrid Node	NMI	Non-Maskable Interrupt
HPFS	High Performance File System	NPAP	Network Printing Alliance Protocol
		NTS	Network Transport Services
		NVDM	NetView Distribution Manager
		OSI	Open Systems Interconnection
		P-Node	Point-to-Point Node
		PCI	Peripheral Component Interconnect

PCL	Printer Control Language	SMP	Symmetric Multiprocessing
PFA	Predictive Failure Analysis	SNA	System Network Architecture
PPDS	IBM Personal Printer Data Stream	SNMP	Simple Network Management Protocol
PSF	Print Services Facility	SPX	Sequenced Packet Exchange
POR	Power-On Reset	SRVIFS	Service Installation File System
POST	Power-On Self Test	TAP	Telocator Alphanumeric Protocol
PUN	Physical Unit Number	TCP/IP	Transmission Control Protocol/Internet Protocol
RAID	Redundant Array of Inexpensive Disks	UAA	Universally Administered Address
RIPL	Remote Initial Program Load	UDP	User Datagram Protocol
RPC	Remote Procedure Call	UNC	Universal Naming Convention
SCSI	Small Computer System Interface	VIM	Vendor Independent Messaging
SDM	Software Distribution Manager	WAN	Wide Area Network
SIA	System Information Agent		

Index

A

- abbreviations 341
- acronyms 341
- ADF Files 212
 - structure 214
- AF_INET Address family 300
- AF_NB Address family 300
- AF_OS2 Address family 300
- Alert Manager 77
 - alert information 79
 - alert processing options 77
 - configuring 80
 - command macros 80
 - editing 82
 - Error Conditions 85
- AnyNet function
 - 2217 Nways Multiprotocol Concentrator 296
 - APPC over TCP/IP 296
 - benefits to OS/2 Warp Server 301
 - Common Transport Semantics 299
 - IPX over SNA gateway 298
 - LTLW 298
 - native Sockets services 300
 - NetBIOS over SNA 298
 - NetBIOS over SNA gateway 298
 - non-native Sockets services 300
 - product changes 295
 - publications 304
 - RFC 1001/1002 299
 - SNA over TCP/IP 296
 - Sockets over IPX 298
 - Sockets over NetBIOS 297
 - Sockets over SNA 296
- APPC over TCP/IP 296

B

- Backup and Recovery
 - ADSM 280
 - backup method 284
 - backup set 284
 - backup strategy 291
 - compression 285
 - creating a new method 284
 - DCDB Replicator 277
 - device support 280
 - Disaster Recovery Utility
 - boot disk options 290
 - creating boot diskettes 290
 - supported devices 290
 - features 279
 - Filters
 - file filters 286
 - tree filters 286

Backup and Recovery (*continued*)

- generation 285
- incremental backups 287
- positioning 279
- rulebook 286
- scenarios 288
- SCSI options 281
- storage device 284

bibliography 335

C

- CASENG3.CMD 151
- CASENG6.CMD 151
- CASPREP 169
- CASSETUP 126, 144, 227, 319
 - application profiles 155
 - CASSETUP.STR 153, 163
 - configuring 161
 - correct version 153
 - installing 151
 - MPTS 5.0 Profile file 324
 - OS/2 Warp V3 profile file 319
 - SystemView Manager Profile file 328
- change control (CC) 126
- CID 124
- CID-enabled applications 144, 211, 212
- Code Server
 - aliases 200
 - definition 196
 - directory structure 147, 198
 - installing 148
 - TCP/IP client 141
 - using NetWare 142
 - using TCP/IP 138
- Coexistence
 - SystemView and NetFinity V3 115
 - SystemView and NVDM/2 117
- Common Transport Semantics 294
- Critical File Monitor 67
 - default files 68

D

- DCAF 100, 118
- Dictionary file 50
- Discovery filters 33
 - group filters 33
- DiskCamera 210
 - description 210
 - limitations 211
- DMI 78, 82, 105
- DTMF 105

E

- ECC Memory Options 69
 - ECCMEM command line 70
- Event Scheduler 89, 226
 - using 226

F

- File Transfer 75
 - compression 75
 - disabling 77
 - DOS transfer limitations 75
- FNDLOG 195

G

- Groups, in SystemView
 - adding systems to group 34
 - creating 31
 - detail view 36
 - icon view 35

H

- HP JetAdmin
 - configuring 273
 - device support 271
 - features 270
 - installing 272
 - protocol required 272
 - managing 274

I

- IBM 4019 Printer 240
- IBM 4029 Printer 240
- IBM Networking Blueprint 293
- IEEE P1284.1 255

L

- LANINSTR command 178
- LAPSRSP 175
- LexMark 4039 Printer 265
- License control 6
- License Management 107
 - location brokers 113
 - nodelocked 108
 - security levels 111
 - server-based 109
- LTLW, see AnyNet

M

- MAKENFS.CMD 141
- MarkVision Print Utility
 - configuring 259
 - functions 255
 - installing 256
 - protocol required 257

- MarkVision Print Utility (*continued*)
 - installing (*continued*)
 - setup screen 258
 - managing 264

MIB 105

MIF 105

Multiprotocol Transport Networking

- access node 294
- address mapper node 295
- address mapping 294
- CTS function 294
- function compensation 294
- gateway node 295
- native Sockets services 300
- NB30 API 297
- NetBIOS over TCP/IP 299
- non-native Sockets services 300

N

- NetBIOS over SNA 298
- NetBIOS over TCP/IP 299
- NetView Distribution Manager
 - commands 196
 - NVDM.CFG 191
- NFS 125, 138
- NFS mount command 141
- Non-CID-enabled applications 144, 196
 - scripts 207
- NPAP 255
- NvDM/2 116
- NvDM/6000 116, 228

O

- OS2WS.PRO 156, 319

P

- Power-On Error Detect 85
- Predictive Failure Analysis 86
 - drive options 88
 - information 87
- Print Services Facility/2
 - creating PSF/2 queue 243
 - device 235
 - input data streams 235
 - installing 236
 - AFP job conversion 237
 - postscript job conversion 237
- PSF/2 Devices 238
 - creating 238
 - printer attachment types 239
- publications 275
- Resource library 253
 - inline resources 253
 - resource groups 253
- supported printer data streams 240
- TCP/IP attachment 242

- Print Services Facility/2 (*continued*)
 - terminal transform 236
 - transforms 243
 - additional transforms 244
 - definition of 243
 - generic transform 245
 - passthru 250
 - transform exit 243
 - Upload'n'Print 250
 - using APRINT 251
 - using Print Submitter 251
- Printing in OS/2 Warp Server
 - bidirectional printer support 234, 255
 - creating printer objects 232
 - installing printer drivers 233
 - Print drivers 231
 - printer objects 231
 - printer ports 231
 - publications 275
 - sharing print resources 234
- Process Manager 92
 - alerts 94
 - working with 94
 - process information 92
 - remote commands 93
 - stopping remote processes 93

Q

- QSoft Dictionary 47

R

- RAID Manager 70
 - adding/deleting drives 74
 - description 70
 - DLL errors 72
 - parity storage 74
 - read ahead 74
 - rebuild priority 73
 - stripe size 73
 - supported RAID adapters 75
 - viewing information 71
- RCSHD.EXE 98
- Remote Session 96
 - keystrokes 97
 - PM applications 98
 - sample sessions 98
- Remote Workstation Control 98
 - actions 99
 - comparing to DCAF 100
 - CONFIG.SYS considerations 100
 - keystrokes 102
 - limitations 99
 - session states 103
- Response Files 171
 - for SystemView Manager 181
 - included with SystemView 212
 - samples 171

- Response Files, CID 172
 - definition 172
- RFC 1001/1002 299

S

- Screen View 104
- Security Manager
 - password checking 42
 - setting up User ID/Password 40
- SEDISK utility 134
- SERVICE.INI 132, 163
- SERVICE.LST 132
- SETBOOT command 99
- SMP OS/2 Warp Server
 - Adapter and Protocol Services enhancements 308
 - Advanced Print Services enhancements 312
 - definition of 305
 - File and Print Sharing Services
 - enhancements 309
 - High Memory Support 307
 - kernels 308
 - OS/2 Warp Server Backup/Restore
 - enhancements 310
 - Raw I/O File System 307
 - Remote Access enhancements 310
 - STRACE 308
 - supported hardware 306
 - SYSLEVEL 308
 - Systems Management enhancements 311
 - TCP/IP enhancements 309
 - TCPBEUI enhancements 308
 - threads 305
 - tracking clients 312
- SNA over TCP/IP 296
- SNMP 77, 80
- Sockets interface 296, 298, 299
- Sockets over IPX 298
- Sockets over NetBIOS 297
- Sockets over SNA 296
- Software Distribution
 - CID-enabled applications 144, 211, 212
 - communications requirements 187
 - components 185
 - distributing 223
 - error log 195
 - Event Scheduler 226
 - installation modes 123
 - installing operating systems 143
 - Non-CID-enabled applications 144, 196
 - preparing non-CID applications 202
 - prerequisite tasks 188
 - process explained 221
 - product table 127
 - publications 230
 - response files included 212
 - summary table 229
 - using redirected drives 127

- Software Inventory 46, 315
 - dictionaries 48
 - export to database 50
 - exporting to database 317
 - Inventory Report example 315
 - reports 49
- SRVIFS 125, 128
 - client 134
 - comparing to LAN Server 138
 - installing 131, 133
 - OS/2 boot diskettes 134
 - creating for client 167
- SVINST command 159
- System Information Tool 44, 313
 - SCSI information output 313
- System Monitor 58
 - context menus 61
 - export to database 66
 - notebooks 63
 - report information 58
 - settings 65
 - tips 66
- System Partition Access 90
 - actions 91
 - ESDI considerations 91
- System Profile 55
- SystemView
 - architecture 28
 - components 3
 - DOS/Windows Client 6
 - Manager 4
 - OS/2 Client 5
 - Desktop folder contents 30
 - function summary 119
 - product-specific installation 15
 - publications 121
 - remote installation 159
 - response file 181
- SystemView Agent 105
 - subagents 106
- SystemView Client 15
 - DOS/Windows Client 18
 - installing 15
 - OS/2 Client install 16
 - configuring 24
 - required parameters 17
- SystemView Manager
 - adding/removing options 26
 - coexisting with NetFinity 115
 - configuring 19
 - Hard disk usage 10
 - integrated installation 11
 - managing clients 31
 - NetBIOS resources 9
 - optional components 13
 - prerequisites 7
 - protocols 9
 - public access 21

- SystemView Manager (*continued*)
 - required parameters 14
- SystemView Model 2

T

- THINIFS 135
- transforms in PSF/2
 - See* Print Services Facility/2, transforms

V

- VIM 78

W

- WAV files 77, 81

IBML®

Printed in U.S.A.

SG24-4702-00

